Næste generation af NemID

Review af RMC og ICGs
Fase 3 scenarieanalyse

Gert Læssøe Mikkelsen
Jonas Lindstrøm
Alexandra Instituttet A/S
14. april 2015

Indholdsfortegnelse

1. Ledelsesresumé 3

2. Indledning 4

3. Perspektiver for review 4

3.1. Privacy 4

3.2. Sikkerhed 6

3.3. Brugeroplevelse 6

3.4. Migrering 6

3.5. Fremtidssikring 6

3.6. Teknisk modenhed 7

4. Review af scenarier 7

4.1. Arkitekturgrundlag 8

4.2. Scenarie 1 – As-is med mindre forbedringer 10

4.3. Scenarie 2 13

4.4. Scenarie 3 16

5. Opsummering 19

1. Ledelsesresumé

Rambøll Management Consulting og Implement Consulting Group (RMC-ICG) præsenterer i rapporten *Næste generation af NemID, Fase 3 Scenarie analyse: oplæg til beslutninger* tre mulige scenarier for den næste genration af NemID. Denne rapport indeholder vores kommentarer til RMC-ICGs rapport. Generelt er vi enige i de fleste af RMC-ICGs vurderinger, og RMC-ICGs rapport virker godt gennemarbejdet.

I scenarie 1 videreføres den nuværende løsning med meget få ændringer. Vælger man at bruge dette scenarie, bør man være opmærksom på, da tidshorisonten er meget lang, at løsninger, der virker sikre i dag, ikke nødvendigvis vil være sikre i fremtiden. Både nye udfordringer, nye anvendelser, øget fokus på sikkerhed og nye krav fra brugere og tjenesteudbydere kan medføre, at en eksisterende løsning i fremtiden kan komme til at fremstå som værende mindre sikker end i dag. Derfor mener vi, det er afgørende, at den næste generation af NemID bliver fleksibel, og at den læner sig op af moderne, internationale standarder, således at nye krav kan implementeres gnidningsfrit. Det samme er tilfældet med privacy, hvor der i øvrigt allerede i dag findes teknologier, der tillader kontekstafhængig information, f.eks. OpenID Connect, der vil beskytte brugernes privatliv bedre end den nuværende NemID.

I scenarie 2 lægges der blandt andet op til, at brugerne skal have mulighed for at kunne logge ind udelukkende ved at angive brugernavn og kodeord. Den løsning kendes allerede fra netbankernes Kontokig og giver bedre brugervenlighed, hvilket vil gøre det mere attraktivt for tjenesteudbydere at bruge NemID. Her bemærker vi, at man skal være opmærksom på, at det præcist bliver specificeret, hvilke data en tjenesteudbyder må give adgang til baseret på et login udelukkende med kodeord. Tjenesteudbydere og brugere må antages at have en interesse i den højeste grad af brugervenlighed, hvilket kan komme til at gå ud over sikkerheden.

Det er også værd at bemærke, at en stor del af de angreb, der er på brugere af NemID i dag, er phishing-angreb, hvor en bruger franarres sit kodeord, f.eks. via en falsk NemID klient. Sådanne angreb bliver mere attraktive, hvis flere tjenesteudbydere giver adgang udelukkende ved hjælp af kodeord.

Scenarie 3 lægger op til mulighed for kontekstafhængig information og brug af flere login-faktorer. Kontekstafhængig information gør det muligt for brugerne at videregive relevant, og kun relevant information, til tjenesteudbydere. Det vil forbedre graden af privacy, da der ikke bliver videregivet ikke relevant information. Dette kan være medvirkende til at nedbringe brugen af CPR-numre hos private tjenesteudbydere. Kontekstafhængig information kan også give bedre brugeroplevelser, men det skal implementeres korrekt, så brugerne ikke ser det som et forstyrrende ekstra skridt i login-proceduren.

Brug af flere login-faktorer er ikke knyttet til mulighed for kontekstafhængig information, men er blot behandlet i samme scenarie. Mulighed for flere login-faktorer vurderer vi er en god ide, da vi forventer, det er noget brugerne i løbet af de kommende år vil møde i andre løsninger. Især vil det være en fordel med løsninger, der kan bruges på tværs af både den nye NemID, men også andre kommercielle løsninger. En bredere anvendelse vil også kunne medvirke til en form for brugerbetaling, for eksempelvis hardware tokens.

I scenarie 2 og 3 forudsættes det i RMC-ICGs rapport, at arkitekturen ændres, således at signatur- og identitetsdelen splittes op. Dette har også andre fordele, og identitetsdelen vil kunne implementeres med mere moderne protokoller, som tjenesteudbyderne måske kender fra andre løsninger. I forbindelse med scenarie 2 og 3

diskuteres det også at ændre arkitekturen ved at indføre brokere som en ekstra aktør. Vi vurderer, at der er en del fordele ved at indføre brokere, men det er svært helt at sige hvilke, da oplægget på dette punkt ikke er særligt konkret.

2. Indledning

Vi vil i denne rapport lave review af tre scenarier for den næste generation af NemID, som de er præsenteret i RMC-ICGs rapport: *Næste generation af NemID, Fase 3 Scenarie analyse: oplæg til beslutninger*. Vi vil hovedsageligt omtale de tilføjelser og kommentarer, vi har til rapporten

I afsnit 3 vil vi præsentere ud fra hvilke perspektiver, vi har lavet review på rapporten, og vil give en kort gennemgang af hvert.

I afsnit 4 følger vores review af arkitekturoplægget (sektion 8 i RMC-ICGs rapport), samt af de tre scenarier fra RMC-ICGs rapport ud fra de perspektiver, der er nævnt i afsnit 3.

Afsnit 5 er en opsummering af de vigtigste pointer på tværs af scenarierne.

Vi har ikke kommentarer til "Øvrigt løsningselement – NemID for børn under 15 år" fra RMC-ICG rapporten, da det meste af emnet ligger uden for vores faglige område.

3. Perspektiver for review

Vores review vil for hvert af de tre scenarier blive gennemført ud fra følgende perspektiver: Privacy, sikkerhed, brugeroplevelse, migrering, fremtidssikring og teknisk modenhed. I de følgende afsnit vil vi forklare, hvordan vi forstår de forskellige perspektiver, og hvad vi i hvert af dem vil lægge vægt på.

3.1. Privacy

Privacy har fået meget offentlig opmærksomhed de senere år, og det har fået nogle brugere til at stille større krav til deres privatlivsbeskyttelse. Vi vil derfor diskutere, hvorvidt graden af privatlivsbeskyttelse i de foreslåede scenarier vil være tilfredsstillende for brugere og tjenesteudbydere mange år frem.

Vi vurderer i denne rapport privacy ud fra hvilke informationer om brugeren der overdrages eller lækkes til både tjenesteudbydere og andre parter, f.eks. identitetsgaranter. Det gælder også indirekte informationer, såsom i hvor høj grad identitetsgaranten eller andre kan spore, hvilke tjenesteudbydere brugeren benytter og hvornår (dette kan sammenlignes med debatten om "meta-data"), og i hvor høj grad det er muligt for tjenesteudbydere at samkøre brugerdatabaser. Derudover vurderer vi det ud fra i hvor høj grad, det er gennemsigtigt for brugeren, hvilke informationer der bliver gjort tilgængelige for hvilke aktører og hvornår.

Nye teknologier og protokoller kan være medvirkende til at forbedre privatlivsbeskyttelsen for brugere og tjenesteudbydere i den næste generation af NemID. Vi vil komme med anbefalinger til, hvilke teknologier vi mener kunne være anvendelige i de forskellige scenarier.

Et eksempel på en sådan teknologi er privacy-preserving attribute-based credentials (p-ABC), der på dansk kaldes *kontekstafhængige akkreditiver*. P-ABC teknologi er blevet behandlet i flere internationale forskningsprojekter, bl.a. EU FP7 forsknings-

projektet ABC4Trust[1], og konkret findes der to implementeringer af teknologien nemlig Microsoft U-Prove[2] og IBM IdentityMixer[3]. P-ABC virker sådan, at der kan laves specielle certifikater, der ikke kan linkes, når de bruges på tværs af tjenesteudbydere, samtidigt med at brugeren kan vælge, hvilke oplysninger fra et certifikat, der skal vises til en tjenesteudbyder. Det at der kan udvælges, hvilke oplysninger der skal videregives, kaldes selektiv eller minimal visning af data (på engelsk selective/minimal disclosure), eller som i rapporten fra RMC-ICG: kontekstafhængig information. Privacy-ABC teknologi gør det også muligt at bruge certifikaterne, uden at identitetsgaranten kan følge med i, hvilke tjenesteudbydere en bruger benytter.

Der findes andre løsninger, der kan understøtte kontekstafhængig information, blandt andet OpenID Connect, OAuth, SAML etc. Der er dog væsentlige forskelle på løsninger baseret på OpenID Connect, OAuth, SAML etc. og på løsninger baseret på p-ABC. En af de største forskelle er, at brugerens brug af sin identitet kan følges af identitetsgaranten i OpenID Connect, OAuth, SAML etc., men at det kan undgås i p-ABC løsninger. Således giver p-ABC brugeren langt større privacy-garantier end de andre løsninger.

At identitetsgaranten kan følge med i, hvilke tjenesteudbydere en bruger benytter, gør sig også gældende ved den nuværende NemID-løsning. Derudover understøtter den nuværende NemID-løsning ikke pseudonymer, idet der er en global identifier af brugeren (PID i certifikatet).

RMC-ICG vurderer, at den nuværende NemID-løsning har et højt niveau af privacy:

> *I alle praktiske sammenhænge er den entydige identifikation af brugeren således reelt begrænset til PID/RID eller CPR. Både PID/RID og CPR er globale identifikatorer, der kan sammenkædes på tværs af tjenesteudbydere.*
>
> *I sig selv kan NemID derfor siges at have et højt niveau af privacy (s.88).*

Men da der findes teknologier, der i langt højere grad end den nuværende NemID-løsning beskytter brugernes privatliv, vurderer vi, i modsætning til RMC-ICG, at den nuværende NemID-løsning *ikke* har et særligt højt niveau af privacy. For eksempel har den tyske eID løsning meget mere fokus på privacy.

OCES delen af NemID bruges både til adgang til det offentlige og som identitetsløsning overfor private virksomheder. I den offentlige administration er der generelt udpræget brug af CPR-numre, og derfor er der behov for at NemID eller relaterede services kan videregive CPR-numre til offentlige services. Dette er et vilkår for NemID, og derfor ikke begrundelsen for vores vurdering.

Overfor private videregives altid PID, hvilket giver entydig identifikation på tværs af tjenesteudbydere. Derudover stilles der en service til rådighed der kan verificere om et givent PID og CPR hænger sammen. Der findes løsninger, der giver mulighed for tjenesteudbyderspecifikke pseudonymer, hvilket giver et højere niveau af privacy end brugen af PID'er. Mulighed for kontekstafhængig information vil også hæve niveauet af privacy, da det kan sænke brugen af CPR-numre. Yderligere er det teknisk muligt for identitetsgaranten at spore hvilke tjenesteudbydere en given bruger benytter. Om dette rent faktisk sker, og i så fald om disse data bliver brugt, ved vi ikke, men det er en teknisk mulighed.

[1] http://www.abc4trust.eu
[2] http://research.microsoft.com/en-us/projects/u-prove/
[3] https://idemixdemo.mybluemix.net/

3.2. Sikkerhed

Sikkerhed, der skal forstås som en garanti for, at en bruger efter autentificering er dén, han udgiver sig for at være, er afgørende for brugernes og tjenesteudbyderes tillid til en identitetsløsning. Vi vil sammenligne den sikkerhed, de forskellige scenarier tilbyder, med både den eksisterende NemID-løsning og med andre lignende løsninger, der er tilgængelige på markedet.

Nye teknologier og protokoller kan være medvirkende til at forbedre sikkerheden for brugere og tjenesteudbydere i den næste generation af NemID. Vi vil, komme med anbefalinger til, hvilke teknologier vi mener kunne være anvendelige i de forskellige scenarier.

Derudover vil vi komme med et bud på, om sikkerheden i de foreslåede scenarier vil være tilstrækkelig til at kunne imødekomme de udfordringer, den næste generation af NemID måtte møde i fremtiden. Det er dog svært at give helt konkrete vurderinger da alle scenarierne i RMC-ICGs rapport er beskrevet på et meget overordnet plan.

3.3. Brugeroplevelse

En god brugeroplevelse er afgørende for, at den næste generation af NemID bliver en succes. Brugeroplevelsen skal her ikke udelukkende forstås som brugervenlighed ift. brugergrænsefladen men omfatter hele den oplevelse og opfattelse, brugeren har af næste version af NemID.

Vi vil for hvert scenarie sammenligne brugeroplevelsen med den nuværende NemID, og vil også sammenligne den med andre eksisterende identitetsløsninger, som brugerne allerede er bekendt med, eller som vi forventer vil blive udbredt i den nærmeste fremtid.

Det er også afgørende, at brugerne ikke bare har nem adgang til at anvende NemID, men at der også er tillid mellem brugere, tjenesteudbydere og identitetsudbydere. Det kan f.eks. sikres ved, at brugeren oplever en gennemsigtighed omkring, hvilken information han lækker til hvilke tjenesteudbydere.

3.4. Migrering

Da NemID er en vigtig del af dansk infrastruktur, er det vigtigt, at overgangen fra den nuværende NemID til den næste generation forløber så gnidningsfrit som overhovedet muligt. Det er ligeledes vigtigt, at den nye leverandør, de involverede myndigheder og tjenesteudbydere er forberedt på de udfordringer, der måtte være.

Vi vil fokusere på de tekniske udfordringer i forbindelse med migreringen og vil ikke diskutere RMC-ICGs bud på de økonomiske omkostninger.

Især vil vi komme med bud på, hvor vanskeligt det vil være for nye tjenesteudbydere at implementere de forskellige nye teknologier, der er i spil til at blive en del af den næste generation af NemID.

3.5. Fremtidssikring

Da en ny løsning vil skulle være i drift i lang tid (frem til 2022), er det afgørende, at løsningen kan håndtere de udfordringer, der vil komme mange år ud i fremtiden.

Det er vanskeligt præcist at forudse, hvilke udfordringer der vil komme, men de kan f.eks. komme i form af nye krav fra brugere og tjenesteudbydere, f.eks. på baggrund

af udbredelsen af nye teknologier og standarder, eller hvis brugere ønsker at anvende NemID til andre formål og fra andre platforme end dem, der er tilgængelige i dag.

Et eksempel på hvor svært det kan være, og hvorfor fremtidssikring er vigtig, er den mængde tid og ressourcer, der er brugt for at få den nuværende NemID-løsning porteret til mobile enheder som smartpones of tablets. Det oplagte valg til underliggende platform var Java, da den nuværende NemID blev udviklet, men med tiden levede det ikke længere op til brugernes krav til en løsning. Det er altid svært at spå om fremtiden, men det er vigtigt, at de problemer der har været med at få NemID fra skærm 1 (PC'en) til skærm 2 (smartphones/tablets) ikke gentages til skærm 3, 4… (f.eks. smart TV, smart watches, enheder i biler).

Da Danmark er et forholdsvist lille marked globalt set, kan vi ikke forvente, at store teknologivirksomheder nødvendigvis tager højde for næste version af NemID (hverken Oracle/Sun (Java) eller Apple tog sig af, at den nuværende NemID ikke virkede på iPads, før den blev porteret til javascript). Derfor er det vigtigt at lægge sig op ad moderne internationale standarder for at minimere risikoen for lignende problemer i fremtiden.

3.6. Teknisk modenhed

Da næste generation af NemID vil blive et kritisk infrastrukturelement i det danske samfund, er det yderst vigtigt med et robust system, og at der i tilfælde af nedbrud, er mulighed for at bruge "failover" systemer.

Vi anser dette for værende endnu mere vigtigt i fremtiden, både fordi vi mener, digital adgang via NemID vil blive anvendt til mange flere formål i fremtiden, og fordi vi mener, det digitale trusselsniveau mod den slags systemer er stigende.

Derfor vil vi vurdere, hvorvidt de teknologier, som løsningerne afhænger af, er modne nok til at kunne bruges i et så kritisk system, herunder om det kan forventes, at der er kommerciel understøttelse på et tilstrækkeligt niveau.

Vi vil også diskutere den generelle robusthed af de forskellige scenarier. Robusthed skal forstås som et systems evne til at sikre oppetid, både generelt, men også over for tekniske fejl og deciderede angreb, bl.a. Denial-of-Service (DoS) angreb.

På trods af de bedre privacy-egenskaber (p-ABC teknologi), som U-Prove og IBM IdentityMixer giver, er der stadig et stykke vej, før de er kommercielt og teknisk modne. Både Microsoft og IBM har for øjeblikket meget fokus på pilotprojekter med hhv. U-Prove og IdentityMixer, så der er mulighed for, at de i løbet af de næste par år bliver teknisk modne på et niveau, så de vil kunne bruges i et projekt som næste version af NemID. Men mulighederne for kommerciel support er p.t. usikre, og det er også usikkert, hvilke protokoller, de konkret vil komme til at understøtte og hvordan.

4. Review af scenarier

I de følgende afsnit vil vi præsentere vores review af de tre scenarier ud fra de valgte review-perspektiver.

Afsnit 4.1 beskriver vores review at arkitekturgrundlaget, som er præsenteret i afsnit 8 i RMC-ICGs rapport. Arkitekturgrundlaget ligger til grund for scenarie 2 og 3, men ikke umiddelbart scenarie 1.

De følgende tre afsnit følger review af de tre scenarier, som der er præsenteret i rapportens afsnit 11, 12 og 13.

4.1. Arkitekturgrundlag

4.1.1. Beskrivelse

Dette afsnit omhandler vores kommentarer til afsnit 8, hvori der foreslås en ny arkitekturmodel, hvor den nuværende model udvides med en eller flere brokere. En broker er en abstraktion imellem identitetsgaranten og tjenesteudbyderen og kan være en tredje part, der modtager information fra identitetsgaranten og videregiver denne eller dele af denne til tjenesteudbyderen. I afsnit 8 i RMC-ICGs rapport sammenlignes der med betalingskortscenarier, hvor en webbutik/tjenesteudbyder, benytter en kortindløser, som er en tredjepart til håndtering af selve kortbetalingen. Der nævnes fire eksempler på allerede eksisterende kommercielle brokere i dansk kontekst (DSI-Next - SikkerAdgang, KMD – NemAdgang, Nets – E-Ident og Signicat – Signicat eID). To andre eksempler i dansk kontekst er NemLogin, som allerede fungerer som broker mellem NemID og offentlige tjenesteudbydere, og som også kan berige den information, der kommer fra identitetsgaranten (NemID) og WAYF. WAYF fungerer som broker af identiteter inden for især undervisningsverdenen og ikke kun i forbindelse med NemID. Microsoft har deltaget i et pilotprojekt om brugen af brokere for adgang til helbredsdata fra kommercielle logintjenester som Google, Yahoo, eller Microsoft[4]. Der blev brugt Microsoft U-Prove i dette pilotprojekt. Pilotprojektet blev gennemført i regi af NSTIC[5] (National Strategy for Trusted Identities in Cyberspace).

Der er i rapporten lagt op til, at der skal være mulighed for flere brokere og flere identitetsgaranter. Modellen med brokere og mulighed for flere brokere og flere identitetsgaranter giver mulighed for en mere heterogen opbygning, hvor forskellige brokere og identitetsgaranter kan understøtte forskellige teknologier, brugeroplevelser m.v. Det er vigtigt at sikre, at alle brugergrupper, herunder handicappede, stadig har ordentlige muligheder hos mindst en broker og identitetsgarant, selv hvis det ikke umiddelbart er kommercielt fordelagtigt som broker/identitetsgarant at understøtte handicappede brugere.

4.1.2. Privacy

Alt efter hvordan en opbygning med brokere bliver implementeret, kan beskyttelse af brugerens privatliv både forbedres, men også forværres. Dette bemærkes også i rapporten:

> *Der er en række problemstillinger i forhold til sikring af brugernes privatliv, der skal håndteres. Eksempelvis bør det vurderes, om der skal udvikles et interface, der sikrer, at brokere ikke har adgang til signeringsdata i forbindelse med, at de fungerer som signeringstjenester. (s. 32)*

Dette gælder dog ikke kun signeringdata men også indentitetsatrributter, og hvis der ikke implementeres tekniske løsninger imod det, kan en broker blive en ekstra aktør, der kan følge og profilere brugeren ud fra hvilke tjenesteudbydere hun benytter. Hvis der til gengæld implementeres tekniske løsninger kan introduktionen af brokere

[4] https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=3050
[5] http://www.nist.gov/nstic/index.html

til dels højne graden af privacy, ved at afkoble tjenesteudbyder og identitetsgaranten.

En anden mulighed for at højne graden af privacy for brugeren er at introducere tjenesteudbyderspecifikke pseudonymer. Dette er også bemærket i rapporten. Pseudonymer og tjenesteudbyderspecifikke pseudonymer er noget, der allerede begynder at komme i kommercielle løsninger, så vi anser det som sandsynligt, at mange brugere allerede i nær fremtid vil forvente dette af et produkt som næste version af NemID.

I rapporten diskuteres det, om tjenesteudbyderspecifikke pseudonymer skal være ens på tværs af brokere.

> *Ved introduktion af tjenesteudbyderspecifikke pseudonymer bør det vurderes, om pseudonymerne skal være ens på tværs af brokere, for at understøtte tjenesteudbyderes anvendelse af flere brokere (s. 32)*

Det bør noteres, at uden brug af p-ABC teknologi kan det være teknisk svært/umuligt at gøre dette, uden at involvere både identitetsgarant og broker. Hvis tjenesteudbyderspecifikke pseudonymer implementeres, er det vigtigt at gøre dette på en måde, så tjenesteudbyderen ikke kan finde brugerens oprindelige identitet ved hjælp af "brute-force" angreb. Et sådan angreb kan ske, hvis f.eks. pseudonymet er implementeret ved at hashe brugerens ID og tjenesteudbyderens navn sammen til et pseudonym. I et sådant tilfælde vil det være muligt for tjenesteudbyderen at udføre samme hashing-operation og dermed tjekke, om en given bruger svarer til et givent pseudonym.

p-ABC teknologi indeholder også tjenesteudbyder specifikke pseudonymer, og gør det faktisk muligt, at brugeren selv kan fungere som broker mellem identitetsgarant og tjenesteudbyder.

Ens pseudonymer på tværs af identitetsgaranter er ikke overvejet i rapporten. Der kan både være fordele og ulemper ved disse, og det er klart, at hvis dette er et ønske, vil det give en mere kompliceret arkitekturmodel.

4.1.3. Sikkerhed

Indførelsen af flere aktører, identitetsgaranter og brokere kan give større robusthed, da der ikke er noget *single point of failure.* Men det øger samtidig mulighederne for at angribe systemet.

> *Der er mulighed for, at brugerne kan vælge løsninger fra forskellige identitetsgaranter og dermed opnå større redundans. Ligeledes kan tjenesteudbydere vælge at integrere til flere brokere. (s.31)*
>
> *Det er væsentligt for den samlede sikkerhed, at både identitetsgaranter og brokere har et højt sikkerhedsniveau (s.30)*

Derudover kan det være sværere for brugeren at overskue, om den broker en bruger anvender, er én brugeren bør stole på. I eksemplet med betalingskort-infrastruktur er der i dag så mange forskellige kortindløsere, at brugere ofte ikke har anden mulighed for at validere, om kortindløseren er troværdig, end ved brugerens tillid til tjenesteudbyderen. Dette er også nævnt i rapporten, og løsningsforslaget med en letgenkendelig URL, hvor godkendte brokere kan få et subdomæne, vurdere vi som en god ide.

4.1.4. Brugeroplevelse

Som beskrevet ovenfor, kan indførelsen af flere aktører gøre det mere uoverskueligt for visse brugere. Dog åbner det samtidig op for differentierede brugsoplevelser, hvor brugerne har en mulighed for at vælge broker/identitetsgarant ud fra, hvilken hun føler giver den bedste brugeroplevelse. For at dette skal fungere i praksis, er det vigtigt at sørge for, at skift af hhv. identitetsgarant og broker kan ske nemt og gnidningsfrit for brugeren (herunder om pseudonymer er ens eller forskellige).

4.1.5. Migrering

Der er mulighed for, at en mere heterogen opbygning kan gøre migrering nemmere, da det kan ske trinvis.

4.1.6. Fremtidssikring

At indføre brokere kan gøre det nemmere at fremtidssikre systemet, da det åbner op for et mere heterogent system, hvor der nemmere kan implementeres nye teknologier og brugsscenarier. Det vil være muligt at introducere p-ABC teknologi på et senere tidspunkt, når denne teknologi bliver teknisk og kommercielt moden, så de brugere, der skulle have lyst, kan vælge en broker og identitetsgarant, der understøtter p-ABC teknologi. Indførelsen af brokere kan også, som beskrevet af RMC-ICG, gøre det nemmere at understøtte interaktion på tværs af EU-grænser (eIDAS forordningen).

Beskrivelsen af brokere i RMC-ICGs rapport er meget overordnet, og det bør undersøges, hvilke konkrete tekniske løsninger der skal til, og hvilke konkrete egenskaber de giver.

4.2. Scenarie 1 – As-is med mindre forbedringer

4.2.1. Beskrivelse

I scenarie 1 videreføres den eksisterende løsning med få mindre ændringer:

Kerneløsningen er en videreførelse af den nuværende løsning med de samme grundlæggende elementer, herunder:

En central lagring af privatnøgler hos leverandøren og 2-faktor-login med kodeord og engangskode (f.eks. nøglekort) til NemID borger og NemID medarbejdersignatur.

Nøglefil til NemID til erhverv (herunder mulighed for decentralt at anvende signatur-serverløsninger).

> *I forbindelse med udbuddet vil det være muligt at kræve visse forbedringer i brugergrænsefladen både for borgere og virksomheder for at opnå øget brugervenlighed (fx kan ønskerne (…) om mere forståeligt sprog imødekommes). (s. 41)*

4.2.2. Privacy

Beskyttelsen af brugerenes privacy vil i scenarie 1 være den samme som i den eksisterende løsning. I forhold til sikkerhed og privacy, vil det ifølge rapporten betyde:

> *Ingen ændring i forhold til nuværende løsning. (s. 50)*

Samt at:

> *(…) Scenarie 1 adskiller sig ikke fra den nuværende løsning i forhold til sikkerhed og privacy, som både nu og fremover kræver en løbende indsats. (s.45)*

Dog forventer vi, at kravene til privatlivsbeskyttelse fra både brugere (se også afsnit om brugeroplevelse), myndigheder og sikkerhedseksperter vil øges med tiden, hvorfor en løsning der yder acceptabel beskyttelse nu, ikke nødvendigvis vil betragtes sådan om nogle år.

De øgede krav kan også fostres af fremkomsten af nye teknologier til privatlivsbeskyttelse, både nogle der allerede eksisterer i dag, og som muligvis vil blive mere udbredt med tiden, men også helt nye.

Et eksempel er anvendelsen af kontekstafhængig information, der i høj grad vil kunne beskytte brugernes privatliv. Det er ikke en del af scenarie 1 (men er en del af scenarie 3). Da brug af kontekstafhængig information kræver, at brugernes certifikater udformes helt anderledes, vil det ikke umiddelbart kunne integreres som en del af scenarie 1 på et senere tidspunkt. Skulle kontekstafhængig information på et tidspunkt blive noget der forventes inden for identitetsløsninger, vil løsninger der ikke understøtter dette til den tid være *relativt* mindre beskyttende over for brugeres privatliv. Mange nyere identitetsløsninger, f.eks. OpenID Connect, Facebook Connect og x.509 v3 certifikater, understøtter kontekstafhængig information, så vi vurderer det sandsynligt, at de fleste fremtidige identitetsløsninger også vil gøre det.

4.2.3. Sikkerhed

Sikkerheden i scenarie 1 vil være den samme som i den nuværende løsning, hvor brugerens sikkerhed er beskyttet af 2-faktor autentifikation med kodeord og nøglekort. Rapporten giver følgende kommentar ift. sikkerhed og privacy for scenarie 1:

> *Ingen ændring i forhold til nuværende løsning. (s. 50)*

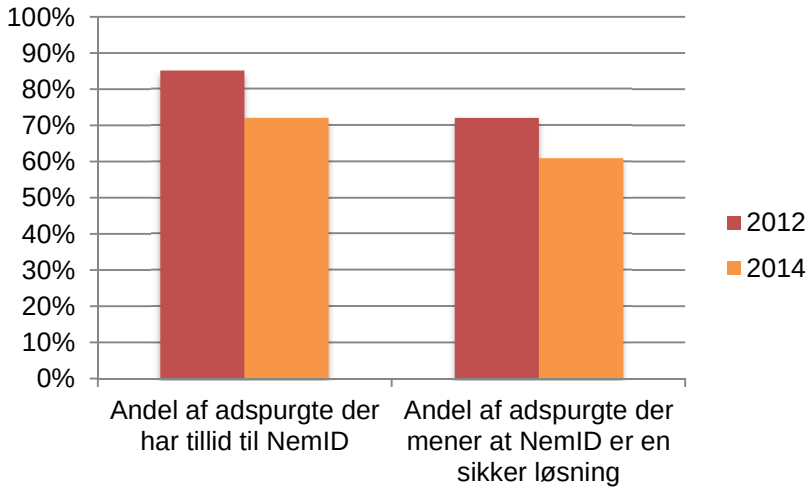
Som i tilfældet med privacy, bør det dog bemærkes, at en sikkerhedsløsning, der vurderes som værende sikker i dag, ikke nødvendigvis vil blive betragtet sådan om nogle år. Dog er det vores indtryk, at tendensen for moderne sikkerhedsløsninger netop er at indføre multifaktor autentifikation, hvilket allerede er en del af NemID. Så det er ikke, som det var tilfældet med privacy, nemt at udpege en teknologi, der vil øge brugernes sikkerhed, og ikke allerede er en del af NemID.

4.2.4. Brugeroplevelse

Ifølge rapporten nyder den nuværende løsning høj tillid blandt brugerne:

> *Årlige brugerundersøgelser af den eksisterende løsning viser en høj grad af tillid til NemID. Det er væsentligt for infrastrukturen, at denne tillid fastholdes. God håndtering af sikkerhed og privacy udgør afgørende elementer i brugernes tillid. (s. 45)*

Det er værd at bemærke, at tilliden til NemID er faldende og er gået fra 85% i 2012 til 72% nu. Andelen der mener, at NemID er en sikker digital adgang er faldet fra 72% til 61% i samme periode:



Figur 1: Uddrag af NemID Imagemåling 2014. Undersøgelsen er baseret på interviews af 1500 danskere over 18 år, der er blevet valgt repræsentativt på køn, alder og geografi.

Undersøgelsen siger ikke noget om, hvorfor tilliden er faldende, men ifølge Digitaliseringsstyrelsen[6], kan det skyldes, at der i de sidste par år har været meget offentlig opmærksomhed om IT-sikkerhed og privacy, hvilket er medvirkende til, at brugere stiller højere krav til deres sikkerhed, deriblandt NemID.

Hvis tendensen fortsætter, vil det være pålagt en ny løsning at skulle opfylde de øgede krav fra brugerne for at opnå samme tillidsgrad. En løsning der viderefører status quo vil ikke nødvendigvis kunne imødekomme disse krav.

F.eks. har nogle brugere udtrykt ønske om, at den nye generation af NemID understøtter kontekstafhængig information. Kontekstafhængig information er brugt i mange moderne teknologier, f.eks. OpenID Connect, Facebook Connect og x.509 v3 certifikater. Efterhånden som disse teknologier bliver mere udbredte, vil nogle brugere opleve fraværet af kontekstafhængig information i NemID som en mangel, hvilket vil give en oplevelse af, at NemID giver en dårligere beskyttelse af deres privatliv end teknologier, der understøtter kontekstafhængig information.

De samme overvejelser gør sig gældende for autentifikationsmetoderne, der anvendes af NemID. Udbredelsen af OpenID Connect og Facebook Connect vil føre til øget brug af single-sign-on, hvor brugeren kan få adgang hos flere tjenesteudbydere ved at logge ind ét sted.

Det er også muligt, at alternative autentifikationsmetoder, f.eks. biometriske metoder, bliver mere udbredt, hvorfor en løsning med brugernavn og kodeord kan komme til at virke omstændelig.

4.2.5. Migrering

Som det også er nævnt i rapporten, mener vi, at hvis den nuværende leverandør fortsætter, vil migreringen kunne foregå relativt smertefrit:

[6] http://www.computerworld.dk/art/232819/danskernes-tillid-til-nemid-dykker-saadan-skal-den-uheldige-tendens-vendes

> *Vurdering af migrering afhænger af, om den nuværende leverandør eller en anden får kontrakten. Hvis den nuværende leverandør får kontrakten, vil migrering give begrænsede udfordringer. Ved skift til ny leverandør vil der være store udfordringer. (s. 50)*

Det bør bemærkes, at hvis en anden leverandør end den nuværende vælges til den nye generation af NemID, og det medfører, at dele af løsningen skal implementeres på ny, er der øget risiko for, at der vil komme sikkerhedshuller i forbindelse med migreringen. I hvor høj grad det er tilfældet afhænger dog af, hvor meget den nye leverandør vælger at ændre på løsningen, og hvilke dele af løsningen det drejer sig om.

4.2.6. Fremtidssikring

Den nuværende løsning har kørt uden store problemer i flere år. Dog er der, som diskuteret i afsnittene 'Privacy', 'Sikkerhed' og 'Brugeroplevelse', risiko for, at løsninger, der virker tilfredsstillende nu, kan blive forældede. I rapporten vurderes det at:

> *Desuden betyder den nuværende forholdsvis "lukkede" arkitektur, at de langsigtede udviklingsmuligheder svækkes. (s. 49)*

Og vi tilføjer, at det kan blive vanskeligt at imødekomme problemerne med forældede teknologier i scenarie 1.

4.2.7. Teknisk modenhed

Den nuværende løsning har kørt uden store problemer i flere år, og al teknologi, der er anvendt, vurderes derfor at være moden.

De problemer, der har været, har været med robustheden af løsningen, idet der har været flere alvorlige nedbrud. Årsagerne har varieret, men har bl.a. været hacking (DoS angreb i april 2013), fejl i forbindelse med opdatering af tredjeparts software (Java opdatering i oktober 2014) og strømsvigt (april 2014). Nogle af disse problemer ville kunne håndteres ved at bruge en mere distribueret arkitektur med flere identitetsudbydere og brokere (se også afsnit 4.1).

Hvis den nuværende løsning fortsætter stort set uændret, er det sandsynligt, at disse problemer vil fortsætte i nogenlunde samme grad og ville – som nu – skulle håndteres løbende.

4.3. Scenarie 2

4.3.1. Beskrivelse

Scenarie 2 dækker de samme funktionelle behov som scenarie 1 (dvs. som i den nuværende løsning) og tilføjer derudover følgende funktioner:

A. Mulighed for 1-faktor-login baseret kun på kodeord.
B. Mulighed for at anvende NemID Borger på erhvervsområdet, f.eks. til personligt ejede virksomheder eller foreninger.
C. Bedre administrative løsninger på erhvervsområdet.

Vi vil i dette afsnit primært diskutere A, da vi ikke har de faglige forudsætninger for at kommentere B og C.

4.3.2. Privacy

Bemærkningerne om beskyttelsen af brugernes privatliv i scenarie 1 gælder også for scenarie 2, og vi har ingen yderligere bemærkninger.

4.3.3. Sikkerhed

I RMC-ICGs rapport bemærkes det, at det i scenarie 2 gælder at:

> *Anvendelse af differentierede sikringsniveauer kræver, at tjenesteudbyder klassificerer data i forhold til de definerede niveauer, så data kun kan tilgås med et passende sikringsniveau. (s. 57)*

Det bør præciseres over for tjenesteudbydere præcis hvilke data, der må være tilgængelige, og hvilke handlinger på vegne af brugeren der er tilladte for hvert sikringsniveau. Det skal sikre mod for lavt sikkerhedsniveau, idet nogle tjenesteudbydere kan have en interesse i at bruge den mest brugervenlige (og mindst sikre) form for autentifikation for at få brugerne hurtigt autentificeret. Det skal også beskytte imod, at en tjenesteudbyder anvender et for højt sikkerhedsniveau, der kan give en dårligere brugeroplevelse end nødvendigt.

I RMC-ICGs rapport foreslås det også, at brugerne selv kan vælge, om de vil bruge 1- eller 2-faktor autentifikation hos en tjenesteudbyder, bare 2-faktor autentifikation anvendes første gang:

> *(…) at der som udgangspunkt vælges et højt niveau (2 faktorer) ved første autentifikation hos en tjenesteudbyder, hvorefter brugeren aktivt kan vælge lavere niveau (1 faktor) ved fremtidige autentifikationer hos samme tjenesteudbyder. (s. 57)*

Her bør det bemærkes, at det forudsætter, at brugerne kan træffe en kvalificeret beslutning om, hvilket sikkerhedsniveau der er tilstrækkeligt, og at valget kun kan træffes i situationer, hvor det lave sikkerhedsniveau er acceptabelt.

I RMC-ICGs rapport bemærkes det, at et phishing-angreb i scenarie 2 vil være mere attraktivt på grund af login baseret kun på kodeord:

> *I takt med at flere tjenesteudbydere vil give adgang til tjenester ved brug af NemID med lavere sikringsniveau, må det antages, at kriminelle i øget omfang vil forsøge at skaffe sig adgang til brugerens akkreditiver til det lavere niveau, fx adgangskode. (s. 57)*

Det bemærkes også, at det vil være nemmere at gennemføre et sådant angreb:

> *Det kan antages, at en fremtidig løsning med understøttelse af differentierede sikringsniveauer vil betyde udbredelse til tjenesteudbydere med mindre fokus på sikkerhed i webapplikationen. Dermed øges risikoen for, at en ondsindet angriber kan tiltvinge sig adgang til en hjemmeside hos en tjenesteudbyder og erstatte NemID klienten med en alternativ klient under angriberens kontrol. (s. 57)*

Vi er enige i begge disse betragtninger.

4.3.4. Brugeroplevelse

Brugeroplevelsen vil blive bedre, hvis 1-faktor login bliver muligt. Det vil give brugerne en velkendt oplevelse, idet funktionaliteten allerede kendes fra netbankernes Kontokig.

For nogle brugere, der går meget op i sikkerhed, kan 1-faktor login med NemID virke mindre sikkert end den nuværende 2-faktor login, og hvis 1-faktor login bliver brugt hos en tjenesteudbyder, hvor en bruger forventer høj sikkerhed, vil det muligvis forringe brugeroplevelsen og gøre brugeren mindre tryg.

Det er uvist i hvor høj grad dette er tilfældet, men da netbankernes Kontokig har været udbredt længe, skulle det kunne danne grundlag for en undersøgelse af, om brugeren oplever, at deres sikkerhed forværres ved brug af 1-faktor login i stedet for 2-faktor login.

4.3.5. Migrering

Indførelse af mulighed for 1-faktor login kræver en separation af autentifikation og signering og:

> *Ved teknisk adskillelse af autentifikation og signering bør identitetsudbyderen implementere og tilbyde et eller flere specifikke login-interfaces til tjenesteudbyderne. SAML2 og/eller OpenID Connect vil være gode kandidater til disse interfaces for autentifikation pga. åbenhed og markedsaccept. (s. 57)*

SAML2 bruges i dag af NemLogin og er som sådan en velkendt løsning i NemID-sammenhæng. OpenID Connect er ikke brugt i det nuværende setup. Det er værd at bemærke, at OpenID Connect er noget enklere for tjenesteudbydere at håndtere end SAML2, både fordi OpenID Connect er mere enkel, men også fordi vi forventer, at OpenID Connect vil være meget udbredt om nogle år, og fordi mange udviklere vil have erfaring med OpenID Connect, når den nye generation af NemID skal rulles ud.

4.3.6. Fremtidssikring

OpenID Connect bygger på OAuth 2.0, der blandt andet kendes fra services fra Google, Facebook og Twitter. Specifikationerne for OpenID Connect blev endeligt udgivet i februar 2014, og flere store firmaer, bl.a. Microsoft, Google, Symantec, PayPal, Deutsche Telekom, Yahoo og Verizon, er repræsenteret i bestyrelsen hos OpenID Connect.

Protokollen betragtes som værende sikker, også til brug i løsninger, der kræver høj sikkerhed. Store spillere på markedet bakker lige nu op om OpenID Connect.

Der er i de senere år sket meget inden for autentifikations-protokoller, og der er nogle risici ved at vælge OpenID Connect.

- En anden protokol end OpenID Connect bliver standard inden næste generation af NemID rulles ud, eller i løbet af dens levetid. Det vil ikke kompromittere løsningen, men det vil mindske gevinsten ved at bruge en bredt anvendt standard.
- Arbejdet på OpenID Connect ophører inden næste generation af NemID rulles ud, eller i løbet af dens levetid, således at specifikationerne ikke længere bliver opdateret. Det vil medføre, at leverandøren ikke kan få hjælpe af det community, der er omkring OpenID Connect til f.eks. at rette sikkerhedshuller.

Vi betragter dog risikoen for begge disse scenarier som værende meget lav, da mange store firmaer bakker op om OpenID Connect. Derfor forventer vi, at OpenID Connect vil blive meget udbredt i den nærmeste fremtid.

4.3.7. Teknisk modenhed

Den eksisterende NemID har været i drift i en årrække uden store problemer, ud over dem vi diskuterede i scenarie 1. De eneste nye elementer er SAML2 eller OpenID Connect, hvis man skulle vælge en af dem til autentifikation.

Vi betragter både SAML2 og OpenID Connect som værende teknisk modne til brug i den nye generation af NemID.

4.4. Scenarie 3

Scenarie 3 indeholder, ud over elementerne fra scenarie 2, følgende:

D. Privacy og kontekstafhængig information

E. Flere login-faktorer

F. Support

Vi vil her diskutere D og E, og ikke F, da vi ikke har faglig indsigt til at diskutere punktet F: Support. Da D og E er forskellige og behandlet forskelligt i rapporten fra RMC-ICG, vil vi også behandle dem hver for sig i de to følgende sektioner

4.4.1. Privacy og kontekstafhængig information – beskrivelse

Muligheden for at afgive kontekstafhængig information ved login kendes allerede fra mere kommercielle løsninger som f.eks. Facebook Connect. Det dækker over, at en tjenesteudbyder kan bede om at få oplyst relevante, og kun relevante oplysninger om brugeren, når denne logger på. På den måde får tjenesteudbyderen troværdige oplysninger om brugeren, samtidig med at brugeren ikke behøver at opgive flere informationer, end tjenesteudbyderen faktisk har brug for.

En form for kontekstafhængig information er tjenesteudbyderspecifikke pseudonymer, hvor tjenesteudbyderen kan genkende brugeren, uden at ydereligere information om brugeren videregives til tjenesteudbyderen. Pseudonymer er behandlet i afsnit 8 i rapporten fra RMC-ICG.

I RMC-ICG rapporten sammenlignes niveau af privacy med den nuværende version af NemID, og RMC-ICG beskriver, at den nuværende NemID-løsning har et højt niveau af privacy.

> *I alle praktiske sammenhænge er den entydige identifikation af brugeren således reelt begrænset til PID/RID eller CPR. Både PID/RID og CPR er globale identifikatorer, der kan sammenkædes på tværs af tjenesteudbydere.*
>
> *I sig selv kan NemID derfor siges at have et højt niveau af privacy. (s.88)*

Vi er uenige i dette: Både brugen af globale identifikatorer (PID i certifikat) som altid bliver videregivet til tjenesteudbyderen, og det at identitetsgaranten (Nets DanID) har mulighed for at spore, hvor brugeren logger ind, gør at løsningen ikke har et højt niveau af privacy. Dette vil kunne forbedres, hvis der indføres kontekstafhængig information.

Derudover vil brugen af kontekstafhængig information kunne give yderligere brugsmæssige forbedringer, blandt andet understøttelse af, at brugeren kan videregive flere oplysninger om sig selv. Det kan være muligt at videregive sin adresse til en webbutik (for forsendelse af varer), det vil være muligt at videregive alder eller aldersinterval uden at videregive sit CPR-nummer. Det vil også være muligt at vise, om man er registeret eller ikke registreret på en bestemt liste, f.eks. ROFUS.

Mulighed for kontekstafhængig information går bedre i tråd med de krav, som vi forventer kommer fra EU (den kommende persondataforordning), herunder "privacy by design".

Teknisk kan kontekstafhængig information implementeres ved enten OpenID Connect, OAuth, SAML etc.; ved brug x509 v.3 certifikater; eller p-ABC teknologi. RMC-ICG peger kun på OpenID Connect og SAML, da disse ses som dem, der vil blive markedsledende:

> *Der findes en række åbne standarder til autentifikation med kontekstafhængig identifikation. Af disse tegner SAML2 og OpenID Connect sig til at blive markedsledende i de kommende år. (s.90)*

Vi er enige i ovenstående, da p-ABC teknologi på trods af de bedre privacy egenskaber p.t ikke er markedsmodent nok. Vi er også enige i, at OpenID Connect formentlig er det interface, private tjenesteudbydere vil foretrække af de to

> *Det må forventes at private tjenesteudbydere fremadrettet vil foretrække OpenID Connect som interface, i takt med at dette interface får større understøttelse (s.90)*

Udfordringer

To udfordringer vi ser ved kontekstafhængig information er:

- Samtykke: Hvis brugeren skal give samtykke til videregivelse af information, vil brugeren se dette som et yderligere forstyrrende skridt, hun skal igennem. Hvordan gøres dette, så det er nemt og samtidigt tydeligt for brugeren, hvem der får hvilken information.
- Vil tjenesteudbydere spørge efter mere information, end de reelt har brug for.

Mange brugere møder allerede samtykke til videregivelse af information ved løsninger som Facebook Connect etc., og der er andre, der har lagt en del arbejde i, hvordan dette samtykke formidles så tydeligt og samtidig smertefrit som muligt over for brugeren. WAYF[7] har lagt meget arbejde i dette, og det er oplagt at trække på nogle af deres erfaringer

Tjenesteudbydere der pr. default spørger efter så mange oplysninger som muligt er et reelt problem. Muligvis vil dette problem løses juridisk via den kommende persondataforordning fra EU. Det er også muligt, at det løses ved at brugerne bliver beviste om, hvilke oplysninger de giver bort, hvis det er tydeligt for dem, når de giver samtykke, og at problemet derfor løser sig ud fra brugernes krav til de tjenesteudbydere, de vælger at benytte.

4.4.2. Privacy og kontekstafhængig information – privacy

Kontekstafhængig information og brugen af tjenesteudbyderspecifikke pseudonymer vil højne graden af privacy meget i forhold til den nuværende løsning, hvis det undgås, at de fleste tjenesteudbydere blot spørger efter fuld information om brugeren. Derudover vil dette minimere brugen af CPR-numre, til bl.a. køn- og aldersverifikation m.v., hvilket også vil højne graden af privacy.

[7] http://wayf.dk/

4.4.3. Privacy og kontekstafhængig information – sikkerhed

En højnelse af privacy vil også give en bedre sikkerhed, da der bliver færre personhenførbare data at håndtere for de forskellige aktører.

4.4.4. Privacy og kontekstafhængig information – brugeroplevelse

Kontekstafhængig information kan give en bedre brugeroplevelse, hvis det bliver muligt at videregive relevant verificerbar information til tjenesteudbydere. Dette kræver dog, at brugeroplevelsen af at give samtykke til videregivelse af data bliver god. Nogle brugere kender allerede delvist til videregivelse af kontekstafhængig information, fra løsninger som f.eks. Facebook Connect.

4.4.5. Privacy og kontekstafhængig information – migrering

Vi har ikke yderligere kommentarer end RMC-ICGs

4.4.6. Privacy og kontekstafhængig information – fremtidssikring

Vi forventer, at mulighed for kontekstafhængig information er med til bedre at fremtidssikre hele løsningen, da det er noget, vi forventer brugerne vil møde andre steder. Derfor vil det også i fremtiden være noget, de forventer af et produkt som næste version af NemID. Hvis det teknisk baserer sig på en internationalt anerkendt standard som OpenID Connect, forventer vi også, at det teknisk vil være fremtidssikret.

4.4.7. Privacy og kontekstafhængig information – teknisk modenhed

Vi vurderer, at både SAML2 og OpenID Connect p.t. er teknisk modne nok til et projekt som dette, og selvom OpenID Connect er en forholdsvis ny protokol, forventer vi ikke dette er et problem, især ikke i løbet af de næste par år. Vi forventer som RMC-ICG, at OpenID Connect vil være den af de to protokoller, der vil blive bedst modtaget af private tjenesteudbydere.

4.4.8. p-ABC teknologi har flere muligheder og vil kunne give et højere niveau af privacy, men vi vurderer, at det ikke p.t. er kommercielt modent nok til et projekt som dette. Det kan ændre sig i løbet af de næste par år, da det virker som om både Microsoft og IBM har fokus på at modne disse teknologier, men det er stadig meget usikkert, om de kan nå et passende niveau af modenhed og kommerciel support inden næste version af NemID. Da der er en del usikkerheder omkring teknologien vil det formentligt også blive dyrere at basere sig på p-ABC teknologi fra starten af projektet. Beskrivelse: Flere login-faktorer

Afsnittet flere login-faktorer omhandler mulighed for andre login-metoder end blot kodeord med nøglekort som anden faktor. Der er i øjeblikket en del fokus på andre måder at logge ind end blot kodeord – også i mere kommercielle løsninger, blandt andet i FIDO Alliance[8], hvor mange store internationale teknologivirksomheder arbejder på fælles løsninger.

Generelt synes vi, det er en god ide med mulighed for flere login-faktorer. Vi er generelt enige i RMC-ICGs vurderinger omkring emnet og har kun få yderligere kommentarer.

[8] https://fidoalliance.org/

Det vil kunne give en bedre brugeroplevelse, hvis der åbnes op for flere login-faktorer, især hvis nogle af disse faktorer er nogen brugerne kan benytte i forbindelse med andre services. Dette kunne være hardware-enheder, som brugerne både kan benytte sammen med næste version af NemID, men samtidigt bruge til at logge ind hos Google. Et eksempel på et sådan produkt er Yubico Security Key, som også er nævnt i rapporten. Dette vil muligvis også gøre det nemmere at få folk til at betale for løsningen, da den kan bruges til andet end NemID.

Brugen af mobiltelefoner, som er nævnt som eksempel af RMC-ICG, kan være problematisk, da man herved ikke er sikker på at få adskilt 2-faktor fra den enhed der bruges til login.

5. Opsummering

Vi er meget enige i de betragtninger, RMC-ICGs rapport præsenterer, og mener, at rapporten adresserer de væsentligste kritikpunkter ved de forskellige scenarier tilfredsstillende. Vi har dog nogle tilføjelser og kommentarer til hvert scenarie:

Da tidshorisonten for den næste generation af NemID er lang (løsningen skal køre indtil 2022), skal løsningen være i stand til at kunne omfavne de krav brugere og tjenesteudbydere måtte komme med i den periode. Det er svært at spå om, præcist hvilke krav, det vil være, men det kan f.eks. imødekommes ved at gøre systemet så fleksibelt så muligt, således at nye teknologier og anvendelser kan implementeres relativt gnidningsfrit. Det kan f.eks. opnås ved at anvende åbne standarder, såsom OpenID Connect. Åbne standarder er under konstant udvikling for at imødekomme fejl og nye krav.

Vi mener ikke, at den nuværende NemID eller en lignende løsning, som i Scenarie 1, vil kunne imødekomme de krav, brugere og tjenesteudbydere måtte komme med. Vi mener heller ikke, at den nuværende løsning, og dermed også en ny identisk løsning, har et tilstrækkeligt højt privacy niveau, fordi løsningen bruger globale identitetsfaktorer, der altid gives videre til tjenesteudbyderen, og fordi identitetsgaranten kan spore, hvor brugeren logger ind.

I Scenarie 2 foreslås det, at 1-faktor login, som det kendes fra netbankernes Kontokig, gøres tilgængeligt for NemID. RMC-ICG mener, at det giver nogle udfordringer for sikkerheden, idet phishing-angreb bliver både nemmere og mere attraktive, men også at det vil give en bedre brugeroplevelse, og at det vil tiltrække flere tjenesteudbydere. Vi er enige i alle disse betragtninger, men mener også, at man meget præcist skal definere, hvilke informationer, der må være tilgængelige på baggrund af et 1-faktor login.

Der skal ske nogle tekniske ændringer, for at 1-faktor login kan gøres muligt, og RMC-ICG foreslår bl.a. at enten SAML2 eller OpenID Connect kan anvendes til autentifikation i den nye løsning. Vi mener her, at OpenID Connect er at foretrække, idet det er en løsning, der anvendes af mange store aktører på markedet, og at den er nem at implementere for tjenesteudbyderne. Kontekstafhængige information, som foreslået i scenarie 3, vil kunne forbedre privatlivsbeskyttelsen, og vi synes derfor det er en god ide. Der er en smule arbejde i at få lavet et setup, hvor det er tydeligt for brugeren, hvilke informationer der gives til hvem og hvornår. Vi vurderer dog dette til at være en forholdsvis lille opgave. Kontekstafhængig information og tjenesteudbyderspecifikke pseudonymer kan enten implementeres ved hjælp af p-ABC teknologi, f.eks. IBM IdentityMixer eller Microsoft U-Prove, men disse teknologier er ikke helt markedsmodne til et projekt som dette. Protokoller som OpenID Connect,

SAML2 og lign. kan også bruges, men man får ikke helt samme privacy garantier, f.eks. kan identitetsgaranten følge med i, hvilke tjenesteudbydere en bruger benytter og hvornår. Dette vil til dels kunne undgås ved at have en broker mellem identitesgarant og tjenesteudbyder.

Brugen af brokere vil komplicere arkitekturen en smule, men ud over de mulige privacy-mæssige gevister bekrevet ovenfor vil der også være andre gevinster. Det kan give et mere robust setup, hvor der er mulighed for failover til en anden broker i tilfælde af nedbrud. Det vil give mulighed for en mere heterogen og dynamisk opbygning, hvor der senere vil kunne indføres nye brugsscenarier og nye protokoller, f.eks. p-ABC baserede protokoller, og hvor muligheden for brug af andre EU eID løsninger vil være nemmere. Forslaget i RMC-ICGs rapport er dog ret ukonkret, og det kræver et mere konkret forslag til arkitekturen, før det er tydeligt, hvilke konkrete fordele/ulemper der vil være.

Vi har følgende konkrete anbefalinger i forhold til de tre scenarier:

- At man ikke fortsætter med den nuværende løsning. Den vil om få år virke forældet, da nye teknologier har funktionalitet, som ikke findes i NemID, og det vil være svært at tilpasse nye krav.
- 1-faktor login er en god idé. Dog skal man meget præcist definere, hvilke data og handlinger, der må være tilgængelige for en bruger, der er logget ind udelukkende med sit kodeord.
- Kontekstafhængig information er en god idé, da det vil give bedre privatlivsbeskyttelse. Derunder foreslår vi også en form for tjenesteudbyderspecifikke pseudonymer. OpenID Connect virker som en moden teknologi til dette. Der findes andre, f.eks. p-ABC, men vi mener ikke, at de er modne til en så omfattende løsning som NemID.
- Hvis man bruger en international standard, som OpenID Connect, vil det også være mere fleksibelt, og ændringer i anvendelser, krav til sikkerhed, nye former for autentifikation, nye platforme osv. vil nemmere kunne integreres. Det er afgørende, da tidshorisonten er så lang.
- Understøttelse af flere login faktorer er også en god idé, der kan gøre løsningen mere fremtidssikret og dynamisk.
- Anvendelse af brokere kan være en god idé. Dog er forslaget ikke tilstrækkeligt konkret i RMC-ICGs rapport, og det er derfor svært at vurdere præcist, hvilke fordele og ulemper, det vil give.