Næste generation af NemID
Fase 2 – Teknisk analyse

Digitaliseringsstyrelsen

Rambøll Management Consulting
Hannemanns Allé 53
DK-2300 Copenhagen S
T: +45 5161 1000
www.ramboll.com

Implement Consulting Group
Strandvejen 56
DK-2900 Hellerup
T: +45 4586 7900
www.implementconsultinggroup.com

28. november 2014

Indholdsfortegnelse

1. Introduktion

1.1 Formål

Denne delrapport har til formål at analysere relevante it-teknologiske løsningsmuligheder for den kommende generation af NemID, både grundlæggende løsningsmodeller i form af tekniske koncepter og løsningsmuligheder for flere af den samlede løsnings delkomponenter. Rapportens analyser vil indgå i det efterfølgende arbejde i Fase 3 vedrørende løsningsscenarier og business case.

Da rapporten er en teknisk analyse, er den skrevet til målgrupper som digitaliseringseksperter, tekniske projektledere og it-arkitekter. Ledelsesresuméet er derimod henvendt til personer med forretningsmæssigt ansvar for de områder, der skal anvende NemID.

1.2 Metodisk tilgang

Første skridt i processen har været at analysere, hvilke forretningsmæssige krav og teknologiske og markedsmæssige forhold der er grundlaget for næste generation af NemID. Denne del af processen er gennemført i Fase 1 af foranalysen.

Derefter har RMC-ICG analyseret en række centrale, funktionelle elementer, der kan have betydning for næste generation af NemID, hvor nogle elementer er en funktion af nye ønsker og behov i forhold til den næste generation af NemID, hvorimod andre er elementer i den eksisterende løsning, der fortsat skal indgå i den næste generation af NemID.

Outputtet fra disse to processer udgør grundlaget for Fase 2, og de beskrives overordnet i afsnit 1.3 og gennemgås detaljeret i kapitel 3.

Herefter skifter fokus fra *hvad*, dvs. fra indholdet i den næste generation af NemID, til *hvordan*, dvs. de konkrete tekniske koncepter for implementeringen af disse elementer i den næste generation af NemID. Her analyseres det, hvordan elementerne fra kapitel 3 it-teknisk kan implementeres. Output fra denne analyse er forskellige løsningskoncepter, der præsenteres og vurderes i kapitel 4.

Slutteligt analyseres en række temaer, der præsenteres i kapitel 5-9, og som omhandler krav til et kommende NemID fra forskellige synsvinkler, herunder i relation til andre systemer som NemLog-in og CPR og andre forhold (håndtering af udlændinge, migrering etc.), der kan have betydning for en kommende løsning.

Samlet set har alle analyserne fokus på at beskrive udfordringer og løsningsmuligheder, samt hvilke afhængigheder der er til andre dele.

Analyserne i Fase 2-rapporten udgør grundlaget for arbejdet i Fase 3 med opstilling og beskrivelse af scenarier for en fremtidig løsning og en efterfølgende analyse af behovsdækning, økonomi, business case, risici og implementeringsmuligheder for disse scenarier.

1.3 Grundlag for Fase 2

Centralt i Fase 2 har været at analysere en bred vifte af løsningsmuligheder, både med udgangspunkt i den eksisterende løsning og de erfaringer, der er høstet i forbindelse med brugen af denne, samt de tilkendegivelser, der har været fra borgere, medarbejdere og andre interessenter siden ibrugtagningen af NemID. Disse tilkendegivelser er bl.a. blevet belyst i denne foranalyses Fase 1. Fokus har været på at åbne op for nye potentielle tekniske elementer i den næste generation af NemID snarere end at indsnævre løsningsfeltet i forhold til det videre arbejde i Fase 3. På baggrund af dette er der identificeret en række centrale elementer, der belyses og analyseres nærmere i kapitel 3. De centrale elementer, der er medtaget i nærværende rapport er følgende:

Brugervenlighed. NemID skal anvendes af flere millioner forskellige brugere, herunder ikke it-kyndige brugere, både som følge af kravene til obligatorisk digitalisering og eventuelt også som

følge af anvendelse i forhold til banker. Det er derfor også en afgørende forudsætning i analysen, at der i den næste generation af NemID generelt skal være fokus på brugervenlighed både i relation til borgere, virksomheder og offentlige myndigheder. Centralt for brugervenlighed i forhold til borgere er, at der skal sikres en større grad af tilgængelighed for de grupper af borgere, hvor særlige hensyn er en nødvendighed i forhold til at sikre, at disse har en reel mulighed for at agere digitalt. For virksomheder og erhvervsorganisationer blev det i Fase 1 fremhævet, at der bør ske en forenkling af oprettelses- og anvendelsesprocessen af NemID i den næste generation af NemID.

Kontinuitet. Det er vigtigt, at der sikres størst mulig kontinuitet og bagudkompatibilitet fra den eksisterende løsning til den næste generation af NemID for at sikre en høj grad af brugervenlighed og omkostningsminimering i forhold til migrering til den næste generation af NemID – både for brugerne og tjenesteudbydere.

Differentierede løsninger til virksomheder og myndigheder. Centralt for næste generation af NemID er at sikre mere differentierede løsninger til virksomheder og myndigheder. Det skyldes, at disse målgrupper i høj grad har differentierede behov i forhold til deres anvendelse af NemID til erhverv; både i forhold til medarbejdernes anvendelse af NemID, de administrative processer og virksomheders og myndigheders rolle som tjenesteudbydere.

It-arkitektur med åbne standarder. Der peges fra mange sider på, at fremtidens NemID bør basere sig på åbne standarder, og infrastrukturen bør være mere fleksibel og åbnes op i flere delelementer, der kan integreres med andre systemer.

Digital autentifikation og signering. En adskillelse af eID og eSignatur vil potentielt bidrage til en mere fleksibel og brugervenlig login-funktionalitet med flere sikringsniveauer, øget privacy samt styrkelse af den juridisk forpligtende elektroniske signering. Samtidig vil denne adskillelse øge konkurrencen bredt i markedet, da flere leverandører vil kunne byde på dele af den samlede NemID-løsning. I høringsprocessen tilkendegav flere interessenter dog en bekymring om, at en adskillelse vil skabe en så stor kompleksitet, at der er en risiko for, at it-svage vil blive koblet af.

Rettighedshåndtering. Flere interessenter fremhævede et ønske om en bedre håndtering af rettigheder og fuldmagt for den næste generation af NemID. Dette gælder både for NemID til borgere og NemID til erhverv.

Fælles indgang til NemID. Der blev blandt nogle af interessenterne udtrykt ønske om en fælles indgang til NemID, fx i form af en profilløsning. Flere af disse fremhævede dog også en betænkelighed ved at lade den private identitet og medarbejderidentiteten smelte sammen i en enkelt profil.

Fleksibilitet. Det er centralt, at den næste generation af NemID er meget fleksibel og over en årrække kan tilpasses som følge af nye funktionelle, teknologiske og sikkerhedsmæssige krav – som en funktion af fx nye klienter, nye login-faktorer, nye protokoller eller ændret trusselsbillede.

Disse elementer gennemgås i kapitel 3 og inkorporeres på forskellig vis i de tekniske koncepter i kapitel 4.

1.4 Proces

Udgangspunktet for analysen har været at kvalificere de elementer, der kan indgå i næste generation af NemID (både eksisterende, der kan videreføres, og nye, der understøtter interessenternes behov), de udviklede tekniske koncepter og de supplerende analyser.

1.4.1 Information og erfaringer

Fællesnævneren for analyserne i Fase 2-rapporten har været at opnå indsigt i, hvad næste generation af NemID skal kunne, hvorfor dette er tilfældet samt hvordan det ud fra et it-teknisk synspunkt kan løses. Derfor baserer Fase 2-rapporten sig bl.a. på relevante parters og interessenters informationer og erfaringer med NemID – både i forhold til den eksisterende løsning, men også i forhold til den næste generation af NemID.

Der er således for de mest kritiske dele blevet gennemført workshops med eksterne eksperter samt eksperter fra højere læreanstalter.

Der er blevet afholdt flere workshops og møder for projektets følgegruppe, der er repræsenteret ved ATP, Uni-C, Danske Regioner, SKAT, KL, Erhvervsstyrelsen og Region Midtjylland (som formand for regionernes egen styregruppe for NemID).

Derudover er der foretaget litteraturstudier og review af internationale konsulentvirksomheders analyser af elektronisk identitetshåndtering. Der har endvidere været en gennemgående tæt dialog med Digitaliseringsstyrelsens egne eksperter, lige så vel som konsulentteamets forretningsmæssige-, tekniske-, juridiske- og sikkerhedsmæssige kendskab til eID og digital signatur naturligvis har været i spil gennem hele processen.

Derudover er ovenstående data blevet yderligere kvalificeret i form af dybdegående interviews, herunder eksperter og specialister inden for privacy fokuserede ABC (Activity Based Credentials) teknologier og NemLog-in arkitekturer. Dette er med henblik på at afdække aspekter, som ovenstående undersøgelser ikke har kunnet afdække. Ligesom der fortsat er løbende dialog med nogle af de interessenter, der deltog i fokusgruppeinterviews i Fase 1.

1.4.2 Afgrænsning

Udgangspunktet for analysen har været at undersøge de områder, der er blevet vurderet som centrale for designet af den nye løsning. Derfor er forhold vedrørende den konkrete implementering og den operationelle drift af løsningen ikke medtaget i analysen. Det betyder derfor, at forhold som fx den konkrete udformning af løsningens front-end ikke er inden for denne analyses scope, ligesom de endelige beslutninger vedrørende login-faktorer og udformningen af præcise servicemål er en del af kravspecificeringen og den kommende dialog med tilbudsgivere.

NemID til erhverv omfatter NemID medarbejdersignatur samt certifikater (VOCES og FOCES), som anvendes ved system-til system integration. Analysen fokuserer på medarbejderens anvendelse, mens system-til system anvendelsen behandles i anden sammenhæng.

1.4.3 Generelle antagelser om løsningsmodellerne

Den nuværende NemID-løsning består af mange dele, hvor hovedparten leveres af Nets DanID, men hvor andre leverandører leverer løsninger til signaturserverfunktionalitet eller andre supplerende løsninger.

I sammenhæng med NemID er der etableret en login-løsning for det offentlige, NemLog-in, som desuden håndterer bl.a. brugeradministration og fuldmagt til borgere og rettigheder til erhverv i relation til offentlige tjenester.

I den nuværende løsning udgøres *basisløsningen* for borgere af NemID med nøglekort, herunder nøglekort i stort format og en telefonisk voice response løsning. Der er supplerende løsninger i form af nøgleviser, og NemID på hardware, hvor certifikat og tilhørende privat nøgle ligger beskyttet på USB krypto token lokalt hos borgeren. For virksomhederne er der to basisløsninger af NemID. Den første løsning er NemID med nøglefil (installeret på computeren) og den anden løsning er NemID med nøglekort (som borgerløsningen). Herudover findes tillige supplerende løsninger som NemID på hardware og NemID signaturserver (afarter af NemID med nøglefil).

I beskrivelsen af fremtidige løsninger for den næste generation af NemID vil der blive arbejdet med en samlet løsning, der består af en eller flere **basisløsninger** og **supplerende løsninger.** Basisløsningen (eller basisløsningerne) skal kunne dække basis behov hos alle brugergrupper, mens de supplerende løsninger skal have større variation og dække særlige behov.

1.5 Rapportens opbygning

Rapporten har følgende opbygning:

Kapitel 1: Ledelsesresumé

Kapitel 2: Kort introduktion til analysens metodik, herunder datagrundlag og databehandling, forudsætningerne for analysen og løsningsmulighederne samt analysens afgrænsninger

Kapitel 3: Præsentation og analyse af mulige elementer i næste generation af NemID

Kapitel 4: Analyse og vurdering af mulige tekniske koncepter

Kapitel 5: Analyse af NemID til erhverv

Kapitel 6: Analyse af forholdet mellem NemLog-in og NemID

Kapitel 7: Analyse af NemID og CPR

Kapitel 8: Analyse af, hvordan udenlandsk eID håndteres

Kapitel 9: Analyse af migreringsmæssige forhold

Kapitel 10: Samlet konklusion, perspektiver til Fase 3 og gennemgang af leverancerne i Fase 2.

1.6 Ordforklaring

I dette afsnit beskrives de væsentligste begreber og termer, som anvendes i rapporten.

- eID og eSignatur anvendes om de to anvendelser af NemID. Begreberne er fra EU's eIDAS-forordning. "Digital signatur" anvendes synonymt med eSignatur
- (Elektronisk, Digital) identitet anvendes om den digitale repræsentation af en entitet (fx person eller virksomhed). Dette svarer til eID
- Autentifikation anvendes om den proces, hvor det sikres, at entiteten er den, vedkommende udgiver sig for at være
- Attributter anvendes om den information, der beskriver den entitet, der har en digital identitet
- Signatur anvendes som udgangspunkt om en avanceret elektronisk signatur som defineret i eIDAS-forordningen (Electronic Identification and Signature) artikel 3 litra 11. Dog anvendes begrebet "digital signatur" som betegnelse for første generation af OCES-infrastrukturen
- For de engelske begreber "Level of assurance" og "Assurance level" anvendes begrebet "Autentitetssikringsniveau" svarende til den danske oversættelse fra eIDAS-forordningen.

Tabel 1: Generelle begreber om nuværende og næste generation af NemID

Begreb	Bruges til/hvorfor
NemID	Bruges både som den nuværende og kommende/næste generation NemID, uanset navnet på en kommende NemID-løsning.
NemID-medarbejdersignatur	Bruges både som den nuværende og kommende NemID-medarbejdersignatur, uanset om en kommende løsning kun omfatter eID eller både eID og eSignatur.
NemID til erhverv	Bruges til de løsninger, der omfatter virksomheder bredt, dvs. MOCES, VOCES, FOCES etc. MOCES= medarbejder-OCES VOCES=virksomhedsOCES FOCES= funktionsOCES OCES= Offentlige certifikater til elektroniske services.
NemID erhverv	Bruges til bankernes løsning.
NemID til borgere NemID Privat	Bruges til de løsninger, der retter sig specifikt til private borgere.

Tabel 2: Tekniske begreber om nuværende og næste generation af NemID

Begreb	Bruges til/hvorfor
Akkreditiver	Repræsentation af en identitet.

Begreb	Bruges til/hvorfor
Login-faktorer	EKSEMPEL: Et akkreditiv/en login-faktor kan være et brugernavn, et brugernavn og password, en PIN-kode, et SmartCard, et token, et fingeraftryk, et pas osv.
Nøglefil	Angiver en af de specifikke løsninger for NemID til erhverv, hvor certifikat og tilhørende private nøgle gemmes i en fil beskyttet med brugerens adgangskode. Nøglefiler kan anvendes til både MOCES, VOCES og FOCES.
Signaturserver	Anvendes som fællesbetegnelse for de specifikke løsninger for NemID til erhverv, hvor certifikat og tilhørende private nøgle er beskyttet på en af kunden valgt kommerciel central løsning. En signaturserver kan både stå hos kunden selv (dvs. en lokal signaturserver) eller hos en betroet tredjepart. Signaturcentralen fra firmaet Signaturgruppen er et eksempel på en signaturserver.
Nøgle	De tal, der står på nøglekortet, og som skal indtastes i forbindelse med anvendelse af nøglekort.
Certifikat	Begrebet er i alle sammenhænge synonym med et X.509v3-certifikat, medmindre andet eksplicit fremgår.
Privat nøgle	Den private nøgle er et centralt element i en public key-infrastruktur og svarer til definitionen af signaturgenereringsdata i eIDAS-forordningen.
Registreringsniveau	Angiver kvaliteten/sikkerheden i registreringsprocessen, hvor 1 angiver lav kvalitet, 4 høj kvalitet. Begreb i STORK2.
Autentifikationsniveau	Angiver sikkerheden ved login (autentifikation). 1 angiver lav sikkerhed, 4 høj sikkerhed (dvs. brug af flere login-faktorer) Begreb i STORK2.
Sikringsniveau Autentitetssikringsniveau	Den samlede vurdering af registreringsniveau og autentifikationsniveau. 1 angiver lav sikkerhed, 4 høj sikkerhed. Assurance Level anvendes i NemLog-in. I STORK2 anvendes ”Quality Authentication Assurance (QAA)”.

Tabel 3: Begreber i mulige tekniske koncepter

Begreb	Forklaring
Identitetsgarant (Registration Authority) + Credential Service Provider eller Certificate Authority	Den organisation, der udsteder akkrediterer og på anmodning (ved login) garanterer, at de fremviste akkreditiver tilhører den entitet, de er udstedt til.
Login-tjeneste	De tjenester, der indestår for brugeres identitet over for tjenesteudbydere og herunder leverer identitetsrelaterede attributter (primære attributter).
Attributtjeneste	De tjenester, der leverer attributter til login-tjenester og tjenesteudbydere.
Identitetsregister (=CPR)	Den funktion/register, der registrerer entiteterne (borgere og medarbejdere).
Verifikation	Den proces, med hvilken en identitetsgarant med tilstrækkelig information sikrer, at en person er entydigt og korrekt identificeret.
Identitetsudbyder (Identity Service Provider)	Et begreb, der både kan dække over identitetsgarant og login-tjeneste.

Tabel 4: Begreber i forbindelse med relevante EU-tiltag

Begreb	Bruger til/hvorfor
eIDAS	EU-forordningen om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner.
Den kommende persondataforordning	Der arbejdes på en persondataforordning i EU. Indholdet er ikke fastlagt i efteråret 2014.
STORK 2	Secure idenTity acrOss boRders linKed 2.0. Et EU-projekt, der har til formål at skabe et fælles elektronisk identifikations- og autentifikationsområde.

2. Ledelsesresumé

2.1 Baggrund

Denne delrapport indgår i en samlet analyse til forberedelse af et beslutningsgrundlag for næste generation af NemID. Den nuværende kontrakt om NemID udløber i november 2017, og dermed skal den samlede løsning genudbydes, så den kan være implementeret, inden kontraktens udløb.

Første delrapport beskriver interessenternes behov, resultatet af en offentlig høring og en brugeranalyse.

Denne delrapport dækker anden fase af analysen til forberedelse af et beslutningsgrundlag forud for næste generation af NemID. Analysen fokuserer på de teknologiske muligheder for en e-identitetsinfrastruktur i den offentlige og private sektor og skal behandle relevante løsningsmodeller.

I tredje fase opstilles og analyseres en række scenarier på grundlag af de to første delrapporter.

I anden fase er der gennemført tekniske analyser på baggrund af erfaringerne med den eksisterende NemID-løsning og de bidrag fra interessenterne, der blev indsamlet i første fase. Analysen er udført af RMC-ICG's konsulenter med indgående viden om områderne med bistand fra Digitaliseringsstyrelsens eksperter. Sideløbende er der gennemført dialog med eksterne tekniske eksperter fra bl.a. de højere læreanstalter og drøftelser med følgegruppen for de offentlige interessenter for NemID.

Centralt i Fase 2 har været at analysere en bred vifte af tekniske løsningsmuligheder med fokus på at åbne op for nye løsninger snarere end at indsnævre løsningsfeltet i forhold til det videre arbejde i Fase 3.

Arbejdet i Fase 2 har haft som forudsætning, at den næste generation af NemID både skal håndtere eID og eSignering. En anden forudsætning er, at løsningen skal tilbyde de nuværende basisløsninger for borgere og virksomheder, der dækker behovet hos den største del af brugerne samt supplerende løsninger, der dækker særlige behov.

2.2 Elementer i næste generation NemID

Erfaringerne med den nuværende løsning og bidrag fra interessenter har ført til opstilling af en række **elementer i næste generation af NemID** forstået som potentielle nye anvendelser i den næste generation af NemID, såsom adskillelse af eID og signering, flere sikringsniveauer (dvs. både 1- og 2-faktor-login), mere differentieret information til tjenesteudbyderne bl.a. af hensyn til privacy, nye login-faktorer samt eventuelt en NemID-profil for borgere og medarbejdere.

Adskillelse af eID og eSignatur er først og fremmest vigtig for at skabe grundlag for at dække behovet for nye funktionaliteter, fx mere brugervenlig login-funktionalitet med fx 1-faktor login, øget privacy samt styrkelse af den juridisk forpligtende elektroniske signering. Denne adskillelse kan tilvejebringes som en funktionel adskillelse i eID og eSignering inden for samme tekniske løsning eller ved en opbygning af separate teknologiske løsninger.

Både brugere og tjenesteudbydere ønsker lettere login til tjenester med 1-faktor login, og enkelte høringssvar efterlyser muligheden for 3-faktor login (**flere sikringsniveauer***)* i forbindelse med autentifikation i næste generation af NemID. Det vil teknisk set være forholdsvist let at implementere i den kommende NemID-løsning. 1-faktor login skal dog vurderes i forhold til den lavere sikkerhed, det indebærer. Flere sikringsniveauer vil i øvrigt kræve klassifikation af data hos den enkelte tjenesteudbyder for at give det fulde udbytte (det er et spørgsmål om, hvilke data der stadig kræver 2-faktor sikkerhed, og hvilke der kan nøjes med 1-faktor). Det kan betyde ekstra omkostninger hos de tjenesteudbydere, der har behov for at understøtte forskellige sikringsniveauer. Det vil dog være muligt at indrette løsningen, så tjenesteudbyderne selv kan vælge, om de vil implementere et lavere sikringsniveau.

Der blev endvidere i Fase 1 tilkendegivet behov for at tilvejebringe mere differentierede login-faktorer (medier som fx nøglekort, USB krypto-token, biometri) til autentifikation, både af hensyn til brugernes valgmuligheder og for på sigt at kunne øge sikkerheden. Ved valg af model for leverance af login-faktorer til autentifikation skal der foretages en vurdering og afvejning af, hvor mange løsninger det offentlige skal levere, og dermed også hvor stort et spillerum andre leverandører har i forhold til at levere supplerende løsninger.

Der er generelt i den offentlige debat og i høringssvarene blevet udtrykt ønske om at tage øget hensyn til beskyttelsen af borgernes privatliv – dvs. **privacy**. Det kan bl.a. gøres ved, at en ny NemID-løsning understøtter målrettet overførsel af data til tjenesteudbydere i login-processen gennem **kontekstafhængig information.** Det giver mulighed for større brugerkontrol og indblik i, hvilke attributter der videregives til tjenesteudbyderen. Anvendelsen af kontekstafhængige attributter vil sikre en større grad af *privacy* for borgere og en større fleksibilitet for især private tjenesteudbyderne i forhold til, hvilke attributter de modtager. På den anden side vil det dog også kræve, at brugerne involveres mere, da de aktivt skal tage stilling til, hvilke informationer der skal videregives til de specifikke tjenesteudbydere. Dog er der ikke behov for aktivt accept fra brugerne i forhold til de offentlige tjenesteudbydere, da de har adgang til de nødvendige informationer om borgere, jf. CPR-loven. Privacy-håndtering vurderes derfor også som et nødvendigt element i den næste generation af NemID for at sikre, at brugerne har tillid til systemet, hvilket kan sikres gennem en høj grad af transparens og privacy. Øget privacy kan imødekommes med forskellige tekniske løsninger.

En NemID-profil skal forstås som en digital afspejling af den enkelte brugers forskellige identiteter og fuldmagter og kan dermed potentielt opfylde ønsket om indblik og kontrol over anvendelsen af ens NemID. Det kan implementeres med en front-end baseret løsning, der kan etableres forholdsvist uafhængigt af de underliggende arkitekturer, hvor kompleksiteten primært vil være afhængig af integrationer til eksterne systemer. Alternativer i form af fx en profil med et NemID pr. person (dvs. én identitet) forudsætter, at der anvendes samme tekniske koncept til borger og erhverv – hvor medarbejdercertifikat erstattes af et NemID for borgere (POCES), der både anvendes i forhold til personens rolle som borger og i forhold til rollen som medarbejder. Implementeringen af dette alternativ vurderes til at være en omfattende og teknisk kompliceret opgave – særligt for tjenesteudbyderne, som i dag bruger NemID til erhverv (MOCES) og i forbindelse med opbygningen af attributhåndtering af virksomhedstilknytning og roller.

Virksomhederne, der p.t. skal administrere medarbejdere i flere forskellige løsninger (både NemID og NemLog-in), og borgere, der ønsker digitale fuldmagtsløsninger svarende til den almindelige anvendelse af fuldmagt, har rejst ønske om en tættere sammenhæng mellem NemID og *fuldmagt og rettigheder*. Der er etableret en løsning til at håndtere fuldmagter for borgere, men som høringssvarene viser, er denne løsning endnu ikke udbredt i tilstrækkelig grad til at dække behovene.

Fuldmagter og rettigheder for erhverv og borgere håndteres to forskellige steder i to forskellige systemer. Når en borgerfuldmagt er uddelegeret til en virksomhed, kan den findes i NemLog-in Brugeradministration og også i nogle af tjenesterne selv, hvilket gør administrationen besværlig for virksomhederne. I forslagene til tekniske koncepter er der også forslag til løsninger på dette i en kommende e-identitetsinfrastruktur. Da håndtering af fuldmagter og rettigheder primært ligger i NemLog-in, og ikke mindst i de enkelte tjenester, er det en selvstændig og større opgave at afdække behov og løsninger, og derfor anbefaler RMC-ICG, at dette løses som et selvstændigt projekt – der favner fuldmagter og rettigheder i den samlede offentlige identitetsinfrastruktur.

2.3 Tekniske koncepter

Med de i afsnit 2.2 definerede elementer som udgangspunkt, har RMC-ICG analyseret det **tekniske koncept** i den nuværende løsning samt markedet for e-identitets og e-signeringsløsninger. Der er identificeret to hovedtyper til at håndtere e-identitet: Løsninger baseret på Public Key Infrastructure (PKI) - som den nuværende NemID-løsning - og andre løsninger baseret på Identity Management Systems (IMS), baseret på dedikerede identifikationsteknologier.

Til eSignering er det alene PKI-baserede løsninger, der er relevante, da anvendelse af PKI-teknologi sikrer uafviselighed dvs. at en afsender ikke senere kan påstå, at en signeret meddelelse, ikke stammer fra ham. Der er opstillet fem tekniske koncepter, der på forskellig måde dækker de behov, der er beskrevet ovenfor, og i forskelligt omfang er bagud kompatible. Koncepterne kan bruges som grundlag for leverandørstrategi og i dialogen med en eventuel privat samarbejdspartner. To af koncepterne (3 og 5) har en funktionel opdeling i identitetsgarant og login-tjeneste, der påvirker NemLog-in's rolle (jf. afsnit 4.3.3 og 4.3.5).

Alle fem koncepter har et praktisk potentiale i forhold til den konkrete udformning af infrastrukturen for den fremtidige generation af NemID.

Koncepterne kan anvendes til både NemID til borgere og NemID til erhverv. Som udgangspunkt antages det, at *samme* koncept anvendes både til NemID til borgere og NemID til erhverv, men en tilgang baseret på *forskellige* teknologiske koncepter eller kombinationer af disse for NemID til borgere og NemID til erhverv kan også være en mulighed.

I alle koncepterne kan lokale certifikater og tilhørende private nøgler understøttes og dermed give bagudkompatibilitet, hvilket primært dækker NemID til erhverv. De tekniske forhold og den samlede kompleksitet i den forbindelse kræver nærmere analyse, ligesom anskaffelsesforholdene skal besluttes.

2.4 Andre analysetemaer

Et hovedfokus for næste generation af **NemID til erhverv** er at udvikle bedre løsninger til virksomheder og myndigheder. Det er RMC-ICG's foreløbige vurdering, at der er behov for en vifte af løsninger til erhvervsområdet, og at virksomheder og myndigheder har brug for at kunne anvende løsninger tilpasset enkelte segmenter i højere grad, end der tilbydes p.t.

Mange virksomheder kan anvende samme løsninger som borgere (der er 274.000 enkeltmandsvirksomheder), hvis tjenesteudbydere på anden vis, fx via attributter, kan få information om, at der er tale om virksomhed. Andre - specielt store virksomheder og myndigheder - har behov for lokale signaturløsninger, eventuelt med brug af signaturservere (jf. Fase 1-rapporten).

For alle virksomhedstyper skal administrationsløsningerne forbedres og differentieres for at skabe bedre forhold for virksomhederne. RMC-ICG vurderer, at dette kan gøres inden for rammerne af den nuværende arkitektur.

For virksomhederne, der administrerer deres medarbejdere både i NemID og NemLog-in, er der behov for at forbedre samspillet mellem **NemID og NemLog-in.** Det er uafhængigt af, hvilket teknisk koncept der vælges som grundlag for næste generation af NemID. Der er en række facetter i forholdet mellem NemID og NemLog-in, der kræver beslutninger i de kommende faser i arbejdet med næste generation af NemID. Det knytter sig fx til rollefordelingen i forhold til autentifikation over for forskellige tjenesteudbydere og i forhold til håndtering af kontekstafhængige informationer samt det tekniske sammenspil mellem de to systemer. Disse udfordringer bør analyseres nærmere i en selvstændig analyse, der omfatter alle elementer af den nationale e-identitetsinfrastruktur.

Der er flere sammenhænge mellem **NemID og henholdsvis CPR og CVR.** CPR anvendes som udgangspunkt for registrering i forbindelse med udstedelsen, brugerne kan anvende CPR-nummeret som bruger-id, og offentlige tjenester kan få oplyst borgeres og udvalgte medarbejderes CPR-numre gennem Digitaliseringsstyrelsens PID/RID-tjeneste. CVR anvendes i forbindelse med den initielle registrering af NemID til erhverv. Det er RMC-ICG's anbefaling, at næste generation af NemID skal designes, så den er robust over for en udvikling med supplering eller erstatning af CPR- og CVR-nummeret. Det kan eksempelvis ske for POCES ved, at CPR-nummer og fremtidige personidentifikatorer, som nu, ikke indlejres i NemID. Ligesom der fortsat bør anvendes et unikt ID nummer tilknyttet NemID og en PID/RID-tjeneste, som kan udvides til at omfatte nye identifikatorer.

En igangværende bredere analyse af virksomhedsområdet, der gennemføres i et samarbejde mellem Digitaliseringsstyrelsen og Erhvervsstyrelsen, afdækker og udbygger forholdet mellem NemID og CVR samt behovene på erhvervsområdet generelt.

Der er fra flere sider rejst ønske om bedre **håndtering af udenlandsk eID** i den næste generation af NemID, og med EU's eIDAS-forordning stilles der krav om gensidig anerkendelse af anmeldte nationale eID fra andre EU-lande. Det betyder, at eID fra andre EU-lande skal kunne anvendes i den danske e-identitetsinfrastruktur gennem en gateway, der skal håndtere autentifikation og validering af udenlandske eID.

Det er RMC-ICG's foreløbige vurdering, at der med den nævnte gateway er fundet en løsning, så Danmark lever op til eIDAS-forordningens krav. Dermed forventes en del af behovet for udlændinges login i danske tjenester at kunne løses.

Der gennemføres parallelt med denne foranalyse en analyse af udenlandske borgers og virksomheders behov i forbindelse med adgang til danske tjenester. Når den er gennemført, skal disse foreløbige konklusioner genvurderes.

2.5 Samlet konklusion og perspektivering

Det er RMC-ICG's **konklusion**, at der for de enkelte dele af næste generation af NemID er en række løsningsmuligheder, som er mere eller mindre attraktive. Der er en række tekniske afhængigheder mellem de enkelte dele og tekniske bindinger for næste generation af NemID.

De mest afgørende afhængigheder og bindinger udspringer af kravene om kontinuitet, bagudkompatibilitet og migrering, hvor hensynet til brugerne og tjenesteudbyderne (både offentlige og private) trækker i retning af en kommende løsning med mange fællestræk med den nuværende løsning. Det er helt centralt, at den kommende løsning gør det muligt at tage højde for nye typer af brugerudstyr og nye funktionelle krav samtidig med, at nye trusler mod sikkerheden skal kunne adresseres løbende herunder også i relation til privacy området.

Fase 1-analysen viste, at der for mange brugere og interessenter er behov for sammenhæng i løsningerne. For disse brugere er det vigtigt, at brugergrænsefladerne usynliggør den underliggende modularitet, som den tekniske analyse viser mulighed for - de juridiske aspekter (herunder ansvarsfordeling) skal dog afklares i denne forbindelse. Særligt erhvervsområdet efterspørger mere differentierede løsninger, som den tekniske analyse peger på løsninger for.

De teknologiske koncepter og andre løsningselementer er dog kun noget af det, der skal indgå i udformningen af løsningsscenarier i Fase 3. Der vil også skulle træffes beslutninger om fx dybden i forhold til opfyldelse af de funktionelle krav og behov (basis vs. supplerende løsninger), bredden i forhold til dækning af brugere (fælles vs. domænespecifikke løsninger) og politiske ønsker i forhold til en potentiel flerleverandørstrategi.

I Fase 3 skal der udvælges de væsentlige mål og funktioner, der skal indgå i de scenarier, der skal opstilles og analyseres i fasen. Hvilke borgerbehov skal dækkes, og hvordan skal virksomheder og myndighedernes behov i forhold til medarbejdernes anvendelse, administration af NemID og som tjenesteudbydere håndteres. Når disse forretningsmæssige rammer er fastlagt, skal de tekniske komponenter, der kan bidrage til at løse de forretningsmæssige behov, analyseres i forhold til deres sikkerhedsmæssige, migreringsmæssige og økonomiske konsekvenser.

3. Elementer i næste generation af NemID

I dette kapitel præsenteres de tiltag, der vurderes som mulige elementer i næste generation af NemID. Elementerne har til formål at understøtte potentielle, nye anvendelser af den fremtidige generation af NemID. De fungerer derfor som grundlag for udarbejdelsen af de tekniske koncepter.

Det nuværende NemID's livscyklus har været udgangspunktet for at indhente viden om potentielle nye anvendelser og centrale krav der er til næste generation af NemID. Elementerne er således udvalgt på baggrund af input fra behovsafklaringen i Fase 1, konsulentteamets tekniske viden, dialog med Digitaliseringsstyrelsen og relevante ekspertgrupper samt de internationale erfaringer, der er relevante for den danske NemID-løsning.

Følgende elementer vurderes som mulige nye anvendelser i den næste generation af NemID og danner udgangspunkt for de tekniske koncepter (jf. kapitel 4):

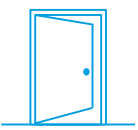
A. Adskillelse af eID og eSignatur
B. Flere sikringsniveauer
C. Kontekstafhængig information
D. Fokus på øget privacy
E. En NemID-profil
F. Fuldmagt og rettigheder.

3.1 Adskillelse af eID og eSignatur

Da arbejdet med implementeringen af en national identitetsinfrastruktur for alvor blev igangsat med overvejelser i sidste halvdel af 1990'erne, var en PKI-baseret løsning det oplagte valg på grund af teknologiens modenhed. OCES blev derfor naturligt baseret på PKI og X.509v3-standarden, og i anvendelse blev det valgt *ikke* at foretage en skarp skelnen mellem eID og eSignatur.

Den tætte binding mellem eID og eSignatur betyder, at begge skal have samme høje sikkerhed. Da autentifikation har langt højere anvendelseshyppighed og anvendes til login i de fleste tjenester, er der behov for mere fleksibilitet for eID, mens eSignatur fortsat skal have ensartet høj sikkerhed. Det gør det relevant at analysere værdien i at lave en større adskillelse af de to begreber og funktionaliteter med henblik på at kunne tilbyde ny og mere fleksibel funktionalitet (som beskrevet i senere afsnit). Høringssvarene i Fase 1 bakker op om dette, hvor der i den forbindelse blev tilkendegivet et stærkt ønske om adskillelse af eID og eSignatur af bl.a. 41concepts, Banedanmark, Dansk Erhverv, Dansk IT, DI ITEK, IT Branchen m.fl.

RMC-ICG vurderer endvidere, at en eventuel adskillelse af autentifikations- og signeringsfunktionaliteten kan være nødvendig for at tilgodese brugernes ønsker om en mere brugervenlig login-funktionalitet med flere sikringsniveauer, øget privacy samt styrkelse af den juridisk forpligtende elektroniske signering. I det følgende vurderes dette element i forhold til den eksisterende løsning, nye potentielle perspektiver og nye mulige løsningsmodeller.



Nye elementer

3.1.1 Den eksisterende løsning

De nuværende login- og signeringsløsninger er implementeret på den samme platform, hvor der ikke skelnes mellem privatnøgle-operationer for eID og eSignatur.

Denne afhængighed betyder, at den samlede løsning er relativt ufleksibel i forhold til muligheder for implementering af ny funktionalitet, som beskrevet i dette kapitel.

3.1.2 Nye perspektiver

De senere år er der i omverden en klar tendens til at adskille autentifikation og signering. Senest er der foretaget en eksplicit skelnen i eIDAS-forordningen[1].

Samtidig er standarder og kommercielle løsninger, som retter sig specifikt mod eID, modnet til et niveau, som matcher rene PKI-baserede løsninger.

Både en *funktionel* adskillelse af login- og signeringsdelen (dvs. hvor begge dele er baseret på PKI-teknologi) og en *teknologisk* adskillelse (dvs. hvor identifikationsdelen ikke er PKI-baseret) vil kunne bidrage til en større fleksibilitet af den samlede løsning og vil give mulighed for at kunne tilbyde flere autentifikationsløsninger (login-faktorer) til brugere. Samtidig vil denne adskillelse muliggøre en nemmere implementering og understøttelse af kontekstafhængig information om brugere, flere sikringsniveauer og vil derfor kunne bidrage til større sikkerhed og privacy.

Endeligt vil der være en simpel model for tildeling af eID-funktionalitet uden eSignatur-funktionalitet for visse brugergrupper, hvis dette ønskes. Det kan eksempelvis være relevant for børn og unge under 15 år.

3.1.3 Potentielle løsninger

Adskillelse af eID og eSignatur kan implementeres mere eller mindre transparent for brugerne.

I den ene ende af skalaen vil brugeren opleve totalt adskilte systemer (infrastrukturer) for eID og eSignatur. De vil skulle anvende forskellige akkreditiver (fx brugerID, adgangskode og nøglekort), som måske endda leveres af forskellige leverandører med forskellige brugervilkår og forskellige registreringsprocedurer. Dette vil potentielt kunne give en stor fleksibilitet, men vil sandsynligvis samtidig have meget stor negativ påvirkning på den samlede brugeroplevelse. RMC-ICG vurderer, at omkostningerne langt vil overgå fordelene ved denne løsning.

I den anden ende af skalaen vil adskillelsen af eID og eSignatur være fuldstændig transparent for brugerne – og styret af teknologien bag brugergrænsefladen. Brugerne vil ikke opleve nogen ændring i forhold til den eksisterende løsning ud over, at de får mulighed for ny funktionalitet (som fx flere autentitetssikringsniveauer, øget privacy etc.). Og de vil kunne anvende samme akkreditiver til både eID og eSignatur.

Hvis eID- og eSignatur-funktionaliteten bliver leveret af forskellige leverandører, men der anvendes samme adgangskode og nøglekort (eller eventuelt andre akkreditiver), er der et særligt forhold omkring sikring af brugerens egenkontrol over de private nøgler til signering, som skal iagttages i det konkrete design af den endelige løsning.

Den teknologiske adskillelse, hvor der ikke nødvendigvis anvendes PKI til autentifikation, vil (på sigt) potentielt kunne åbne endnu flere nye muligheder, som beskrives senere i dette kapitel (jf.

[1] http://certifiedsignature.eu/2014/03/01/eidas-electronic-identification-and-signature-electronic-trust-services-final-draft/

afsnit 3.4), kapitel 4 (jf. koncept 4 og 5) og specifikt i bilag 3 om autentifikationsteknologier og protokoller.

En sådan adskillelse af eID og eSignatur vil naturligt påvirke de tjenesteudbydere, der i den eksisterende løsning har direkte interface til NemID-leverandøren. Omkostningerne ved en omlægning til en større adskillelse af eID og eSignatur vil kunne begrænses (eller afkobles) gennem udvidelse af TU-pakken i den eksisterende løsning. Det skyldes, at det er muligt for en ny leverandør at videreudvikle TU-pakken, da den eksisterende pakke er baseret på Open Source licenser.

Offentlige tjenesteudbydere, som anvender NemLog-in, vil ikke umiddelbart blive påvirket af den teknologiske adskillelse af eID og eSignatur, da autentifikationen ikke sker direkte mod NemID-leverandøren, men derimod mod login-tjenesten.

Det skal derimod ud fra et teknisk synspunkt pointeres, at det skal være muligt i en vilkårlig lang overgangsperiode at tilbyde autentifikation med både ny (ikke PKI-baseret) eID-teknologi – hvis denne besluttes - og den eksisterende PKI-baserede løsning.

Tabel 5: Fordele og ulemper ved adskillelse af eID og eSignatur

Vurderingsparametre	Fordele	Ulemper
Brugervenlighed	Kan implementeres transparent for brugerne med anvendelse af samme akkreditiver.	
Funktionalitet	Giver mulighed for at tilføje ny funktionalitet (fx forskellige sikringsniveauer).	
Sikkerhed	Det vil være muligt at indføre ekstra sikkerhedsparametre for eSignatur alene, uden at det påvirker eID (som har en højere anvendelsesfrekvens). Det kunne som eksempel være en art CVC-kode, som det kendes fra kreditkort, hvis det vurderes at have værdi.	Introduktion af øget kompleksitet, hvis brugere skal sikres egenkontrol over private nøgler til signering og samtidig anvende samme akkreditiver i to teknisk adskilte løsninger for hhv. eID og eSignatur.
Migrering		Tjenesteudbydere, der ikke anvender login-løsninger som NemLog-in, skal eventuelt tilrette den tekniske løsning til håndtering af nye eID-interfaces.
Marked	Følger i højere grad markedstendenser og eIDAS-forordningen.	
Arkitektur	Mulighed for større modularitet og segmentering.	Løsningen bliver mere kompleks.
Økonomi		Tjenesteudbydere med direkte interface til NemID-leverandør kan blive pålagt omkostninger til tilretning.

3.1.4 Konklusion

Analysen viser, at den tætte binding mellem eID og eSignatur giver tekniske begrænsninger, og at en adskillelse af eID og eSignatur i næste generation af NemID giver bedre muligheder for fx flere sikringsniveauer og øget privacy samt styrkelse af den juridisk forpligtende elektroniske signering. Derfor anbefaler RMC-ICG, at man adskiller eID og eSignatur med henblik på at få en mere fleksibel infrastruktur.

Denne adskillelse kan tilvejebringes som en funktionel adskillelse inden for samme tekniske løsning eller ved en opbygning af separate teknologiske løsninger (hvis man vælger at basere NemID på ikke-PKI-teknologier).

RMC-ICG anbefaler, at adskillelsen sker med størst mulig transparens for brugerne med anvendelse af samme login-faktorer, så brugerne ikke skal forholde sig til den underliggende tekniske forskel på login og signering.

RMC-ICG anbefaler, at minimere omkostningerne for tjenesteudbydere, der ikke anvender NemLog-in eller lignende løsninger. Eksempelvis gennem en udvidelse af TU-pakken.

3.2 Flere sikringsniveauer

Ved opbygning af et it-system er det almindelig praksis at klassificere de data, som systemet håndterer, og vælge et sikkerhedsniveau, der som minimum er tilstrækkeligt til beskyttelse af disse data. NemID er en tværgående infrastruktur og skal derfor som minimum understøtte den sikkerhed, der er behov for i de systemer, som kræver høj sikkerhed. Men løsningen kan designes, så brugeren oplever differentieret sikkerhed afhængig af den konkrete anvendelse.

I Fase 1 fremstod det tydeligt, at der i den næste generation af NemID er et ønske om differentierede sikringsniveauer blandt interessenterne, særligt hos private tjenesteudbydere og inden for det offentlige uddannelsesområde. Det er særlig i relation til autentifikation, hvor der er et behov for at kunne autentificere sig på et lavere sikkerhedsniveau end i dag. I det følgende vurderes dette element i forhold til den eksisterende løsning, nye potentielle perspektiver og nye mulige løsningsmodeller.

3.2.1 Den eksisterende løsning

NemID og OCES-standarden (en af hjørnestenene i infrastrukturen i det eksisterende NemID), var oprindeligt designet med henblik på opnåelse af *ét* ensartet og højt sikkerhedsniveau.

Anvendelse af NemID for borgere er i dag baseret på 2-faktor sikkerhed i form af enten brugerID/adgangskode og nøglekort, mens medarbejdersignaturer kan anvende traditionel PKI med kodeordsbeskyttet nøglefil.

Brugerne oplever dog allerede i dag i nogle sammenhænge 1-faktor autentifikation, når de gennem banken anvender kontokig, hvor autentificeringen udelukkende sker gennem 1-faktor i NemID-klienten. Løsningen er implementeret med såkaldte korttidscertifikater og sikring for, at elektroniske underskrifter på transaktioner kun kan foretages, hvis brugeren mindst en gang i sessionen er autentificeret med to faktorer.

I modsætning til bankdelen af den eksisterende løsning dækker OCES-delen både eID og digital signatur-funktionalitet med samme tekniske løsning baseret på centralt placerede X.509-certifikater og tilhørende private nøgler eller lokalt placerede for MOCES, VOCES og FOCES. Denne tætte kobling i OCES-delen betyder, at det ikke *umiddelbart* er muligt at levere et lavere sikkerhedsniveau i den eksisterende løsning, da det vil kræve en tilpasning af den eksisterende infrastruktur, og ændringer i tjenesteudbydernes snitflader.

3.2.2 Nye perspektiver

Gennem de senere år er der dannet en vis international konsensus for opdeling i sikringsniveauer. Eksempelvis definerer STORK2[2] (se bilag 1 for STORK2's opdeling af sikringsniveauer), Kantara[3]

[2] STORK2 står for "Secure idenTity acrOss boRders linKed". STORK2 er et projekt, der har til formål at gøre det lettere for borgere at få adgang til offentlige løsninger online på tværs af EU-medlemsstater. STORK2 er derfor bl.a. med til at skabe fælles regler for opdeling i sikringsniveauer. Se https://www.eid-stork.eu/ for yderligere information om STORK2.

og NIST[4] alle fire niveauer gående fra ingen eller minimal sikkerhed til meget høj sikkerhed for brugers identitet.

eIDAS-forordningen definerer tre niveauer svarende til de tre øverste sikringsniveauer for Kantara og NIST. Disse niveauer bliver dog først defineret mere præcist i en implementeringsakt, der bliver udgangspunktet for et såkaldt "trustframework" for EU. Digitaliseringsstyrelsen arbejder ligeledes på at etablere et dansk trustframework med udgangspunkt i Kantara og eID-forordningen, som kan anvendes i forhold til det kommende udbud for næste generation af NemID.

Den eksisterende NemLog-in tjeneste til de offentlige tjenester, der anvender OIOSAML, er allerede designet og specificeret til håndtering af 4 sikringsniveauer - fra level 1 (lav) til level 4 (høj), og den eksisterende NemID-løsning med 2-faktor autentifikation er indplaceret som level 3.

Under antagelser af, at der i en kommende NemID-løsning benyttes de fire definerede sikringsniveauer (eller en delmængde heraf), vurderer RMC-ICG, at NemLog-in relativt simpelt vil kunne håndtere differentierede niveauer inklusive håndtering i forhold til singlesign-on og step-up, hvor en bruger skal løftes i sikringsniveau, eksempelvis fra 1- til 2-faktor autentifikation.

3.2.3 Potentielle løsninger

Håndtering af differentierende sikringsniveauer ved brug af traditionel PKI bør baseres på *forskellige* certifikater med tilhørende certifikatpolitikker for hvert sikringsniveau. Dette skyldes, at modtager af et brugersigneret token eller elektronisk dokument har certifikatet (og derigennem krav fra certifikatpolitik) som udgangspunkt for vurdering af det aktuelle sikringsniveau. En sådan anvendelse af flere typer certifikater kan gøres transparent for den enkelte bruger, mens modtager af brugersignerede tokens eller elektronisk dokumenter skal kunne skelne de forskellige certifikater.

I de nedenstående afsnit præsenteres en række forskellige potentielle løsninger til håndtering af flere sikringsniveauer. Hvert afsnit afsluttes med en vurdering af løsningens fordele og ulemper.

3.2.3.1 Differentierede registreringsniveauer

Der har ikke været et *udbredt* ønske om flere forskellige registreringsniveauer, dvs. fx STORK2's RP1-RP4 (jf. bilag 1). Dog er det anført, at en udvidelse af NemID til også at omfatte skoleelever bør være baseret på mulighed for registrering lokalt på skoler med lavere registreringsstyrke end for den eksisterende NemID.

Udlændinge, fx ansøgere til optagelse på en dansk uddannelsesinstitution, er en anden gruppe, som kunne have fordel af et lavere registreringsniveau. For EU-borgere vil anvendelse af en lokalt anmeldt eID-ordning (jf. eIDAS-forordningen) dog være en mere korrekt løsning. Det skal dog bemærkes, at kravet om anerkendelse af andre nationale eID systemer (på tværs af EU-lande) er begrænset til registreringsniveau 4 og 3. De lavere registreringsniveauer kan dog accepteres på frivillig basis.

Ved introduktion af differentierede registreringsniveauer er det væsentligt, at tjenesteudbydere og andre tredjeparter i forbindelse med anvendelse har adgang til information om sikringsniveau.

---

[3] Kantara er et initiativ, hvor individer og organisationer deltager med det formål at samarbejde om at imødekomme de udfordringer, der relaterer sig til identitetssystemer, Web 2.0-applikationer og services og web-baserede initiativer. Se https://kantarainitiative.org/ for yderligere information om Kantara.

[4] NIST står for "National Institute of Standards and Technology". NIST er et offentligt amerikansk agentur, der arbejder med at udvikle og anvende teknologi, målinger og standarder. Se http://www.nist.gov/ for yderligere information.

I forbindelse med autentikation og eventuelt ved signering af data skal tjenesteudbyder have mulighed for at formidle det laveste accepterede registreringsniveau (eventuelt i form af et samlet laveste sikringsniveau). Det vil samtidig være oplagt, at de anvendte autentifikationsprotokoller giver tjenesteudbyder information om det faktiske sikringsniveau, da dette kan anvendes til logning og dynamisk forøgelse af krav til sikkerhed i applikationen (fx step-up fra 1-faktor sikkerhed til 2-faktor sikkerhed).

Ved introduktion af flere registreringsniveauer bør det overvejes, om man ønsker at tillade brug af autentifikation med et lavere registreringsniveau og supplerende registrering til at løfte brugere til et højere registreringsniveau. Hvorvidt dette kan implementeres, afhænger naturligvis af de konkrete registreringsniveauer. Et sådan løft af registreringsniveau kan være en hjælp for visse brugere, men kan samtidig øge den samlede kompleksitet af løsningen væsentligt.

Tabel 6: Løsningens fordele og ulemper

Vurderingsparametre	Fordele	Ulemper
Brugervenlighed	Mulighed for simpel registrering, hvis der kun er brug for NemID på lavere niveauer.	Kompleksitet og udfordringer med at forstå differentiering, især hvis der ønskes adgang til en service, der kræver højere registreringsniveau end det aktuelle.
Funktionalitet	Øget funktionalitet og eventuelt understøttelse af brugere, der i den eksisterende løsning ikke kan registreres.	
Sikkerhed		Det kan betyde, at tjenesteudbydere presses til at acceptere lavere registreringsniveauer af markedet. Øget kompleksitet kan øge risiko for fejl.
Migrering	Eksisterende brugere kan umiddelbart indplaceres på et givet sikkerhedsniveau.	Tjenesteudbyder skal tilpasse systemer til håndtering af forskellige registreringsniveauer.
Marked	Eventuelt anvendelig for flere tjenesteudbydere.	Udvanding af den generelle opfattelse af sikkerheden i NemID's brand.
Modulær arkitektur		
Økonomi		Øget kompleksitet og dermed øgede udgifter til udvikling, vedligeholdelse og support i infrastrukturen og for tjenesteudbydere.

3.2.3.2 Differentierede autentifikationsniveauer

Langt hovedparten af den nuværende og fremtidige anvendelse af infrastrukturen er knyttet til autentifikation. Fast anvendelse af et højt sikringsniveau ved autentifikation med minimum to faktorer kan være prohibitivt for udbredelsen og unødvendigt for løsninger, hvor sikkerhedsbehovet er mindre. Det er da også særligt i denne sammenhæng, at der har været et ønske fra brugere samt eksisterende og potentielle tjenesteudbydere om understøttelse af 1-faktor autentificering, da anvendelse af både adgangskode og nøglekort er et unødigt højt sikringsniveau for visse løsninger.

I nogle enkelte høringssvar har der dog også været rejst et ønske om et højere autentifikationsniveau end nu, fx med tre login-faktorer.

Blandt brugerne kan der være meget forskellige holdninger til beskyttelse af personlige data og dermed det ønskede autentifikationsniveau. Nogle ønsker en høj grad af bekvemmelighed, mens andre brugere ønsker det højest mulige sikkerhedsniveau.

Det er muligt at implementere en løsning, hvor både tjenesteudbyder og brugeren inddrages i beslutningen om valg af sikringsniveau. Det vil dog altid være således, at det laveste gensidige

acceptable niveau vil blive valgt. Hvis blot enten tjenesteudbyder eller bruger i et konkret tilfælde således ønsker en 2-faktor autentifikation, vil denne derfor benyttes.

RMC-ICG vurderer, at mange brugere foretrækker en enkel løsning uden mange valgmuligheder, og derfor kan løsningen indrettes i brugergrænsefladen, så det er muligt for disse brugere at anvende løsningen uden valg, mens de brugere, der ønsker valgmuligheden, kan vælge den til.

En række offentlige tjenesteudbydere har typisk ikke klassificeret de personlige data, der præsenteres for brugerne i forskellige niveauer. Der skelnes således udelukkende om brugeren er autentificeret eller ej. Det kan kræve store ressourcer at klassificere data yderligere og tilrette applikation til at understøtte forskellige sikringsniveauer. Grundet NemLog-in's design, hvor flere sikringsniveauer allerede er understøttet, kan indførelsen af differentierede niveauer med meget høj sandsynlighed gennemføres for nye løsninger uden at dette vil påvirke eksisterende løsninger. Dette gælder også, selvom der anvendes single sign-on funktionalitet i NemLog-in.

En løsning med flere sikringsniveauer ved autentifikation kan implementeres med forskellige metoder. Den mest oplagte er med anvendelse af en protokol, hvor tjenesteudbyder indledningsvis via en politik angiver det lavest accepterede sikringsniveau over for identitetsgaranten/login-tjenesten. Dette sker i forbindelse med, at brugeren viderestilles til identitetsgaranten/login-tjenesten, hvor der skal afgives akkreditiver. Herefter autentificerer brugeren sig som minimum på det angivne niveau, hvorefter brugeren sendes tilbage til tjenesteudbyder med angivelse af det faktiske sikringsniveau. Denne metodik er eksempelvis direkte understøttet af SAML.

Tabel 7: Løsningens fordele og ulemper

Vurderingsparametre	Fordele	Ulemper
Brugervenlighed	Mulighed for at anvende NemID uden anvendelse af 2-faktor (nøglekort), hvis det ikke er sikkerhedsmæssigt nødvendigt.	Større kompleksitet og varieret brugeroplevelse.
Funktionalitet	Øget funktionalitet	
Sikkerhed		Tjenesteudbydere kan af markedet føle sig presset til at anvende et lavt sikringsniveau. En tjenesteudbyder kan dog ikke udstille fortrolig information, hvis der er autentificeret med et sikkerhedsniveau, der ikke modsvarer fortrolighedsniveauet. Øget kompleksitet kan desuden øge risiko for fejl.
Migrering	Kan implementeres med bagudkompatibilitet.	
Modulær arkitektur		
Økonomi	Væsentlig øget anvendelse kan medfinansiere øget kompleksitet.	Øget kompleksitet og dermed øget udgifter til udvikling, vedligehold og support i infrastrukturen og for tjenesteudbydere.

3.2.3.3 Differentierede signaturniveauer

Som for autentifikation kan der være differentierede sikringsniveauer for signeringsfunktionalitet. I Fase 1 er der kun fremkommet enkelte ønsker om understøttelse af differentierede sikringsniveauer for elektroniske signaturer.

Hvis signering skal understøttes for flere forskellige registreringsniveauer, er den oplagte løsning at anvende certifikater under forskellige certifikatpolitikker. Det er almindeligt (og krævet i OCES-politikkerne), at der indsættes en reference til certifikatpolitikken i certifikater. Erfaringsmæssigt vurderes det dog, at meget få tjenesteudbydere i Danmark med understøttelse af signeringsfacilitet

håndterer politik-felter i certifikater. Da OCES-standarderne er baseret på et fælles højt registreringsniveau, er tjenesteudbyderens accept af en signatur normalt baseret på verifikation af certifikatudstederen. For at minimere risikoen for sikkerhedsfejl vil det derfor være naturligt at certifikater med forskellige registreringsniveauer bliver udstedt i adskilte certifikathierarkier. Dette øger kompleksiteten for certifikatudbyder (CA).

Der er en række udfordringer i forbindelse med introduktionen af flere sikringsniveauer for elektroniske signaturer:

A. Der vil være behov for, at flere forskellige certifikater udstedes under forskellige certifikatpolitikker, så tredjepart efterfølgende kan skelne signaturer under forskellige sikringsniveauer i vurderingen af sikkerheden for en konkret underskrift. Disse politikker skal specificeres og vedligeholdes.
B. I den analoge verden findes der ikke flere forskellige underskrifter med forskellige sikringsniveauer, og det er derfor ikke givet, hvordan en differentieret løsning skal kommunikeres til slutbrugeren. Dette gælder i særlig grad, hvis man vælger at implementere løsninger med lavere sikkerhed end nuværende OCES CP. Differentierede sikringsniveauer i forhold til signaturer anvendes dog i den digitale verden, hvor eIDAS-forordningen sondrer mellem kvalificerede signaturer og andre avancerede elektroniske signaturer og deres respektive anvendelsesområder.
C. Signering anvendes typisk med langt mindre frekvens end autentifikation. Barrieren ved at anvende flere login-faktorer er dermed mindre og tilmed eventuelt ønskelig, da det således tydeligere fremgår, at der foretages en bindende transaktion.

RMC-ICG vurderer, at den eksisterende NemID-løsning kan indplaceres på STORK2 QAA3.

Tabel 8: Løsningens fordele og ulemper

Vurderingsparametre	Fordele	Ulemper
Brugervenlighed	Mulighed for eSignatur uden anvendelse af 2-faktor.	Større kompleksitet og varieret brugeroplevelse. Brugere skal skelne og forstå forskellige niveauer af signaturer.
Funktionalitet	Øget funktionalitet.	Øget kompleksitet.
Sikkerhed	Mulighed for at have højrisiko certifikater, der kun anvendes i særlige tilfælde og mulighed for at begrænse risiko med lav-niveau-certifikater.	Øget kompleksitet, men øget risiko for fejl eksempelvis accept af lavniveau signatur, hvor der kræves højniveau signatur.
Migrering		
Marked		Ikke umiddelbart efterspurgt af markedet.
Modulær arkitektur		
Økonomi		Øget omkostninger grundet øget kompleksitet og flere CP'er.

3.2.4 Konklusion

Analysen viser en række fordele ved at understøtte flere sikringsniveauer i forbindelse med autentifikation i næste generation af NemID.

RMC-ICG vurderer, at den kommende NemID-løsning skal kunne leve op til betingelserne for at blive anmeldt til Kommissionen på level "Substantial" i eIDAS forordningen (svarende til STORK QAA3 niveau).

RMC-ICG vurderer endvidere, at behovet for differentierede registreringsniveauer er begrænsede og samtidig vil øge kompleksiteten af den samlede infrastruktur. Endvidere vurderer RMC-ICG, at det eksisterende OCES-registreringsniveau som udgangspunkt er tilstrækkeligt, men at en kommende løsning bør være designet til at kunne håndtere løft i registreringsniveau i takt med at

trusselsbilledet ændres, fx hvis der sker øget forekomst af identitetstyveri i forbindelse med registrering.

RMC-ICG vurderer, at understøttelse af differentierede autentifikationsniveauer vil have stor værdi i en lang række sammenhænge. Særligt vil det kunne dække behov i det private marked, der derved kan bidrage med en større andel af finansieringen. Løsningen bør implementeres med fokus på brugerinddragelse og brugervenlighed. Løsningen vil i øvrigt kræve klassifikation af data hos den enkelte tjenesteudbyder for at give det fulde udbytte.

RMC-ICG anbefaler endvidere, at en kommende løsning implementeres med signaturfunktionalitet med ét fast niveau svarende til STORK QAA3-niveau, men at løsningen er forberedt til at kunne migreres til at understøtte QAA4 i takt med, at trusselsbilledet ændres.

Som konsekvens af at have flere autentifikationsniveauer, men et signeringsniveau, bør der ske en adskillelse af eID og eSignatur. Da understøttelse af flere sikringsniveauer i det nuværende tekniske koncept kun vil være muligt ved ændringer i den bagvedliggende infrastruktur, vil behovet indgå som input i arbejdet med nye tekniske koncepter.

3.3 Kontekstafhængig information om brugerne

I den analoge verden er personer identificerede ved forskellige attributter i forskellige sammenhænge. Ved betjening i forhold til det offentlige er man ofte identificeret med CPR-nummer, mens man fx i forhold til indkøb af cigaretter i en kiosk er identificeret som en person over eller under en vis alder.

I den digitale verden kan der være et tilsvarende behov for at anvende forskellige attributter til at identificere brugere i en given kontekst.

Fase 1 har vist et sådant behov for at identificere brugere over for både de offentlige og private tjenester ved hjælp af en række varierede attributter som fx:

A. CPR i forhold til offentlige myndigheder
B. Alder over 18 år ved køb af visse tjenester (fx online gambling)
C. Navn og adresse ved almindelig nethandel
D. Tjenesteudbyderspecifik identifikation (TU specifik PID), hvis bruger blot skal kunne genkendes på tværs af sessioner hos tjenesteudbyderen.

Der blev desuden i Fase 1 udtrykt ønske om, at attributter, der videregives til tjenesteudbyderen, skal kunne vises for brugeren, så brugeren kan afgøre, hvad der skal videregives. Det er RMC-ICG's vurdering, at det skal ske ud fra princippet om, at brugeren skal have kontrol over, hvilke attributter der videregives (privacy by default). Dette princip kan i visse sammenhænge dog naturligvis afviges. Eksempelvis ved autentifikation mod offentlige tjenester, der med hjemmel i CPR-loven har adgang til de nødvendige informationer om borgeren ved CPR-nummer.

3.3.1 Den eksisterende løsning

I den eksisterende NemID login-løsning sendes et signeret brugersigneret XMLDSig-dokument til tjenesteudbydere (herunder NemLog-in), hvor identifikationen er baseret på data i brugerens X.509v3 OCES-certifikat. Således er de eneste data, som tjenesteudbyderen umiddelbart har adgang til, brugerens PID-nummer og eventuelt navn og e-mail-adresse på udstedelsestidspunktet for certifikatet. For offentlige tjenester kan CPR-nummer efterfølgende bestemmes via Digitaliseringsstyrelsens PID-tjeneste.

Den eksisterende løsning er således ufleksibel i forhold til at levere identifikationsdata om brugeren, hvilket særligt rammer private tjenesteudbydere.

3.3.2 Nye perspektiver

Understøttelse af kontekstafhængig information om brugerne vil åbne for en række fordele for både slutbrugere og tjenesteudbydere.

Brugeren har mulighed for en langt større transparens i flow af personlige identifikationsdata med en ensartet grænseflade for accept af videregivelse. Samtidig vil der åbnes for større privatlivsbeskyttelse.

Tjenesteudbyderen har mulighed for at identificere brugere ud fra mere relevante data end i den eksisterende løsning. Det åbner for helt nye muligheder, som ikke lader sig løse i dag. Eksempelvis vil netbutikker få en simpel mulighed for at få en verificeret adresse for en kunde, inden der udsendes varer med høj værdi.

Disse fordele vil primært være relevante i forbindelse med anvendelse i det private marked, men en række offentlige tjenester kan ligeledes benytte teknologien. Eksempelvis kan man forestille sig en række kommunale løsninger, hvor der ved almindelig anvendelse udelukkende er krav om, at brugeren er bosiddende i kommunen.

Det vurderes, at kontekstafhængig information om brugerne vil være en væsentlig forbedring af NemID-infrastrukturen.

3.3.3 Potentielle løsninger

Da den eksisterende løsning baseret på X.509-certifikater og XMLDSig tokens er ufleksibel i forhold til kontekstafhængig information, vil implementering heraf stille krav om ændringer.

Det kan ske inden for rammerne af X.509-standarderne, ved fx at hver bruger har flere certifikater med hver sit sæt af attributter eller ved at anvende korttidscertifikater.

Andre muligheder er at anvende en SAML- eller OpenID Connect-baseret login eller at anvende nye åbne privacy "Attribute Based Credentials"-teknologier som U-Prove fra Microsoft eller Identity Mixer fra IBM. Med disse vil det være muligt at videregive relevante attributter til tjenesteudbyderen og ingen andre. Dette kunne eksempelvis være navn og adresse, men det kan også være mere anonyme attributter som eksempelvis alder og køn eller et tjenesteudbyder-specifikt identitetsnummer for brugeren.

For beskrivelse og vurdering af ABC-teknologier, herunder privacy-fokuserede ABC-teknologier og protokoller, henvises der til bilag 3, og der henvises i øvrigt til afsnit 3.4 om privacy.

Hvis der vælges en løsning med kontekstafhængig information, skal det overvejes, om brugeren i løsningen skal have kontrol over, hvilke attributter der videregives til tjenesteudbyderen (med udgangspunkt i tjenesteudbyderens policy). Ønsket om åbenhed og gennemsigtighed taler for at give brugerne denne mulighed, mens erfaringerne med at udvikle brugervenlige løsninger viser, at denne type valg af de fleste opleves som forvirrende og irrelevant. Brugerkontrol kan implementeres for udvalgte løsninger, når det ønskes, og er derfor ikke noget, der nødvendigvis skal vælges i foranalysen.

Uanset hvilken teknologi der vælges til implementering af kontekstafhængig information om brugeren ved autentifikation, vil det være baseret på en teknisk adskillelse af eID og eSignatur.

3.3.4 Konklusion

Der er flere høringssvar, der rejser ønsket om kontekstafhængig information. Der er desuden tæt sammenhæng mellem kontekstafhængig information og privacy (jf. næste afsnit).

Da det ikke er muligt at levere mere kontekstafhængig information i den nuværende løsning, vil behovet herfor indgå som input i arbejdet med nye tekniske koncepter.

RMC-ICG vurderer, at kontekstafhængig identifikation kan bidrage til beskyttelse af brugernes privacy selv ved en bredere anvendelse af NemID.

Kontekstafhængig identifikation vil have værdi for private tjenesteudbydere, hvor de kan identificere brugerne ved andet end PID. Kontekstafhængig identifikation vil desuden have værdi for visse offentlige tjenester, der ikke har behov for at identificere brugerne på CPR-niveau. Dette kan potentielt være mere relevant i fremtiden. På nuværende tidspunkt anvender de fleste offentlige tjenester CPR.

RMC-ICG anbefaler, at en løsning med kontekstafhængig identifikation implementeres, så brugeren inddrages, når det er relevant, men ikke involveres, når fx CPR videregives til en offentlig myndighed i de tilfælde, hvor det er nødvendigt for servicering af brugeren.

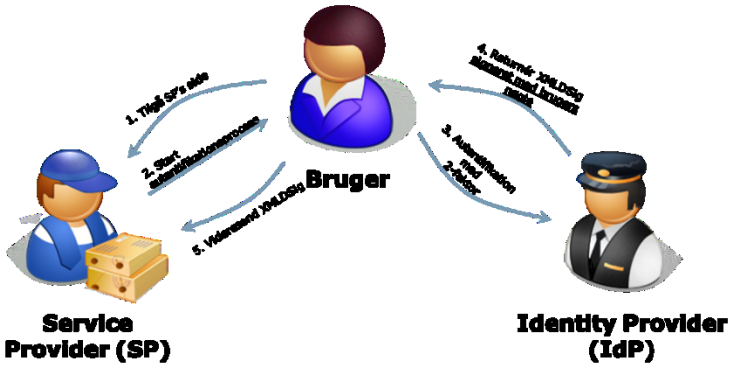
3.4 Fokus på øget privacy

Transparens og privatlivsbeskyttelse vurderes som væsentlige elementer i den samlede tillid til en ny infrastruktur for næste generation af NemID. Hvis brugerne er usikre på, hvorvidt registrerede data behandles med respekt for privatliv, eller hvis data rent faktisk ikke behandles inden for rimelige rammer, kan det have samme skadelige effekter, som hvis systemet ikke har tilstrækkelig it-sikkerhed. Dette øgede fokus på privacy blev endvidere vægtet i høringssvarene i Fase 1. Desuden indgår krav om privacy til interoperabilitetsrammen i eIDAS-forordningen og forventes at indgå i en kommende persondataforordning.

3.4.1 Den eksisterende løsning

I den eksisterende NemID-løsning (dvs. OCES-delen, ikke bank-delen) er autentifikation baseret på anvendelsen af tokens underskrevet af brugeren selv og sendt til tjenesteudbyder. Formatet for det anvendte token er et digitalt XMLDSig-dokument. Tjenesteudbyder identificerer efterfølgende brugeren ved brug af data, der findes i det tilhørende certifikat. Certifikatet indeholder et entydigt identifikationsnummer, PID og CVR+RID for hhv. borger og medarbejder og eventuelt navn og e-mail-adresse.

Figur 1: Sammenspillet mellem tjeneste, bruger og identitetsudbyder ved autentifikation



For offentlige tjenester kan PID efterfølgende konverteres til CPR via Digitaliseringsstyrelsens PID-tjeneste. Tilsvarende gælder for CVR+RID, hvis CPR er registreret for den konkrete medarbejdersignatur.

Konsekvensen er en *alt-eller-intet* situation, hvor offentlige tjenesteudbydere i praksis enten får et PID/CVR+RID, som giver meget få informationer til den videre identifikation i tjenesteudbyderens systemer, eller via CPR-opslag/CPR-validering får kendskab til CPR-data, der i mange sammenhænge, især for private tjenesteudbydere, ikke er ønskelig og/eller nødvendig.

For borgere opbevarer NemID-leverandøren udelukkende data, som er nødvendige for at opretholde autentifikations- og signeringstjenesterne.

Desuden er der for brugeren mulighed for via selvbetjening at slå udvidet logning til (opt-in), så der gemmes information om, hvilken tjenesteudbyder NemID har været anvendt mod.

I den eksisterende kontrakt er NemID-leverandøren forpligtet til at have en ”Privacy ansvarlig”-funktion. NemID-leverandøren har offentliggjort en privatlivspolitik, der er baseret på OECD’s Privacy Policy Generator.

3.4.2 Nye perspektiver

I de senere år er der kommet et større fokus på opsamling, behandling og videregivelse af data. Dette er blandt andet drevet af nye trends som Cloud og Big Data, tjenester, der indsamler store

mængder data som Facebook og Google, og ikke mindst offentlig opmærksomhed omkring Wikileaks, Snowden/NSA m.m.

Disse trends og hændelser påvirker naturligvis diskussionen om de kommende eID- og eSignatur-infrastrukturer, hvor data om brugere skal håndteres af hensyn til sikring af tjenesterne. Samtidig er der mulighed for, at disse infrastrukturer kan understøtte privacy-fremmende teknologier og privacy principper som eksempelvis privacy-by-design og privacy-by-default.

I begyndelsen af dette årtusind blev der på internationalt plan erkendt et behov for standardiseret elektronisk identitetshåndtering med fokus på brugercentrering, privacy og en åben eID-infrastruktur. I 2011 blev en række af tankerne direkte inkluderet i den amerikanske regerings strategi for elektronisk identifikation "National Strategy for Trusted Identities in Cyberspace"[5]. De grundlæggende ideer har ligeledes influeret Storbritanniens nye eID-initiativ, "Digital Assurance Programme"[6].

Hvor PKI tidligere i mange sammenhænge blev opfattet som en generel løsning til både eID og eSignatur, fokuseres der nu mere på at opdele disse. Dette giver en særlig øget fleksibilitet i forhold til eID med mulighed for understøttelse af privacy-fremmende teknologier. En række initiativer giver tjenesteudbydere mulighed for at identificere brugere udelukkende med attributter, der er nødvendige i en given kontekst.

eIDAS-forordningen, artikel 5, omhandler specifikt privacy med henvisning til direktiv 95/46/EF og krav om at lette gennemførelse af princippet om ”privacy-by-design” som et specifikt kriterium for interoperabilitetsrammen i artikel 12. Derudover er der rapporteringskrav til tilsynsmyndigheden, bl.a. ved brud på beskyttelse af persondata i artikel 18.

Endvidere ses det, at der i takt med den generelle digitalisering er internationale trends, der peger mod et øget fokus på og regulering af privatlivsbeskyttelse. Dette afspejles eksempelvis i forslag til den kommende EU-forordning om persondatabeskyttelse.

Der er derfor en række juridiske forhold, der gør, at privacy i høj grad skal inkorporeres i næste generation af NemID.

3.4.3 Potentielle løsninger

Som beskrevet i afsnit 3.3, vil kontekstafhængig identifikation kunne bidrage til øget privatlivsbeskyttelse, særligt i forhold til det private marked. Dette vil naturligvis kræve, at tjenesteudbyderne udelukkende får adgang til de attributter, som er nødvendige for at kunne levere en tjeneste for brugeren.

Visse løsninger kan desuden nøjes med betinget identifikation. Som eksempel kan nævnes Den Blå Avis, der i dag giver brugere mulighed for at lave en såkaldt NemID-validering. Denne validering består i et login med NemID efter, at brugere har autentificeret sig med Den Blå Avis' lokale bruger-id/kodeord. Den Blå Avis gemmer udelukkende PID, der anvendes i forbindelse med anmeldelse af svindelsager til politiet og efterfølgende blokering af efterfølgende forsøg på NemID-valideringer. Det er således udelukkende i forbindelse med svindel, at brugerne identificeres på

[5] http://www.nist.gov/nstic

[6] http://www.digitalassurance.com/

CPR-niveau, og der sker identifikation hos politiet på baggrund af anmeldelsen. Ifølge Den Blå Avis har indførslen af NemID-validering bidraget til, at svindel er reduceret med 12 pct.[7].

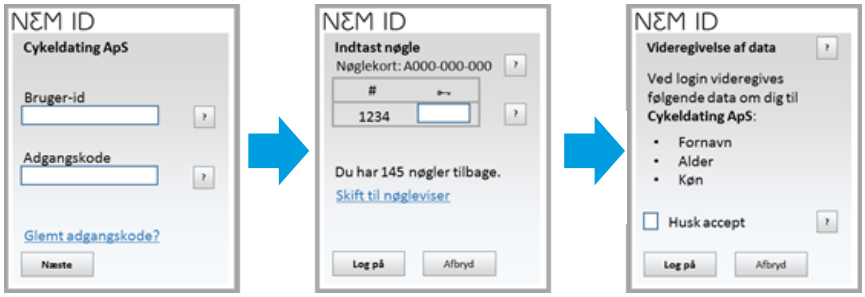
RMC-ICG vurderer, at anvendelse af attributter til identifikation kan understøtte en større grad af privacy og samtidig give en større fleksibilitet for tjenesteudbyderne, der kan nøjes med at modtage nødvendige og relevante attributter for en given bruger.

Hvis teknologien er til stede, vil det samtidig være muligt at gennemføre lovgivning, der støtter øget privacy. Man kunne eksempelvis forestille sig, at en spillelovgivning ikke stiller krav om, at leverandør af online-gambling skal identificere brugere på CPR-nummer, men i stedet skal sikre sig, at brugere er over 18 år og ikke står på den såkaldte ROFUS-liste, samt at det er muligt at identificere brugeren senere, hvis der konstateres ulovligheder i forbindelse med spil (fx hvidvask).

Dette vil dog kræve, at der sker en teknologisk adskillelse af eID og eSignatur, så der kan videreformidles et mere fleksibelt token til tjenesteudbyderen i forbindelse med et login i stedet for et certifikat med op til tre års løbetid. Alternativt kan udfordringen med privacy løses ved at indlægge en obligatorisk login-tjeneste i infrastrukturen.

Det er væsentligt for løsningen, at videregivelse af data er brugerkontrolleret og transparent. Dette kan ske ved, at brugeren giver sin accept til videregivelse af attributter i forbindelse med første login hos en given privat tjenesteudbyder.

Figur 2: Illustration af brugers accept vedrørende videregivelse af attributter ved første login



Der findes en række teknologier, der understøtter attributbaserede akkreditiver (Attribute Based Credentials). Som væsentlige eksempler kan nævnes:

- Simpel SAML 2.0 (som implementeret i NemLog-in)
- OpenID Connect
- U-Prove (Microsoft)
- Identity Mixer (IBM).

Af disse vurderer RMC-ICG, at de "klassiske" ABC-teknologier, SAML 2.0 og OpenID Connect er modne til at blive anvendt, når en ny løsning skal implementeres, mens privacy-fokuserede ABC-teknologier, U-Prove og Identity Mixer stadig er nye teknologier uden bred markedsaccept på nuværende tidspunkt.

Der er dog åbne spørgsmål i forhold til anvendelse af brugerkontrolleret videregivelse af attributter til understøttelse af øget privacy:

[7] http://sikkerhed.dba.dk/hvad-goer-dba

- Kan løsningen designes, så brugerne forstår konceptet (ikke blot ”click-to-continue”)?
- Er der eller vil der vise sig at være et reelt markedsbehov for løsninger baseret på privacy-fokuserede ABC som U-Prove og Identity Mixer som kan sikre anonymitet, og hvor identitetsudbyderen ikke får information om, hvilken tjenesteudbyder brugeren autentificerer sig overfor?
- Vil tjenesteudbydere generelt være *privacy-aware* eller anmode om flest mulige attributter? Kan/skal det styres?
- Teknologivalg- og modenhed på tværs af platforme (pc, mobil, tv etc.), OS (Windows, Android etc.) og applikationer (browsere, native apps etc.).

Tabel 9: Løsningens fordele og ulemper

Vurderingsparametre	Fordele	Ulemper
Brugervenlighed	Øget transparens ved videregivelse af data.	Risiko for, at brugere generelt ikke forstår eller finder ABC relevant.
Funktionalitet	Direkte (brugerkontrolleret) adgang til nødvendige relevante identitetsattributter for tjenesteudbyder.	Risiko for, at løsningen misbruges til at kræve irrelevante identitetsattributter af brugerne.
Sikkerhed	Mulighed for generel forøgelse af privacy for den enkelte bruger. Mulighed for at begrænse anvendelsen af cachede PID/CPR-data hos diverse tjenesteudbydere.	Risiko for nye sikkerhedsfejl i forbindelse med øget kompleksitet.
Migrering	Kan implementeres parallelt med og uafhængigt af den eksisterende løsning, således at eksisterende løsninger ikke påvirkes.	Vil typisk være relevant for nye løsninger, da eksisterende tjenesteudbydere allerede har identificeret brugeren på PID/CPR – medmindre identifikation ønskes/kræves på ny af brugeren eller tjenesteudbyderen
Marked	Efterspurgt i en række offentlige løsninger i Fase 1. Desuden efterspurgt af FDIH i høringssvar.	
Modulær arkitektur	Kan implementeres med understøttelse af flere identitetsudbydere og flere sikringsniveauer. Kan desuden naturligt indgå i STORK2-setup.	
Økonomi	Potentiale for mindre svindel ved nethandel. Bredere anvendelse af NemID og dermed potentielt flere parter til finansiering. Kan baseres på industri-standard-API’er (fx OpenID Connect) med mulighed for billigere implementering for identitetsudbydere og tjenesteudbydere.	Kan give øgede implementerings- og driftsudgifter for NemID-leverandøren og eventuelt øgede supportudgifter. Dette gælder særligt i forbindelse med migrering af eksisterende løsninger.

3.4.4 Konklusion

Der er generelt et øget fokus på privacy, og det indgår som nævnt også som et krav i eIDAS-forordningen.

RMC-ICG anbefaler derfor, at privacy-håndtering tænkes ind i løsningen for næste generation af NemID – eksempelvis ved at understøtte kontekstafhængig information om brugerne.

3.5 En NemID-profil

I forbindelse med brugerundersøgelsen gennemført i Fase 1 har nogle brugere ytret ønske om én samlet indgang til NemID, med én profil for borgere og medarbejdere.

3.5.1 Den eksisterende løsning

I den nuværende NemID-løsning har brugere flere forskellige identiteter, fx som privatperson og som medarbejder, hvilket indebærer et NemID pr. identitet med forskellige nøglekort og dermed flere login-processer.

3.5.2 Nye perspektiver

Der blev i Fase 1 givet udtryk for et behov for, at brugerne kan få overblik over anvendelsen af deres NemID og deres forskellige identiteter og roller, fx udgående og indgående fuldmagter med et NemID.

Der er også behov for, at personer med flere NemID (dvs. fx både et NemID til borgere og et eller flere NemID-medarbejdersignaturer) får lettere ved at håndtere disse identiteter. Det kan fx ske ved, at den enkelte bruger kun har en identitet (dvs. ét nøglekort), der kan bruges til flere roller.

3.5.3 Potentielle løsninger

Der blev i Fase 1 arbejdet med en brugergrænseflade, hvor brugerne kan få overblik over anvendelsen af deres NemID via en samlet indgang – en NemID-profil. Den samlede indgang til NemID skal forstås som en digital afspejling af den enkelte brugers forskellige identiteter og fuldmagter. På denne måde bliver det muligt for den enkelte bruger at have overblik over forskellige identiteter og kontrollere forskellige roller fx udgående og indgående fuldmagter med et NemID.

I det følgende afsnit vil det blive beskrevet, hvordan etablering af en NemID-profil som samlet indgang til NemID teknologisk kan implementeres. Det kan principielt ske på to forskellige måder:

1. Profilløsning med et NemID pr. person
2. Front-end baseret profilløsning.

3.5.3.1 Profilløsning med ét NemID pr. person

I denne løsning dannes kun en identitet fx med ét NemID pr. person. Dette NemID kan bruges til både rollen som borger (over 15 år) og rollen som medarbejder – eventuelt i flere virksomheder. NemID skal have information om personers forskellige roller i form af kontekstafhængige attributter (dvs. informationer om brugere).

Tildeling af roller kan styres centralt (efter fastlagte regler) eller til en vis grad af de enkelte personer og virksomheder.

En løsning med et NemID pr. person vil kræve store ændringer i den samlede NemID-infrastruktur:

- Medarbejdercertifikat erstattes af et nyt personcertifikat, der både anvendes i forhold til personens rolle som borger og i forhold til rollen som medarbejder – hvilket kan være en udfordring for udenlandske medarbejdere uden privat NemID.
- Udstedelsen skal ændres til en proces, hvor et NemID først bestilles og derefter tildeles roller af henholdsvis borger og virksomhed
- NemID både i back-end og front-end skal ændres
- Tjenesteudbyderne skal ændre snitflade til NemID, så det er muligt at håndtere NemID med attributter, der viser roller.

Modeller for håndtering af attributter vil blive analyseret i forbindelse med de tekniske koncepter.

I øvrigt vil en model med et NemID kræve en yderligere analyse, både af tekniske og eventuelt juridiske forhold.

3.5.3.2 Front-end baseret profilløsning

Alternativt kan ønsket om en samlet grænseflade opnås ved, at brugeren får et samlet overblik over sine identiteter ved at lægge en "glasplade" over forskellige systemer. "Glaspladen" vil gøre det muligt at præsentere information om en persons forskellige NemID'er og eventuelle fuldmagter i en brugergrænseflade, svarende til Min Side på borger.dk.

Som forældre vil man derfor kunne få adgang til sine børns NemID profiler. Hvis barnet er mellem 15-18 år vil dette kræve, at barnet giver forældrene en fuldmagt. En sådan løsning vil kræve integration til et eller flere øvrige systemer. Desuden er der i 2014 ikke systemer, der rummer data om forældremyndighed med tilstrækkelig kvalitet.

Den tekniske kompleksitet ved etablering af en NemID profil med en glaspladeløsning vil afhænge af, hvor meget den skal omfatte herunder integrationer til eksterne systemer fx vil visning af fuldmagter vil kræve integration til NemLog-in, SKAT og andre offentlige løsninger, der håndterer fuldmagter.

Erfaringerne fra etableringen af Min side på borger.dk viser, at det kan være et omfattende og ressourcekrævende arbejde at etablere en glaspladeløsning.

3.5.4 Konklusion

Der er flere måder at danne "en profil" på. Den front-end baserede løsning ("glaspladen") kan etableres uafhængigt af de underliggende arkitekturer, men indebærer integrationer til eksterne systemer og kan derfor være potentielt kompliceret og dyrt at implementere.

En anden løsningsmodel med et NemID pr. person, der både anvendes i forhold til personens rolle som borger og i forhold til rollen som medarbejder, vil ligeledes være omfattende og teknisk kompliceret at implementere. Løsningen vil kræve store ændringer i den samlede NemID-infrastruktur og forudsætter, at der anvendes samme tekniske koncept til borger og erhverv, og at det eksisterende medarbejdercertifikat erstattes af et nyt personcertifikat.

3.6 Fuldmagt og rettigheder

Fase 1 har vist, at både borgere, medarbejdere og tjenesteudbydere har behov for håndtering af fuldmagt og rettigheder i næste generation af NemID eller i tæt sammenhæng hermed i andre løsninger, fx i NemLog-in.

For borgere kan en fuldmagtsløsning anvendes i forbindelse med værgemål, at et familiemedlem hjælper et andet og ejendomshandler. En smidig fuldmagtsløsning vil bidrage til at undgå sikkerhedskompromitterende handlinger, fx at en borger udleverer sin personlige NemID til andre.

For virksomheder kan bedre løsninger til at håndtere fuldmagt, fx én generel erhvervsfuldmagt, og rettigheder lette arbejdet både for administratorer og medarbejdere, der udfører opgaver for andre virksomheder og borgere, fx revisorer, advokater mv.

Det er RMC-ICG's erfaring fra mangeårigt arbejde med rettigheder og fuldmagter, at der er store udfordringer ved at samle fuldmagter og rettigheder i et fælles register. Fx kan både fuldmagter og rettigheder være brede eller specifikke, have forskellige tidsbegrænsninger og dække meget forskellige handlinger som at købe, sælge, repræsentere, klage osv. Det kan gøre en samlet løsning meget kompleks rent teknisk at konstruere samt at navigere i (dvs. brugervenlighedsmæssigt) for brugerne. Det kan desuden være både vanskeligt og dyrt for tjenester at tilpasse sig til en sådan ekstern rettigheds-/fuldmagtstjeneste. Generelt må det derfor konstateres, at håndtering af rettigheder og fuldmagter er på et tidligt udviklingsstadie.

3.6.1 De eksisterende løsninger

I den nuværende infrastruktur er opgavefordelingen i forhold til fuldmagt og rettigheder følgende:

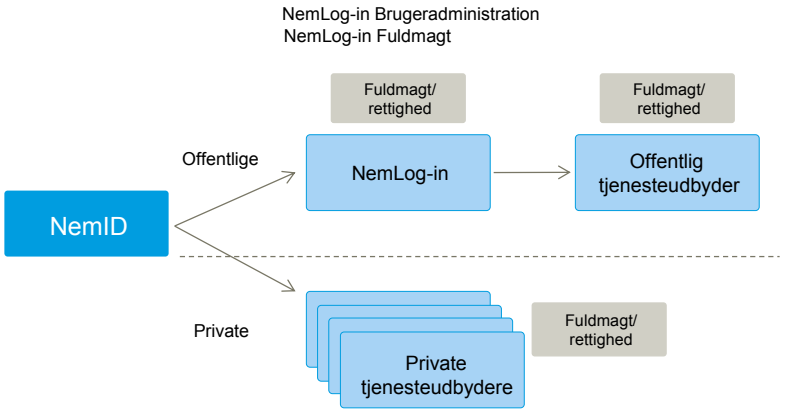
NemID håndterer login (autentifikation) og signering. Desuden har NemID til erhverv egen rettighedsstyring til virksomhedernes administratorer og tilbyder en tjeneste (isLRA - Local Registration Authority), hvor andre kan spørge, hvem der er administrator. IsLRA tjenesten giver således mulighed for at tjekke, om en given bruger er signaturadministrator på baggrund af et CVR- og et RID-nummer. Denne tjeneste anvendes af nogle tjenester – om end fejlagtigt - til rettighedsstyring.

- I forhold til offentlige tjenester er der følgende tilbud til både virksomheder og myndigheder, som anvender disse:
  - NemLog-in Brugeradministration understøtter virksomheders og myndigheders administration af medarbejderes rettigheder i de tilsluttede offentlige tjenester samt tildeling af fuldmagt til medarbejdere i andre virksomheder (fx revisorer, advokater).
  - NemLog-in Fuldmagt understøtter, at borgere kan anmode om og tildele fuldmagt i forbindelse med offentlige tjenester.
- Tjenesteudbydere har ansvaret for at brugere autoriseres korrekt på grundlag af rettigheds- og fuldmagtsinformation fra NemLog-in (attributter) eller fra egen brugeradministrationsløsning. Fx har både SKAT og Digital Post egne fuldmagtsløsninger. For Digital Post suppleret med, at man med en papirfuldmagt kan få læseadgang til et familiemedlems Digital Post.

Som det fremgår, understøtter NemLog-in p.t. alene offentlige tjenesteudbydere.

Nets DanID tilbyder løsningen "Nets rettighedsstyring", som på samme måde som NemLog-in tilbyder virksomheder og myndigheder administration af medarbejderes rettigheder i de tilsluttede tjenester. Rettighedsstyringen er rettet til private tjenesteudbydere, men enkelte offentlige tjenester anvender også løsningen.

Figur 3: Oversigt over administration af fuldmagt/rettighed i infrastrukturen



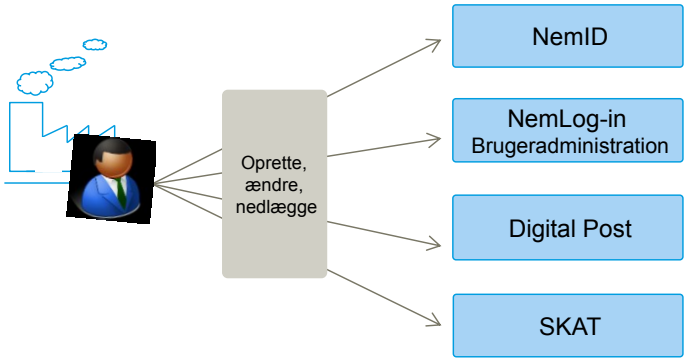
For at en tjenesteudbyder kan udnytte rettigheds- og fuldmagtsinformation fra NemLog-in (attributter), skal tjenesten tilrettes til at kunne læse attributter og til at tildele rettigheder på grundlag af disse. NemLog-in Fuldmagt er blevet etableret i efteråret 2013, og offentlige tjenesters understøttelse af denne fuldmagtsløsning må forventes at ske løbende over en længere periode.

NemLog-in rettighedsstyring er en videreførsel af Virk BRS, som er det tidligere fælles offentlige virksomhedsrettede brugerrettighedssystem. Der var allerede fra etableringen mere end 60 erhvervsrettede digital services der anvendte rettighedsstyring via NemLog-in Brugeradministration. Rettighedstildeling i NemLog-in Brugeradministration er derved i forhold til erhvervsbrugere allerede udbredt.

Teknisk set indeholder NemID ikke rettighedsinformation bortset fra den nævnte administratorinformation. Den bruges i et vist omfang af andre tjenester.

Information om fuldmagt og rettigheder i øvrigt indgår som attributter i de tokens, som NemLog-in udsteder, og som læses af de offentlige tjenester.

Figur 4: Virksomhedernes administration i forskellige offentlige tjenester



Den enkelte virksomhed skal administrere sig selv og sine medarbejdere i forhold til mange forskellige offentlige løsninger, og virksomhederne ønsker en bedre sammenhæng i dette arbejde. En bruger kan ikke agere som administrator på tværs af systemerne. I stedet har hvert system en eller flere administratorroller, og ledelsen i virksomheden skal aktivt forholde sig til, hvilken medarbejder der må udfylde hver af disse administratorroller.

RMC-ICG vurderer, at det vil være værdifuldt for virksomheder at have en samlet tilgang og overblik over deres adgang på tværs af systemer.

3.6.2 Potentielle løsninger til borgere

I NemLog-in Fuldmagt kan der gives fuldmagt til borgere til en eller flere tjenester, ligesom man kan anmode om at få fuldmagt til en eller flere tjenester. NemLog-in Fuldmagt dækker ikke Digital Post og SKAT. Borgere oplever således at skulle håndtere fuldmagter i flere løsninger.

Flere høringssvar foreslår i Fase 1, at arbejdet med at understøtte fuldmagter og rettigheder for borgere intensiveres med en fælles, brugervenlig løsning til at håndtere fuldmagter. Det kan ske ved at bygge videre på NemLog-in Fuldmagt eller etablere en løsning i andet regi. Placering (og den tekniske udformning) af en sådan løsning i den samlede infrastruktur behandles i kapitel 4 om tekniske koncepter.

Ligeledes fremhæver høringssvarene, at mange flere tjenester end nu skal tilsluttes en sådan fuldmagtsløsning. Anvendeligheden af et sådant fælles register afhænger af, hvor mange tjenester der tilsluttes og hvor hurtigt.

3.6.3 Potentielle løsninger til erhverv

For erhvervsområdet er håndtering af fuldmagter og rettigheder ligeledes fordelt på NemLog-in Brugeradministration og forskellige tjenester, hvilket gør det vanskeligt for virksomhederne at administrere brugere. Flere høringssvar giver udtryk for en klar forventning om, at den næste generation af NemID vil kunne tilbyde en brugervenlig løsning til at administrere og understøtte fuldmagter og rettigheder for virksomheder og myndigheder. En mulig løsning på dette er, at flere offentlige tjenester anvender NemLog-in Brugeradministration, eller at der på andre måder skabes bedre sammenhæng i administration på tværs af tjenester. Det kan fx ske ved, at forskellige tjenester koordinerer processen, så virksomheder præsenteres for samlede pakker af vilkår.

3.6.4 Konklusion

I den eksisterende NemLog-in er der etableret en løsning til at håndtere fuldmagter for borgere, men som høringssvarene i Fase 1 viser, er denne løsning ikke udbredt i tilstrækkelig grad til at dække behovene.

Information om administratorrettigheder i NemID anvendes uden sikkerhed for, at pågældende administratorer rent faktisk har de rettigheder, som han tildeles i andre tjenester.

Fuldmagter og rettigheder for erhverv håndteres i NemLog-in Brugeradministration og også i de enkelte tjenester, hvilket gør administrationen besværlig for virksomhederne. I forslagene til

tekniske koncepter (afsnit 4.3) er der præsenteret forskellige attributbaserede løsninger på dette for den samlede e-identitetsinfrastruktur.

Det er en forudsætning for denne udvikling af tekniske koncepter, at NemID fortsat kun håndterer autentifikation, og at fuldmagter og rettigheder håndteres i andre dele af den samlede identitetsinfrastruktur, fx i NemLog-in. Det udelukker dog ikke, at samme leverandør kan stå for både autentifikationsløsningen og løsninger med attributter til fuldmagt og rettigheder.

Da håndtering af fuldmagter og rettigheder primært ligger i NemLog-in og ikke mindst i de enkelte tjenester, er det en selvstændig stor opgave at afdække behov og løsninger. RMC-ICG anbefaler, at dette løses som et selvstændigt projekt – der dækker fuldmagter og rettigheder i den samlede e-identitetsinfrastruktur.

3.7 Samlet konklusion

I ovenstående kapitel har RMC-ICG på baggrund af vurderingen af potentielle nye anvendelser for næste generation af NemID beskrevet nye potentielle løsninger for disse.

RMC-ICG vurderer, at adskillelse af eID og eSignatur er et vigtigt element i den næste generation af NemID og vigtig forudsætning for nye funktionaliteter (fx mere brugervenlig login-funktionalitet med flere sikringsniveauer, øget privacy samt styrkelse af den juridisk forpligtende elektroniske signering). Denne adskillelse kan tilvejebringes som en funktionel adskillelse inden for samme tekniske løsning eller ved en opbygning af separate teknologiske løsninger (hvis man vælger at basere eID på ikke-PKI-teknologier).

RMC-ICG vurderer, at den fremtidige anvendelse af NemID – i tråd med den internationale udvikling – peger i retning af en mere differentieret opdeling af sikringsniveauer. Særligt vil dette kunne dække behov i det private marked, der hermed potentielt kan bidrage med en større andel af finansieringen. Løsningen bør implementeres med fokus på brugerinddragelse og brugervenlighed. Der bemærkes dog, at differentierede sikringsniveauer forudsætter en klassifikation af data og den nødvendige tilretning af tjenester for at give det fulde udbytte. Omkostningerne og omfanget af ressourcer ved etableringen af en løsning med flere sikringsniveauer kan derfor potentielt være store hos de enkelte tjenesteudbydere. Derfor skal den endelige vurdering ses i lyset af strategiske cost/benefit overvejelser.

RMC-ICG vurderer, at der er behov for, at NemID understøtter kontekstafhængig information om brugerne med mulighed for større brugerkontrol og indblik i, hvilke attributter der videregives til tjenesteudbyderen. I den forbindelse vurderes det, at anvendelsen af kontekstafhængige attributter vil sikre en større grad af privacy for borgere og en større fleksibilitet for tjenesteudbyderne, i forhold til hvilke attributter de modtager. Privacy-håndtering vurderes derfor også som et nødvendigt element i den næste generation af NemID for at sikre, at brugerne har tillid til systemet, hvilket kan sikres gennem en høj grad af transparens og privatlivsbeskyttelse. Håndteringen af privacy kan imødekommes med forskellige tekniske løsninger (jf. afsnit 3.4 og bilag 3 om autentifikationsteknologier og protokoller).

Etableringen af en NemID-profil, dvs. digital afspejling af den enkelte brugers forskellige identiteter og fuldmagter, kan løses på flere måder. En løsning i brugergrænsefladen alene (front-end baseret ”glasplade”-løsning) – kan etableres uafhængigt af de underliggende arkitekturer, men indebærer integrationer til eksterne systemer. En løsning med et NemID pr. person vil kræve store ændringer i den samlede NemID-infrastruktur. Det forudsætter, at der anvendes samme tekniske koncept til borger og erhverv, og at medarbejdercertifikatet erstattes af et nyt personcertifikat, der både anvendes i forhold til personens rolle som borger og i forhold til rollen som medarbejder. RMC-ICG vurderer derfor, at det potentielt er en omfattende og teknisk kompliceret opgave at implementere begge løsningsmodeller.

Der er rejst ønske om en tættere sammenhæng mellem NemID og fuldmagt og rettigheder. Det kan løses på flere måder både i forbindelse med den ovennævnte NemID-profil og ved revision af de erhvervsrettede løsninger, som beskrives nedenfor. Da håndtering af fuldmagter og rettigheder

primært ligger i NemLog-in og ikke mindst i de enkelte tjenester, er det en selvstændig stor opgave at afdække behov og løsninger, og RMC-ICG anbefaler, at dette løses gennem et selvstændigt projekt – der favner fuldmagter og rettigheder i den samlede identitetsinfrastruktur.

Som det er vist, kan ovennævnte ønsker og behov til en ny generation NemID kun vanskeligt eller slet ikke imødekommes, uden at den grundlæggende arkitektur ændres. I næste kapitel beskrives den nuværende arkitektur samt nye tekniske koncepter, der på forskellig vis imødekommer ønsker og behov.

Tekniske koncepter

4. Tekniske koncepter

Formålet med kapitel 4 er at præsentere de tekniske koncepter, som RMC-ICG vurderer, kan imødekomme krav til den næste generation af NemID. Kapitlet vil indledningsvist præsentere den eksisterende tekniske infrastruktur for derefter at fremføre forudsætningerne for de tekniske koncepter, herunder de grundlæggende antagelser for næste generation af NemID samt de arkitekturprincipper, den tekniske analyse bygger på. Herefter præsenteres og vurderes de fem koncepter. Kapitlet afsluttes med en samlet konklusion.

Formålet med koncepterne er, at de skal fungere som en teknologisk ramme for udviklingen af fremtidige scenarier i Fase 3. Det er derfor vigtigt at pointere, at koncepterne *ikke* skal opfattes som specifikke løsningsmodeller, men som et udgangspunkt for en dialog omkring udviklingen af scenarierne i Fase 3, hvor de efter behov vil blive analyseret, vurderet og tilpasset.

Koncepterne har taget hensyn til input fra Fase 1-rapporten og den dialog, der her har været med interessenter, slutbrugere, eksperter og Digitaliseringsstyrelsen.

Sideløbende med dette analysearbejde er der lavet oplæg til arkitekturprincipper for design af den næste generation af NemID, ud fra hvad der er anerkendt bredt i markedet som gængse og anbefalede arkitekturprincipper for it-projekter og e-identitets- og signeringsinfrastrukturer.

Erfaringer fra den eksisterende løsning, mulige nye elementer i den kommende generation af NemID og arkitekturprincipper har således været udgangspunktet for udarbejdelsen af koncepterne - og denne proces beskrives i nedenstående figur.

Figur 5: Oversigt over processen for udarbejdelsen af de tekniske koncepter

4.1 Den eksisterende tekniske arkitektur

Den eksisterende arkitektur for NemID bygger på en samlet autentifikations- og signeringsløsning med anvendelse af samme certifikat til de to formål og med samme bagvedliggende mekanisme (baseret på signering) til både autentifikation og signering.

Certifikatet indeholder meget få indbyggede attributter, og disse er primært defineret i forhold til behovet for signeringsoperationer. Dette minimumssæt af attributter omfatter:

- Navn (kan erstattes af ”pseudonym”, hvis det ønskes af bruger)
- PID for borgerløsning
- RID for erhvervsløsning
- CVR-nummer og organisationsnavn for erhvervsløsningen
- Optionel mailadresse.

Den eksisterende arkitektur har tre varianter for håndtering af certifikater:

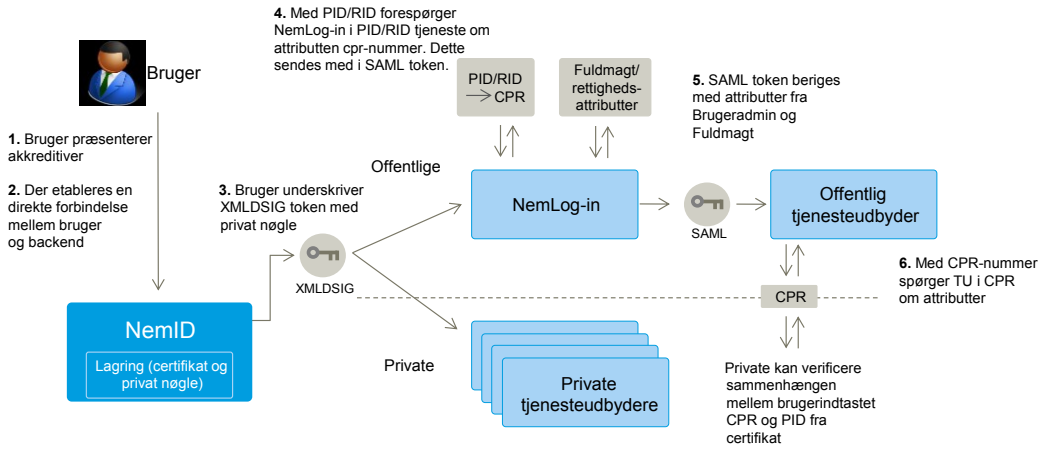
- Certifikat i central løsning med de tilhørende private nøgler placeret hos Nets DanID. Brugeren kontrollerer adgangen til certifikatet med kodeord og nøglekort, som de facto akkreditiv. Teknisk kan denne løsning karakteriseres som ”authentication as a service”.
- Lokale certifikater og tilhørende private nøgler på brugerens udstyr (pc, USB krypto-token)

- Lokale certifikater og tilhørende private nøgler på signaturserver.

Langt størstedelen af NemID-brugerne anvender den centrale løsning (basisløsningen), som derfor beskrives i det nedenstående.

Den nuværende basisløsning for borgere består af et NemID med nøglekort, herunder nøglekort i stort format og en telefonisk voice response-løsning. Der er supplerende løsninger i form af nøgleviser og NemID på hardware, hvor certifikat og tilhørende privat nøgle ligger beskyttet på USB krypto-token lokalt hos borgeren. De offentlige tjenesteudbydere kan indhente yderligere attributter ved hjælp af NemLog-in eller gennem CPR-registret ved at anvende PID/CPR-tjenesten ejet af Digitaliseringsstyrelsen. For virksomhederne er der to NemID-basisløsninger med nøglefil (installeret på computeren) og NemID med nøglekort (som borgerløsningen). Herudover findes tillige NemID på hardware og NemID med signaturserver (afart af NemID med nøglefil). De private tjenesteudbydere kan i modsætning til de offentlige tjenesteudbydere kun anvende et minimumsæt af attributter. Brug af CPR kan kun ske efter samtykke eller ved direkte indtastning.

Figur 6: Den eksisterende tekniske arkitektur for centralt lagrede private nøgler



Løsninger med lokalt lagrede private nøgler kræver, at login-tjenesten understøtter denne type. Det gør NemLog-in.

Løsninger med lokale certifikater og tilhørende private nøgler på en lokal signaturserver leveres af tredjeparter og kan designes til at imødekomme lokale behov som i sundhedsvæsenet, hvor NemID skal anvendes i fx EPJ-systemer, således at medarbejdersignaturen kan anvendes til at autentificere sig over for identitetsgaranten.

4.2 Forudsætningerne for de tekniske koncepter

De tekniske koncepter, som er præsenteret i dette afsnit, bygger på følgende grundlæggende antagelser i forhold til den næste generation af NemID:

- Understøttelse af eID- og eSigneringsfunktionalitet for borgere
- Næste generation af NemID skal som nu håndtere autentifikation og signering, mens autorisation (fuldmagter og rettigheder) skal håndteres af andre dele af den samlede infrastruktur
- Understøttelse af eID- og eSigneringsfunktionalitet for medarbejdere
- Understøttelse af en nøglekortbaseret basisløsning
- Udstilling af snitflader, der muliggør andre supplerende løsninger
- Understøttelse af signaturservere for større virksomheder.

Udgangspunktet for de tekniske koncepter har desuden været udvælgelsen af tekniske elementer, der har til formål at understøtte potentielle *nye* anvendelser af (og retningslinjer for etablering af) den fremtidige generation af NemID, og de fungerer derfor som en vigtig grundsten for udarbejdelsen af de tekniske koncepter.

Følgende elementer, der er analyseret i kapitel 3, vurderes af RMC-IMG som mulige nye elementer i den næste generation af NemID:

- Adskillelse af eID og eSignatur
- Flere sikringsniveauer
- Kontekstafhængig information
- Fokus på øget privacy
- En NemID-profil
- Fuldmagter og rettigheder.

Derudover indgår de arkitekturprincipper, der er beskrevet nedenfor, i udviklingen af koncepterne.

De tekniske koncepter vil blandt andet blive anvendt i Fase 3 til løsningsscenarier, hvor de analyseres og vurderes nærmere.

Det skal understreges, at de tekniske koncepter sætter fokus på grundlæggende mulige elementer i en fremtidig infrastruktur og omhandler derfor ikke:

- Brugergrænseflader. Brugerne kan og bør afskærmes fra at se, hvordan løsningen er bygget op
- Implementering af en NemID-profil (jf. afsnit 3.5) med to grundlæggende modeller for at opnå en samlet og ensartet indgang for den private og erhvervsrelaterede anvendelse af løsningen).

I de følgende beskrivelser af mulige tekniske arkitekturer skelnes der mellem primære og sekundære attributter.

De primære attributter er de kontekstafhængige attributter, der er *besluttet* i infrastrukturen, og som beskriver entiteten. Valg af attributter (herunder eventuelt valg af dynamisk PID) er en væsentlig del af implementeringen og den løbende drift og skal reguleres i en governance-struktur.

Det skal også besluttes, i hvilket omfang og hvordan brugeren selv informeres, og om brugeren skal godkende, hvilke attributter der overføres til tjenesteudbyder.

Tabel 10: Eksempler på primære attributter

Private	Erhverv
Har NemID	Navn
PID	RID
Køn	Stilling
Alder (eller fx over/under 18)	CVR
Navn	Virksomhedens adresse
Adresse	CPR-nummer
CPR-nummer	Tegningsberettiget
Statsborgerskab	Rolle
Bopælskommune	

De sekundære attributter omfatter de andre attributter, som tjenesteudbydere har brug for om entiteterne i forbindelse med tjenesten. Hvad disse attributter *kan* omfatte, fremgår af nedenstående tabel.

Tabel 11: Eksempler på sekundære attributter

Private	Erhverv
Spærreliste for online spil.	Rettighedsdata: Data om rolle, gruppe mv., der har

Private	Erhverv
Spiludbydere skal tjekke, at spillere ikke er tilmeldt spærrelisten.	relevans for tildeling af rettigheder: • Fx attributter fra NemLog-in Brugeradministration • Fx fuldmagt, som delvist kan komme fra NemLog-in Fuldmagt.
Personlig indkomst, fx fra eIndkomst.	
Sundhedsdata, fx praktiserende læger.	

4.2.1 Arkitekturprincipper

Af nedenstående afsnit fremgår de principper, som RMC-ICG vurderer vigtige i udviklingen af arkitekturen for næste generation af NemID. Disse principper, som er i overensstemmelse med OIO arkitekturguide[8], har fungeret som generelle retningslinjer for, hvordan de tekniske koncepter skulle udvikles og iagttages ved den konkrete opbygning af infrastruktur for den næste generation af NemID.

4.2.1.1 Åbenhed og standarder

Infrastrukturen for den næste generation af NemID skal udvikles med fokus på kommerciel og teknisk åbenhed for at understøtte interoperabilitet mellem identitetsgarant(-er), login-tjenester, attributtjenester og tjenesteudbydere etc. på tværs af markedet. En høj grad af interoperabilitet vil være med til at sikre en stærk og robust infrastruktur, hvor det vil være muligt at udvide den næste generation af NemID i forhold til ny funktionalitet og teknologiske krav, samtidigt med at det vil mindske omkostninger for potentielle leverandører.

Udviklingen af infrastrukturen skal således ske efter anerkendte standarder med henblik på at understøtte national og international interoperabilitet.

4.2.1.2 Modularitet

Et system bestående af enkelt moduler vil som regel være mere fleksibelt end et stort monolitisk opbygget system. Mulighederne for tilpasning af enkelte moduler øges, og afhængigheden af leverandørspecifikke løsninger reduceres.

Der skal derfor som udgangspunkt tilstræbes en modulær opbygning for næste generation af NemID. En modulær opbygning vil være med til at skabe en større fleksibilitet og robusthed, når løsningen skal understøtte nye teknologier. Den vil endvidere tilvejebringe en større sandsynlighed for, at kommercielle aktører kan træde til og tilbyde nye innovative løsninger og produkter.

Samtidigt øges mulighederne for at korrigere og/eller supplere samt videreudvikle løsningen på ethvert tidspunkt i forløbet, hvis den teknologiske udvikling gør det nødvendigt.

Den modulære arkitektur gør det lettere at opbygge en testbar løsning, hvilket potentielt vil give færre omkostninger, højere kvalitet og færre forsinkelser. Krav om testbarhed skal i denne sammenhæng også omfatte muligheder for at teste tjenesteudbyderens løsninger. Det skal dog understreges, at en modulær opbygning kræver stramme og præcise styringsmekanismer med en

[8] http://arkitekturguiden.digitaliser.dk/principper

meget klar placering af det totale ansvar for leverancen, både under implementering og anvendelsen af systemet.

En modulær opbygning af en samlet løsning kan fx omfatte funktionelle moduler i form af adskillelse af autentifikations- og signeringsdelen, adskillelse af basisløsningen fra supplerende løsninger eller en adskillelse af identitetsgarant- og loginopgaver.

4.2.1.3 Redundans

For at sikre en høj stabilitet og dermed en høj grad af tilgængelighed skal der for den næste generation af NemID sikres tilstrækkelig redundans, således at systemet i tilfælde af fejl fortsat fungerer i henhold til de opstillede driftsmål. Redundans skal sikres gennem anvendelsen af dublerede enheder (eventuelt placeret på forskellige adresser) og autorisering af fall-back rutiner.

4.2.1.4 Privacy by Design

For at kunne beskytte privatlivets fred er det vigtigt, at sådanne hensyn inkluderes fra begyndelsen af etableringen af den næste generation af NemID. Ved at indføre princippet om Privacy by Design sikres der ikke kun en høj grad af privacy, men den enkelte bruger vil, hvis relevant, få mulighed for større kontrol over de informationer, der videregives.

4.2.1.5 Sikkerhed

Det er afgørende, at den nationale infrastruktur for elektronisk identitet og signatur har et højt sikkerhedsniveau både i forhold til driftsstabilitet og datasikkerhed. Opbygning af infrastrukturen skal derfor fra begyndelsen være robust, samtidig med at den er fleksibel for løbende at kunne adressere nye sikkerhedsmæssige trusler.

4.3 Koncepterne

I det følgende præsenteres og vurderes fem forskellige tekniske koncepter.

Koncepterne er blevet udviklet og opstillet med henblik på at optimere den næste generation af NemID og har derfor tre primære formål:

- Muliggøre øget konkurrence på leverandørsiden gennem størst muligt funktionsopdeling og dermed mulighed for en flerleverandørstrategi
- Anvendelse af ”mainstream” (dvs. ikke-PKI-baseret) teknologi i forhold til autentifikation
- Størst muligt kontinuitet i forhold til den eksisterende løsning.

Koncept 1, 2 og delvist Koncept 3 anvender en traditionel PKI-baseret-infrastruktur (som i den eksisterende NemID-løsning), mens Koncept 4 og 5 anvender andre autentifikationsmekanismer og baseres på IMS.

I Koncept 2 og 4 er det identitetsgaranten, der leverer attributter til tjenesteudbyderen.

Koncept 3 og 5 lægger derimod op til en skarp adskillelse af identitetsgarant og login-tjeneste, hvor identitetsgarant(-er) alene står for autentifikation. Det er således login-tjenesten, der i disse koncepter henter garanti for identiteten hos identitetsgaranten, videreleverer denne garanti og leverer attributter til tjenesteudbyderen. Ansvar for en autentifikation/validering er dermed fordelt mellem identitetsgaranten (der står for entitet og de tilhørende akkreditiver) og login-tjenesten (der står for identiteten over for tjenesteudbyderen).

Følgende tabel giver en summarisk oversigt over koncepterne:

Tabel 12: Summarisk oversigt over koncepterne

Teknisk arkitektur	Samlet funktionalitet	Funktionsopdelt
PKI	**Koncept 1:** PKI/X.509 baseret – langtidscertifikater. Separat attribut-tjeneste.	**Koncept 3:** PKI/X.509 baseret – langtidscertifikater.

	Koncept 2: PKI/X.509 baseret – Korttidscertifikater Anvendes til at levere attributter.	Identitetsgarant adskilt fra login-tjeneste(r), der leverer attributter.
Ikke-PKI	**Koncept 4:** IMS-baseret - identitetsgarant leverer attributter.	**Koncept 5:** IMS-baseret. Identitetsgarant adskilt fra login-tjeneste(r), der leverer attributter.

Koncepterne adskiller sig således både i forhold til graden af anvendelsen af PKI-infrastruktur til autentifikationsfunktionalitet og i forhold til opgaveopdeling, dvs. hvilke roller og hvilket ansvar de forskellige leverandører skal varetage.

Erfaringer oparbejdet fra både den tidligere digital signatur-løsning og den nuværende version af NemID med stor accept af nøglekortløsning – bekræftet af forskellige brugerundersøgelser - dvs. en central opbevaring af private nøgler for borgere (og ikke lokalt på borgeres udstyr) danner ligeledes en vigtigt præmis for udarbejdelsen af disse koncepter.

Koncepterne er bygget ud fra en forudsætning om, at den næste version af NemID tager udgangspunkt i en løsning som nu med basisløsning for borgere baseret på nøglekort og to basisløsninger for NemID til erhverv, som baseres på nøglefil og nøglekort. En nøglekortbaseret løsning kan i denne sammenhæng teknisk set betragtes som en ”authentication as a service”, hvor en central tjeneste registrerer identiteter og autentificerer brugerne med eller uden brug af en PKI-baseret-løsning. Løsningerne vil i alle koncepter kunne suppleres med andre løsninger, fx certifikater og tilhørende private nøgler placeret på brugernes private SmartCard-udstyr eller på signaturservere.

Fælles for alle opstillede koncepter er understøttelse af signeringsfunktionalitet gennem PKI-teknologi, hvor der anvendes langtidscertifikater – svarende til den eksisterende NemID-løsning.

Koncepterne kan anvendes både til NemID til borgere og NemID til erhverv, og der kan vælges samme, forskellige koncepter eller deres kombination til de to.

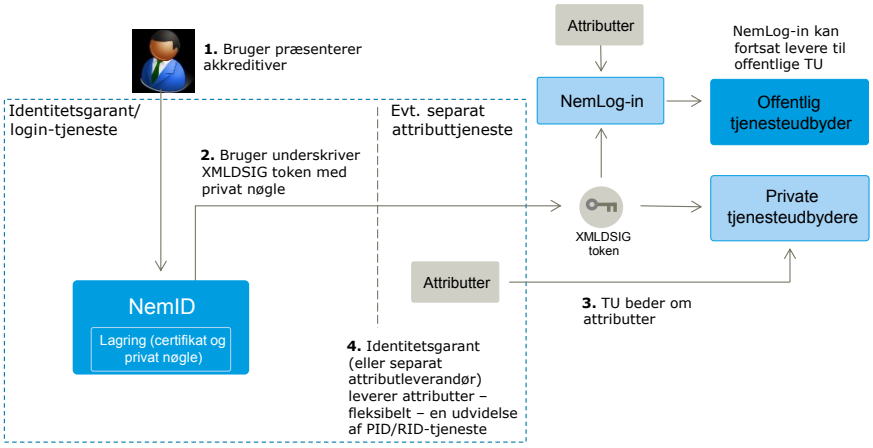
4.3.1 Koncept 1: NemID med separat attributtjeneste

Koncept 1 (jf. nedenstående figur) er i høj grad en videreførelse af den nuværende løsning med PKI-infrastruktur og anvendelse af X.509v3-certifikater og hvor der også vil kunne leveres en kontekstafhængig information i form af attributter. De private nøgler vil i basisløsningen blive opbevaret centralt og beskyttet med engangskoder, dvs. med nøglekort.

Konceptet er illustreret på den nedenstående figur.

Som nu, varetager identitetsgaranten i dette koncept rollen som login-tjeneste – særligt for private tjenesteudbydere og for de offentlige løsninger, der ikke anvender NemLog-in autentifikations-tjeneste. Attributter vil i konceptet blive leveret separat af identitetsgaranten/login-tjenesten eller af en separat attributleverandør, fx gennem en udvidelse af den eksisterende PID/RID-tjenesten.

Figur 7: Koncept 1



Ved udstedelsen vil identitetsgaranten danne (forskellige) certifikater til både autentifikation og signering - på den måde adskilles de to funktionaliteter (eID og eSignering) fra hinanden.

Understøttelse af flere sikringsniveauer vil i konceptet kræve:

- Udstedelse af certifikater til henholdsvis 1-faktor og 2-faktor autentifikation med udvidelse af OCES-politikker til at håndtere dette og med et minimum af attributter, som kan suppleres med yderligere attributter fra en attributtjeneste (hvis man vil anvende PKI til 1-faktor autentifikation)
- Udstedelse af certifikat til signering med attributter som nu.

Det betyder, at en bruger potentielt skal have tre certifikater: certifikat til 1–faktor autentifikation, certifikat til 2-faktor autentifikation og et certifikat til signeringsfunktionalitet.

Nedenstående tabel opsummerer konceptet i forhold til vurderingsparametrene.

Tabel 13: Vurdering af Koncept 1

Parametre	Vurdering
Brugervenlighed	Løsningen bliver lidt mere kompleks med potentielt tre certifikater pr. bruger (ved 1- og 2-faktor autentifikation). Det forventes, at brugeren i høj grad kan afskærmes fra den underliggende tekniske kompleksitet, da der som udgangspunkt vil være samme leverandør af de tre certifikater, og da der bruges samme teknologier (PKI). Dog vil der være forskel for brugeren i forhold til anvendelse af 1-faktor og 2-faktor autentifikation.
Migrering	Meget høj bagudkompatibilitet. Eksisterende login-tjenester og tjenesteudbydere fortsætter uændret (både offentlige i forhold til NemLog-in og specialiserede signaturserver løsninger og det private i forhold til NemID).
Arkitektur/teknologi	Kendt og velafprøvet setup. Behov for ændring af den nuværende binding mellem klient og back-end. God teknologisk sammenhæng mellem signering og autentifikation. Separat attributtjeneste er arkitekturmæssigt simpel, men måske ikke den mest ”elegante” og ”udviklervenlige” løsning set fra tjenesteudbydernes side.
Modenhed	Moden og velafprøvet koncept og teknologi.
Økonomi	Konceptet er en udvidelse af den eksisterende NemID-løsning med en

Parametre	Vurdering
	separat/adskilt attributtjeneste – og dets økonomi vurderes til at være på samme niveau som den nuværende løsning.

4.3.2 Koncept 2: NemID med attributtjeneste baseret på kortidscertifikater

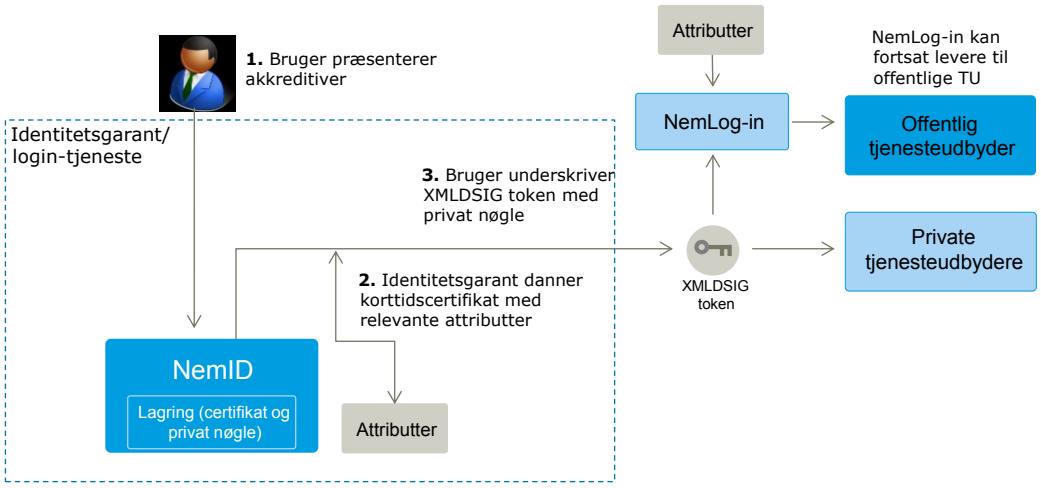
Koncept 2 (jf. nedenstående figur) bygger på anvendelsen af korttidscertifikater til autentifikation, der gør det muligt at tilbyde "on demand"-attributter til identifikation afhængigt af deres behov for information om brugerne til de specifikke tjenester. Til signering anvendes langtidscertifikater som i den nuværende løsning.

Konceptet adskiller sig fra Koncept 1 primært ved at attributterne (information om brugere) kan "bæres" i korttidscertifikater. Identitetsgaranten i dette koncept varetager rollen som login-tjeneste – særligt for private tjenesteudbydere og for de offentlige løsninger, der ikke anvender NemLog-in autentifikations-tjeneste.

Korttidscertifikater og tilhørende private nøgler genereres centralt efter autentifikation med adgangskode og engangskoder (OTP). Konceptet kræver langtidscertifikater til at understøtte signeringsfunktionaliteten.

Anvendelse af korttidscertifikater giver en særlig udfordring i forhold til erhvervsløsninger, der baseres på nøglefil, herunder løsninger hvor nøglefiler opbevares på signaturservere, og i forhold til webtjenester. Disse løsninger skal kunne tilpasses således, at de vil kunne anvende kortidscertifikater. Alternativt vil der være behov at generere (afledte) langtidscertifikater på baggrund af kortidscertifikater.

Figur 8: Koncept 2



Understøttelse af flere sikringsniveauer til autentifikation vil i konceptet kræve udstedelse af korttidscertifikater til henholdsvis 1-faktor og 2-faktor autentifikation og udvidelse af OCES-politikker til at håndtere dette (hvis man vil anvende PKI til 1-faktor autentifikation). Som nævnt skal langtidscertifikater til signering udstedes separat.

Nedenstående tabel opsummerer konceptet i forhold til vurderingsparametrene:

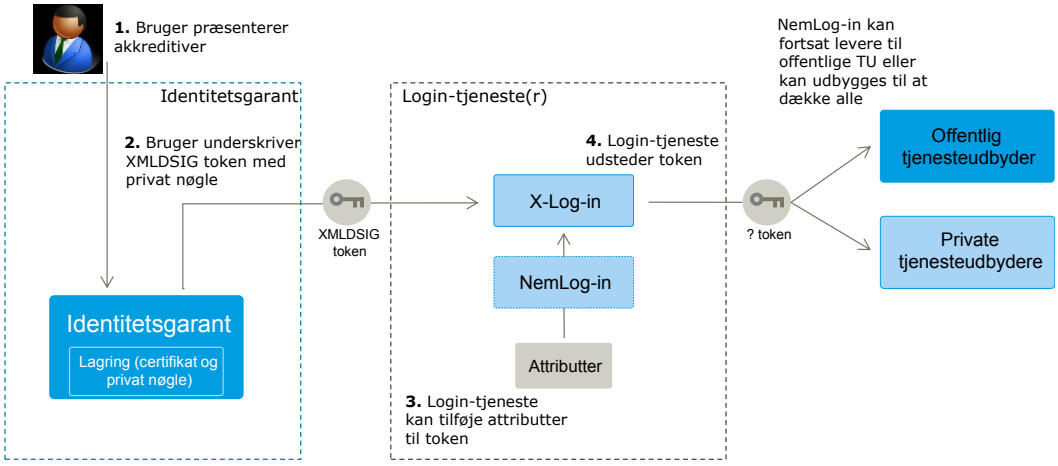
Tabel 14: Vurdering af Koncept 2

Parametre	Vurdering
Brugervenlighed	Løsningen bliver lidt mere kompleks med potentielt to typer af korttidscertifikater pr. bruger (ved 1- og 2-faktor autentifikation) og et langtidscertifikat til signering. Det forventes, at brugeren i høj grad kan afskærmes fra den underliggende kompleksitet, da der som udgangspunkt vil være samme leverandør af de tre certifikater, og da der bruges samme grundlæggende teknologier. Dette vil også gælde hvis langtidscertifikater udstedes af en anden leverandør. Der vil være forskel for brugeren i forhold til anvendelse af 1-faktor og 2-faktor autentifikation.
Migrering	Meget høj bagudkompatibilitet. Eksisterende login-tjenester og tjenesteudbydere fortsætter uændret (både offentlige i forhold til Nem-Login samt specialiserede signaturløsninger og det private i forhold til NemID). Der vil være behov for at opretholde Certificate Revocation List for at sikre bagudkompatibilitet og langtidscertifikater til signering.
Arkitektur/teknologi	Velkendt teknologi i Danmark (kortidscertifikater anvendt af bankerne i den eksisterende løsning). Ikke udbredt i forhold til nationale eID-infrastrukturer. Behov for ændring af den nuværende binding mellem klient og back-end. God teknologisk sammenhæng mellem signering og autentifikation. Hurtigere og mere effektiv kommunikation mellem login-tjeneste og tjenesteudbydere (kun et token) i forhold til Koncept 1. Behov for stor tilpasning i forhold til løsninger der anvender signaturservere og i forhold til webtjenester. Disse løsninger skal kunne tilpasses til at kunne anvende korttidscertifikater. Alternativt vil der være behov for at generere (afledte) langtidscertifikater på baggrund af kortidscertifikater.
Modenhed	Korttidscertifikat-teknologi ikke så udbredt som traditionel PKI.
Økonomi	Konceptet er en udvidelse af den eksisterende NemID-løsning – og dets økonomi vurderes til at være på samme niveau som denne løsning.

4.3.3 Koncept 3: NemID - PKI-baseret og identitetsgarant adskilt fra login-tjenesten

Koncept 3 bygger – i modsætning til de to tidligere koncepter - på en *adskillelse* af identitetsgarantens opgaver, som omfatter håndtering af certifikatteknologi fra login-tjenestens opgaver, som omfatter fleksibel tilføjelse af attributter.

Figur 9: Koncept 3



Ved udstedelsen vil identitetsgaranten udstede et certifikat, som brugerne kan anvende til *både* autentifikation og signering. I basisløsningen for borgere og i den nøglekort baserede basisløsning for virksomheder lagres certifikatet centralt hos identitetsgaranten.

I konceptet kan en eller flere login-tjenester fungere som indgang for alle tjenesteudbydere. Principielt vil denne arkitektur kunne anvende NemLog-in modellen fra det offentlige - hvor NemLog-in afkobler tjenester fra NemID – til også at omfatte private tjenester. Attributter (dvs. informationer om brugere) kan lagres i login-tjenesten eller hentes i realtid hos attributtjenester.

Konceptet kan indebære en mulighed for, at login-tjenesten ”linker” til og kan få identitetsgarantier fra flere leverandører, dvs. ikke kun fra en national identitetsgarant. De andre garanter kan fx omfatte andre EU-lande (svarende til PEPS-funktionalitet dvs. Pan-European Proxy-functionality), eller kommercielle tjenester som fx Google og Facebook.

RMC-ICG vurderer, at understøttelse af flere sikringsniveauer til autentifikation i dette koncept kræver flere certifikater, men både bruger og tjenester vil fuldstændigt være afkoblet fra dette i kraft af login-tjenesten. Et alternativ kan være, at login-tjenesten danner afledte identiteter af brugerens oprindelige identitet.

Konceptet anvender traditionel PKI-teknologi mellem identitetsgarant og login-tjenester (og til signering).

Til kommunikation mellem login-tjenester og tjenesteudbyder kan der vælges flere teknologier – og de kan ændres over tid - både de “klassiske” som fx SAML og OpenID Connect og de nye med fokus på privacy som fx privacy-fokuserede ABC-teknologier og protokoller (se i øvrigt afsnit 3.4 og bilag 3).

Adskillelse af identitetsgarantens opgaver fra login-tjenestens opgaver skal håndteres i forhold til erhvervsløsninger med nøglefil (herunder signaturservere), hvor kravet om bagudkompatibilitet fordrer et behov for direkte adgang til identitetsgaranten. Nedenstående tabel opsummerer konceptet i forhold til vurderingsparametrene.

Tabel 15: Vurdering af Koncept 3

Parametre	Vurdering
Brugervenlighed og funktionalitet	Høj brugervenlighed – brugeren ser kun login-tjenesten, der skjuler helt, at der er flere certifikater. Dog vil der være forskel for brugeren i forhold til anvendelse af 1-faktor og 2-faktor autentifikation. Mulighed for fleksible attributter tilpasset forskellige behov. Mulighed for SSO på tværs af offentlige og private tjenesteudbydere.
Migrering	Der kan sikres bagudkompatibilitet for private tjenester, ved at identitetsgaranten i en længere overgangsperiode kan betjene tjenester

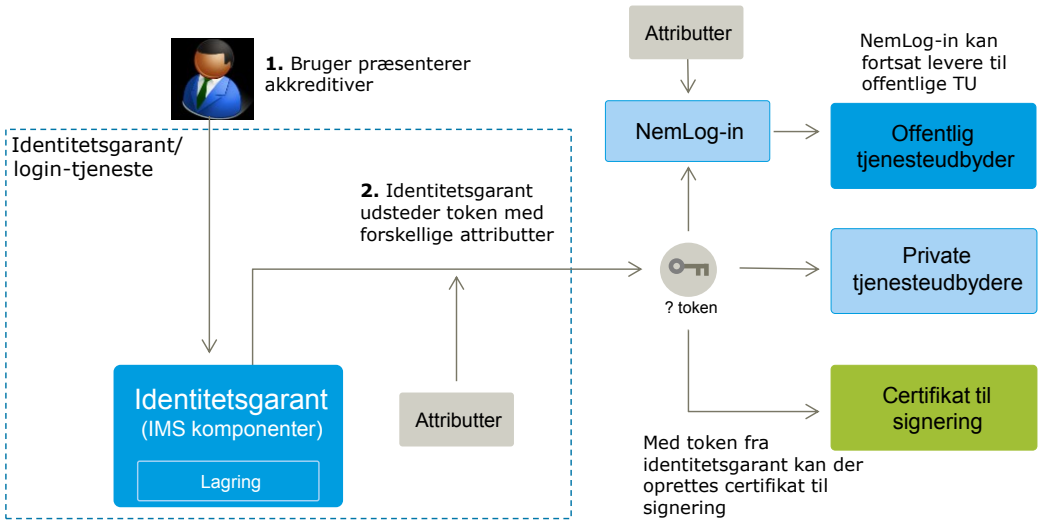
Parametre	Vurdering
	direkte. Behov for at sikre bagudkompatibilitet i forhold til signaturserverløsninger gennem direkte adgang til identitetsgaranten. Eksisterende offentlige tjenester kan fortsætte uændret.
Arkitektur/teknologi	Kompleksiteten øges, da der introduceres et ekstra lag i arkitekturen (dog ikke for det offentlige, hvis NemLog-in får ny rolle). Det samme gælder for de private tjenester, som i dag anvender login-tjenester. Afkobling af login-tjeneste giver mulighed for løbende tilføjelse af nye protokoller uden stort impact for tjenesteudbydere. Hurtigere og mere effektiv kommunikation mellem login-tjeneste og tjenesteudbydere (kun et token, der rummer de relevante attributter).
Modenhed	Moden og velafprøvet teknologi.
Økonomi	Adskillelse af identitetsgarant og login funktioner vil sandsynligvis betyde øgede omkostninger på grund af øget kompleksitet og behov for koordinering og styring på tværs af leverandører.

4.3.4 Koncept 4: NemID – IMS-baseret

Konceptet er opbygget efter samme arkitekturprincipper som den eksisterende løsning, men uden anvendelse af PKI-teknologi til autentifikation. Konceptet bygger på, at identitetsgaranten/login-tjenesten anvender et IMS, dvs. uden certifikater til entiteter.

Konceptet svarer til Koncept 1, hvor identitetsgaranten varetager rollen som login-tjenesten og leverer token til tjenesteudbyderen (herunder NemLog-in) med de valgte attributter.

Figur 10: Koncept 4



Udstedelsesflowet kan starte med udstedelse af eID, hvorefter brugeren kan bede om et certifikat til signering (signering i konceptet bygger fortsat på en separat PKI-løsning, som er fuldstændigt adskilt – dvs. også teknologisk - fra identitetsfunktionalitet).

NemLog-in kan i konceptet fortsætte uændret eller kan udbygges (som i Koncept 3 og 5) til fx at være en login-tjeneste for private (og eventuelt med mulighed for single sign-on).

Til kommunikation mellem login-tjenester og tjenesteudbyder kan der vælges flere teknologier – og de kan ændres over tid - både de "klassiske" ABC-teknologier som fx SAML og OpenID Connect og de nye med fokus på privacy som fx privacy-fokuserede ABC-teknologier (beskrevet i øvrigt afsnit 3.4 og bilag 3).

Nedenstående tabel opsummerer konceptet i forhold til vurderingsparametrene.

Tabel 16: Vurdering af Koncept 4

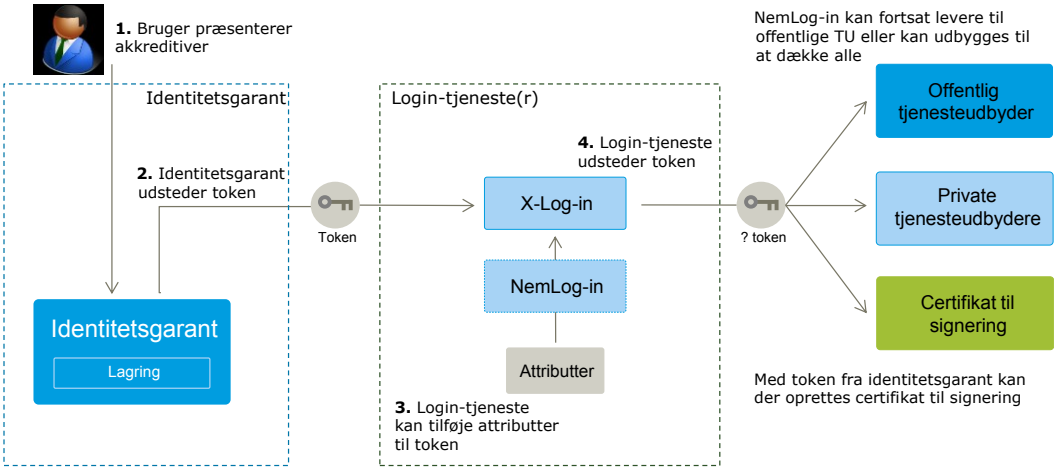
Parametre	Vurdering
Brugervenlighed og funktionalitet	En fuldstændig teknologisk adskillelse mellem eID og signering kan indeholde udfordringer i forhold til brugergrænsefladen, hvilket dog afhænger af den konkrete implementering. Mulighed for fleksible attributter.
Migrering	Ikke-bagudkompatibel i forhold til det private og løsninger der forudsætter PKI-funktionalitet (fx signaturserverbaserede løsninger). Dog kan lokale certifikater og tilhørende private nøgler i signaturserverløsninger baseres på signeringsdelen, som bygger på PKI. Det kræver en nærmere analyse.
Arkitektur/teknologi	Velkendt teknologi for signering. Mulighed for eventuelt at anvende standard off-the-shelf IMS-produkter. Hurtigere og mere effektiv kommunikation mellem login-tjeneste og tjenesteudbydere (kun et token).
Modenhed	IMS-løsninger er primært rettede mod enterprise-brug og p.t. ikke udbredt i meget stor skala (dvs. med millioner af brugere).
Økonomi	Større samlede omkostninger som følge af behov for tilpasninger hos tjenesteudbydere samt behov for etablering af to separate infrastrukturer (autentifikation og signering).

4.3.5 Koncept 5: NemID – IMS-baseret med identitetsgarant adskilt fra login-tjeneste

Konceptet lægger op til en adskillelse af identitetsgarantfunktionen fra opgaver, der varetages af login-tjenesten inkl. tilføjelse af attributter. Identitetsgaranten anvender ikke PKI, men et IMS) uden certifikater til entiteter. Konceptet kan således betragtes som en variant af Koncept 3, men kommunikationen mellem identitetsgaranten og login-tjenesten baseres *ikke* på XMLDSig.

Identitetsgaranten leverer kun autentifikation til login-tjenester i form af en token med de valgte attributter. Login-tjenesten kan implementeres som en ny tjeneste (eventuelt flere) eller gennem modificering af NemLog-in.

Figur 11: Koncept 5



Konceptet giver ligesom Koncept 3 mulighed for potentielt flere identitetsgaranter fra andre EU-lande eller kommercielle tjenester, fx Google og Facebook, og snitfladen til login-tjenester kan understøtte flere protokoller.

Til kommunikation mellem login-tjeneste og tjenesteudbyder kan der vælges flere teknologier, som over tid både kan omfatte "klassiske" SAML og OpenID Connect og (på sigt) privacy-fokuserede ABC-teknologier som U-Prove og Identity Mixer.

Signeringsfunktionalitet i konceptet bygger fortsat på en PKI-løsning, der er modulært og teknologisk adskilt med samme forhold som i Koncept 4.

Nedenstående tabel opsummerer konceptet i forhold til vurderingsparametrene.

Tabel 17: Vurdering af Koncept 5

Parametre	Vurdering
Brugervenlighed og funktionalitet	En fuldstændig teknologisk adskillelse mellem eID og signering kan indeholde udfordringer i forhold til brugergrænsefladen, hvilket dog afhænger af den konkrete implementering. Mulighed for fleksible attributter tilpasset forskellige behov.
Migrering	Ikke-bagudkompatibel i forhold til det private og løsninger, der forudsætter PKI-funktionalitet (fx signaturserverbaserede løsninger). Dog kan lokale certifikater og tilhørende private nøgler i signaturserverløsninger baseres på signeringsdelen, som bygger på PKI.
Arkitektur/teknologi	Velkendt teknologi for signering. Mulighed for eventuelt at anvende standard off-the-shelf IMS-produkter. Kompleksiteten øges, da der introduceres et ekstra lag i arkitekturen (ikke for det offentlige, hvis NemLog-in får ny rolle). Afkobling af login-tjeneste giver mulighed for løbende tilføjelse af nye protokoller uden stort impact for tjenesteudbydere. Hurtigere og mere effektiv kommunikation mellem login-tjeneste og tjenesteudbydere (kun et token).
Modenhed	IMS-løsninger er primært rettede mod enterprise-brug og p.t. ikke udbredt i meget stor skala (dvs. med millioner af brugere).
Økonomi	Sandsynligvis største omkostninger: Adskillelse af identitetsgarant og login-funktioner vil sandsynligvis betyde øgede omkostninger på grund af øget kompleksitet og behov for koordinering og styring på tværs af leverandører. Større samlede omkostninger som følge af behov for tilpasninger hos tjenesteudbydere samt behov for etablering af to separate infrastrukturer (autentifikation og signering).

4.3.6 Sammenhæng mellem koncepter og arkitekturer med lokale signaturløsninger

Der er i alle koncepterne mulighed for fortsat at have løsninger med lokale certifikater og tilhørende private nøgler på brugerens udstyr eller på signaturservere.

En majoritet af NemID-medarbejdersignaturer består af forskellige typer af nøglefilsløsninger (herunder signaturserver), der er optimeret til den daglige konkrete anvendelse for den enkelte medarbejder. Dette giver eksempelvis mulighed for at anvende X.509 infrastrukturen mere direkte i standardprodukter som e-mail-klienter og i specialiserede X.509-baserede løsninger. Særligt sundhedssektoren har baseret sikkerheden i en række løsninger på X.509 teknologi, hvor en ændring vil give store omkostninger til omlægning.

Koncepterne 1, 2 og 3 er baseret på PKI/X.509, og det giver umiddelbar sammenhæng til lokalt opbevarede certifikater og tilhørende private nøgler baseret på samme teknologi.

Koncepterne 4 og 5 (som er IMS-baseret) har ikke PKI som grundlag, men da der skal bruges PKI-infrastruktur til signering, kan lokale certifikater og tilhørende private nøgler udstedes ved hjælp af denne infrastruktur.

Der er behov for yderligere tekniske analyser, når der er større overblik over, hvilke løsningsmodeller der foretrækkes både i nøglekortsløsningen og i løsninger med nøglefiler.

Nøglefilsløsninger til erhverv kan anskaffes og implementeres på flere måder. Enten som en del af et samlet udbud og leveret af samme leverandør som en nøglekortsløsning eller leveret som en separat leverance. Denne separate leverance kan Digitaliseringsstyrelsen have ansvaret for, eller den kan fx overlades til markedet.

RMC-ICG anbefaler, at understøttelse af modellen for nøglefiler fastholdes som en del af løsningen for virksomheder og myndigheder. RMC-ICG vurderer, at understøttelse nemmest implementeres som i den eksisterende medarbejdersignatur-løsning, hvor det på registreringstidspunktet vælges, om brugeren skal anvende nøglekort, signaturserver, nøglefil eller hardware-beskyttelse (SmartCard og USB krypto-token) eller andet.

4.3.7 Tekniske koncepter og samarbejde med privat partner

Koncepterne giver forskellige muligheder i et eventuelt samarbejde med en privat partner.

I det nuværende samarbejde med bankerne leverer Nets DanID en fælles front-end (NemID-navnet, nøglekort og applet), mens back-enden er forskellig.

Koncepterne 1, 2 og 4 lægger op til enten, at samarbejdet med en privat partner omfatter hele løsningen, eller at der fortsat samarbejdes om front-end, mens back-end er forskellig.

Koncepterne 3 og 5 åbner mulighed for, at det offentlige og partnerne samarbejder om identitetsgaranten, men at der kan vælges forskellige eller samme login-løsning.

4.4 Konklusion

Overordnet set sætter de tekniske koncepter fokus på den mulige grundlæggende arkitekturmæssige opbygning af en kommende løsning.

Koncepterne skal fungere som en teknologisk ramme for udviklingen af fremtidige scenarier i Fase 3 og er dermed ikke endelige løsningsmodeller. De skal derimod ses som et udgangspunkt for en dialog omkring udviklingen af scenarierne i Fase 3, hvor de efter behov vil blive analyseret og tilpasset.

RMC-ICG vurderer, at alle fem koncepter har et praktisk potentiale i forhold til den konkrete udformning af infrastrukturen for den fremtidige generation af NemID. Dog vurderer RMC-IMG, at koncepterne baseret på PKI-teknologi er dem, hvor omfanget af migreringstilpasninger for tjenesteudbydere vil være generelt mindre end for IMS-baserede koncepter. Dette kan have en afgørende indflydelse på den samlede økonomi for IMS-koncepterne, der skal rumme etablering af to infrastrukturer (IMS til eID og PKI til eSignering). Koncept 2 med korttidscertifikater, men også Koncept 3 med adskillelse af rollen som identitetsgaranten fra login-tjenesten, forventes at give problemer og behov for tilpasninger i forhold til lokale certifikatløsninger.

RMC-ICG vurderer, at koncepter, hvor man adskiller identitetsgaranten fra login-tjenesten (dvs. Koncept 3 og 5), både er de mest fleksible i forhold til fremtidig understøttelse af nye forretningsbehov og teknologier (protokoller, akkreditiver) og kommercielt mest åbne i forhold til eventuelle nye markedsaktører. Denne afkobling betyder dog øget behov for koordinering, styring og support - og dermed et større omkostningsniveau.

Koncepterne kan anvendes til både NemID til borgere og NemID til erhverv. Som udgangspunkt antages det, at *samme* koncept anvendes både til nøglekort basisløsningen for NemID til borgere og NemID til erhverv. For NemID til erhverv baseret på nøglefil betyder kravet om bagudkompatibilitet, at der er behov for en direkte PKI-baseret adgang til identitetsgaranten/login-

tjenesten. Derfor kan en tilgang baseret på *forskellige* teknologiske koncepter (eller kombinationer af disse) for NemID til borgere og NemID til erhverv også være en mulighed.

Koncepterne giver forskellige løsningsmuligheder i forhold til et eventuelt samarbejde med private partnere.

Koncepterne kan anvendes som beslutningsgrundlag i forbindelse med dialogen med private partnere, i kravspecifikationsfasen eller senere i tilbudsvurderings-/dialogfasen med de potentielle leverandører.

Koncepterne vil blive yderligere evalueret og eventuelt tilpasset i Fase 3 som et led i opstillingen og vurderingen af løsningsscenarierne.

5. NemID til erhverv

5.1 Baggrund

I dette kapitel analyseres de behov, der knytter sig til NemID til erhverv. Behovene knytter sig til de private virksomheders og myndigheders anvendelse af NemID i forhold til offentlige og private tjenester samt behov i forbindelse med myndighedernes anvendelse af løsningen, herunder regionernes anvendelse af NemID på sundhedsområdet.

Parallelt med denne tekniske analyse gennemføres en analyse af virksomheders behov i forhold til NemID, ligesom regionerne gennemfører en analyse af regionernes, herunder store dele af sundhedsvæsenets, behov. Disse analyser afsluttes først efter færdiggørelsen af denne rapport, og der indgår derfor kun delresultater fra disse analyser i rapporten.

5.2 Behov

Dette afsnit omhandler de behov som virksomheders og myndigheders medarbejdere og administratorer har i forhold til deres anvendelse af NemID. Afsnittet omfatter derfor ikke anvendelsen af virksomhedscertifikater (VOCES) og funktionscertifikater (FOCES), som hovedsagelig bruges til system til system kommunikation.

Erfaringerne med NemID, en lang række af høringssvarene, andre interessenttilkendegivelser og brugerundersøgelserne i Fase 1 vedrører virksomheders og myndigheders anvendelse af NemID-medarbejdersignatur.

Opsamlingen fra Fase 1 peger på et stærkt behov for at forenkle de administrative processer i forbindelse med oprettelse og vedligeholdelse af data, samtidig med at de administrative processer bør være mere brugervenlige. I tråd med dette er der også markant behov for mere brugervenlige understøttende processer til medarbejdernes generelle anvendelse af NemID.

Det er endvidere markant, at behovene i forhold til erhvervsløsningen er meget differentierede. Det knytter sig til aspekter som:

- Ejerforhold: Personligt ejede virksomheder, selskaber, foreninger, frivillige foreninger, fonde, personligt ejede mindre virksomheder
- Antallet af medarbejdere der skal have NemID: Enkeltmandsvirksomheder hvor kun ejeren selv skal have NemID, virksomheder med få NemID og virksomheder med mange NemID
- Antallet af virksomheder i fokus: En virksomhed, en gruppe af virksomheder med fælles eje eller med fælles administrator, koncerner
- Hvorvidt en virksomhed lader tredje part agere på dens vegne
- Anvendelsen: Anvendes NemID i forhold til login på webløsninger (virk.dk, sundhed.dk) eller i egne applikationer som på sundhedsområdet.

På sundhedsområdet anvendes NemID i vid udstrækning i egne applikationer, der i baggrunden kommunikerer med nationale løsninger som FMK (medicinkortet) og e-journal. Sammen med de særlige arbejdsforhold i fx sygehusene betyder det, at der fortsat er behov for en nøglefilsbaseret login- og signeringsløsning og ikke kun en nøglekortsbaseret løsning. Desuden betyder de særlige arbejdsforhold på sundhedsområdet større krav til robusthed i form af meget høj oppetid og fall-back-løsninger. Sundhedsområdet har foretaget store investeringer i nøglefilsløsningen med brug af signaturservere og lægger derfor vægt på, at den kommende løsning skal kunne implementeres med begrænsede migreringsomkostninger.

Disse aspekter gør, at virksomhederne har meget forskellige behov, samtidig med at der stilles krav om, at virksomhederne skal kunne vokse og ændre sig, uden at det får konsekvenser for anvendelsen af NemID:

- Mange virksomheder har behov for en løsning, der er identisk med som borgerløsningen, da brugssituationerne er ens. Det gælder fx virksomheder med kun én NemID-medarbejdersignatur.

- Mange virksomheder har brug for en nøglefilsløsning. Det gælder anvendelser med mange daglige login og i fx sundhedssektoren, hvor et nøglekort er upraktisk i den kliniske arbejdssituation.
- NemID-medarbejdersignatur skal kunne anvendes i relation til andre virksomheder end den er udstedt til.

Behovene dækker både NemID til login og signering. Antal af transaktioner, der genereres i forbindelse med signering, er generelt meget mindre end tilsvarende antal i forbindelse med autentificering. Inden for bestemte domæner og fagområder (som fx sundhed) er signering dog helt afgørende for at kunne understøtte den nødvendige funktionalitet af løsninger og arbejdsprocesser.

5.2.1 Anvendelsesområder

Dette afsnit beskriver virksomhedernes anvendelse i forhold til de vigtigste tjenesteudbydere.

Private virksomheder og myndigheder anvender NemID i forhold til obligatoriske offentlige virksomhedsløsninger (fx virk.dk, SKAT, NemRefusion, Digital Post etc.) til afsendelse og modtagelse af sikker e-mail samt til login i virksomhedens systemer.

Myndigheder anvender endvidere NemID i forhold til offentlige nationale løsninger (fx på sundhedsområdet).

Begge parter anvender NemID i forhold til private tjenesteudbydere (fx forsikring, Post Danmark Erhverv) og i mindre omfang til banker, som generelt har andre løsninger til login og signering end NemID.

En bredere analyse af anvendelsesområder gennemføres som en del af de tidligere nævnte analyser af virksomheders og regioners behov, herunder store dele af sundhedsvæsenet, i forhold til NemID.

5.3 Tekniske løsninger

På grundlag af ovenstående foreløbige analyser af virksomheders og myndigheders behov for anvendelse vil RMC-ICG i de følgende afsnit beskrive forskellige forbedringsmuligheder.

5.3.1 Forbedringer inden for den nuværende løsningsramme

Den nuværende løsning har flere specifikke løsninger til virksomheder:

- NemID-medarbejdersignatur med nøglekort, dvs. samme løsning som til borgere
- NemID-medarbejdersignatur med nøglefil på egen pc
- NemID-medarbejdersignatur med nøglefil på USB krypto-token/SmartCard
- Signaturserverløsning hvor en tredjeparts leverandør leverer nøglebeskyttelse.

De administrative processer inden for disse løsninger kan gøres mere brugervenlige, fx ved:

- En mere brugervenlig og målgrupperet brugergrænseflade
- Bestilling for flere CVR pr. bestilling/aftale gennem udvikling af pakker for denne brugergruppe. Pakkerne kan omfatte både vejledninger, sider med links og tilpasning af aftalesæt og regler
- At virksomhedens aftale med NemID kan underskrives af ejeren med NemID til borger, hvilket allerede eksisterer i dag for personligt ejede virksomheder.
- Lettere administration for personligt ejede virksomheder
- Bedre sammenhæng i administrationen af NemID, NemLog-in, Digital Post og andre offentlige løsninger (jf. Født digital).

Alle ovennævnte løsningsmuligheder vil kræve nærmere analyser af behov og konkrete løsningsmodeller. Digitaliseringsstyrelsen og Erhvervsstyrelsen har et samarbejde om tilpasninger af NemLog-in, så der opnås bedre og mere effektive forløb for brugerne, og disse erfaringer kan også anvendes i forhold til NemID.

5.3.2 Supplere med anvendelse af NemID til borgere i erhvervssammenhæng

SKAT har haft succes med at anvende NemID til borgere som login på SKAT's erhvervsselvbetjening for selskaber med personlig hæftelse (enkeltmandsvirksomheder). Dette kan umiddelbart lade sig gøre, da virksomheden og den fysiske person er samme juridiske person. Der er 274.000 enkeltmandsvirksomheder i Danmark. Det kan overvejes at lette administrationen væsentligt for en stor del af denne gruppe ved at udvide mulighederne for at anvende NemID til borgere i langt større omfang.

I den forbindelse er det vigtigt at have for øje, at mange erhvervsrettede løsninger fra fx KOMBIT Danmarks Statistik, ATP, Miljøstyrelsen samt Erhvervsstyrelsen er udviklet til at imødekomme virksomhedsbrugere med et medarbejdercertifikat, evt. tilføjet rettigheder fra NemLog-in brugeradministration. Fordelene ved, at enkeltmandsvirksomheder kan anvende NemID til borgere, skal sammenholdes med de omkostninger, som disse tjenesteudbydere vil have til at tilpasse deres løsninger til denne situation.

5.3.3 Supplere med anvendelse af samme NemID-medarbejdersignatur i flere virksomheder

Det er i dag muligt for virksomheder at bemyndige medarbejderne i en anden virksomhed til at udstede og administrere NemID i ens virksomhed[9]. Denne mulighed er dog ikke særlig anvendt antageligt på grund af manglende kendskab.

Det er ligeledes muligt at bemyndige medarbejdere i en anden virksomhed til at udføre andre opgaver (fuldmagt, delegering). Dette kan kun ske i forhold til de enkelte systemer. Processen for fuldmagtsafgivelse/delegering er tung, og der kan skabes mere smidige administrative løsninger ved at tilpasse reglerne og de tekniske løsninger til virksomhedernes behov.

Den ene grundlæggende løsning er fortsat at knytte en NemID-medarbejdersignatur til en konkret virksomhed og give mulighed for at agere for andre virksomheder gennem tildeling af rettigheder (fuldmagt/delegering). Det stiller krav om brugervenlige og effektive løsninger til at administrere rettigheder.

Den anden grundlæggende løsning indebærer at fjerne CVR-nummer fra medarbejdersignaturer og håndtere medarbejderens tilknytning til virksomheder gennem attributter. Det vil indebære juridiske ændringer i forhold til medarbejdersignaturen og vil kræve tekniske ændringer i login-tjenester og tjenester, der bygger på, at CVR-nummeret fremgår af medarbejdersignaturen. Løsningen kan bygge på NemID til borgere eller en særskilt NemID-medarbejdersignatur.

5.3.4 Overlade mere til markedet?

For at dække de meget forskellige behov i forhold til løsningen kan der vælges en model, hvor Digitaliseringsstyrelsen står for en basisløsning, mens de supplerende løsninger overlades til markedet. Det kan ligeledes være relevant, at etablere nogle dele af infrastrukturen separat – fx for login-tjenester. Baggrunden for dette er en antagelse om, at forskellige leverandører vil kunne tilbyde løsninger, der er målrettet forskellige segmenter i markedet og opfylder de helt specifikke behov inden for disse segmenter.

Det kan således besluttes, at Digitaliseringsstyrelsens opgave i forhold til NemID til erhverv vil være at sikre et frit og konkurrencepræget marked. Væsentlige elementer i en sådan tilgang vil være:

[9] http://www.nets.eu/dk-da/Produkter/Sikkerhed/medarbejdersignatur/Ekstern-administration/Pages/default.aspx

- Fortsat administration og ejerskab af certifikatpolitikker
- Specificering af snitflader, der sikrer homogenitet og en sammenhængende infrastruktur
- Regulering til sikring af, at organisationer kan skifte mellem forskellige leverandører uden unødige store omkostninger
- Tiltag, der minimerer initialomkostninger ved etablering af løsninger (eksempelvis skal godkendte NemID-udstedere i videst mulig omfang automatisk accepteres af samtlige tjenesteudbydere – fx gennem login-tjeneste konceptet)
- Sikring af, at der ikke findes organisationer, der ikke kan få NemID-medarbejdersignatur fra et frit marked. Dette kan ske ved udbud med krav om leverance af en basisløsning, der primært er rettet mod mindre organisationer.

RMC-ICG vurderer, at der kan være en risiko for, at der ikke vil vise sig tilstrækkeligt mange leverandører af løsninger på erhvervsområdet. Dette begrundes i markedets begrænsede størrelse og de høje initielle omkostninger for nye aktører.

5.3.5 Valg af teknisk koncept i forhold til NemID til erhverv

Der kan principielt vælges forskellige koncepter for NemID til borgere og NemID til erhverv, men hensynet til de mange virksomheder, der har fordel af samme løsning som NemID til borgere taler for, at der vælges samme koncept til nøglekortsdelen.

Den omfattende anvendelse af nøglefiler på erhvervsområdet kan understøttes i alle koncepter, men bedst i de PKI-baserede koncepter.

5.4 NemID-administratorrollen

Når en virksomhed første gang bestiller et NemID, bliver den første medarbejder i virksomheden, der bestiller en medarbejdersignatur – og som er blevet udpeget ved en aftale - virksomhedens NemID-administrator. Ofte ved medarbejderen ikke at denne får tildelt en administratorrolle i denne proces. Der er efterfølgende mulighed for at udpege flere administratorer i virksomheden. Den eller de personer i virksomheden, der er udpeget til at være NemID-administrator(-er), er underlagt Forretningsbetingelser for NemID-administrator[10].

Andre tjenester ønskede på et tidspunkt at bruge oplysninger om NemID-administratorer til egen rettighedsstyring, og der blev etableret en tjeneste hos Nets DanID (isLRA), der oplyser om, hvem i virksomheden der har denne rolle.

Denne brug af NemID-administratorrollen er juridisk set problematisk, da virksomheden kun har bemyndiget NemID-administratoren til at varetage opgaver og ansvar i henhold til de nævnte Forretningsbetingelser for NemID-administrator og ikke i forhold til andre tjenester.

Det er RMC-ICG's vurdering, at der er behov for at sikre, at tjenester ikke anvender oplysninger i NemID til at tildele rettigheder, som det fx sker i dag ved at bruge administratorrollen (gennem IsLRA) til at styre administratorrettigheder i tjenesten. Konkret anbefaler RMC-ICG, at konsekvenserne undersøges, herunder de juridiske vedr. en eventuel udfasning af isLRA, og om der er behov for at finde andre løsninger til tjenester.

[10] Fra http://www.nets.eu/dk-da/Produkter/Sikkerhed/medarbejdersignatur/Pages/default.aspx

5.5 Konklusion

Det er RMC-ICG's foreløbige vurdering, at der er behov for en vifte af løsninger til erhvervsområdet, og at virksomhederne og myndigheder har brug for at kunne anvende forskellige løsninger rettet mod forskellige målgrupper.

RMC-ICG vurderer, at der kan vælges samme tekniske koncept for basisløsningen for NemID til borgere og NemID til erhverv, og at der kan være supplerende løsninger til erhverv baseret på andre koncepter. Disse løsninger afhænger ikke af de grundlæggende arkitekturvalg, men dog af åbenhed og standardisering, der skal indarbejdes senere i processen, fx i udbudsfasen af næste generation af NemID.

Når analysen af virksomhedsområdet, der gennemføres i et samarbejde mellem Digitaliseringsstyrelsen og Erhvervsstyrelsen, og analysen af sundhedsområdet, der gennemføres i samarbejde med Regionerne, er gennemført, skal disse foreløbige konklusioner genvurderes.

6. NemLog-in og NemID

6.1 Baggrund

Spørgsmålet om det fremtidige forhold mellem NemLog-in og NemID rummer flere facetter, og nogle af disse som fx arkitektur, funktionalitet i forhold til forskellige målgrupper, håndtering af rettigheder og attributter er behandlet andre steder i denne delrapport.

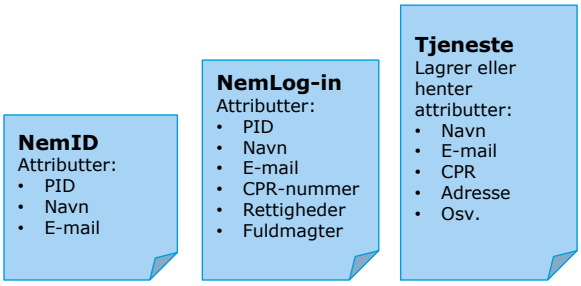
6.2 Den nuværende arkitektur

NemID's opgave er at garantere brugerens identitet i forbindelse med autentifikation og signering. Det gælder både i forhold til offentlige og private tjenesteudbydere.

NemLog-in er en fælles login-tjeneste for offentlige tjenesteudbydere og er desuden suppleret med rettighedsadministration for medarbejdere, en fuldmagtsløsning for borgere og en signeringsløsning.

NemID indeholder er minimum af informationer (attributter), mens offentlige tjenesteudbydere kan få flere attributter fra NemLog-in. Endelig kan tjenesterne selv hente yderligere attributter fra andre tjenester eller fra brugerne selv.

Figur 12: Attributter i NemID, NemLog-in og tjenester



6.3 Potentielle løsninger – fuldmagter og rettigheder

Der er som nævnt i afsnit 3.6 om fuldmagt og rettigheder behov for bedre håndtering af fuldmagter og rettigheder, og løsningen på dette indebærer bl.a. afklaring af, hvordan denne opgave løses af NemID og NemLog-in.

Teknisk set beskrives forskellige modeller for håndtering af rettighedsattributter, hvor den anbefalede model indeholder en klar adskillelse mellem løsning til autentifikation (NemID) og løsninger til rettighedsattributter (herunder NemLog-in).

Arkitekturmæssigt beskrives der i de tekniske koncepter forskellige grundlæggende modeller for, hvordan attributter kan distribueres til tjenesteudbyderne i et samspil mellem NemID og login-tjenester, herunder NemLog-in. Ud fra de valgte relationer kan grænsefladerne i det kommende NemID forberedes til ny funktionalitet, der så kan udbydes med næste NemLog-in udbud.

For på den ene side at understøtte den klare arbejdsdeling mellem NemID og NemLog-in og på den anden side yde bedre service overfor borgere, virksomheder og myndigheder, har RMC-ICG anbefalet, at der etableres et selvstændigt projekt, der dækker håndtering af fuldmagter og rettigheder i den samlede identitetsinfrastruktur.

6.4 Potentielle løsninger – andre forhold

Kapitel 5 om NemID til Erhverv beskriver behov for bedre sammenhæng i det offentliges tjenester, herunder NemID og NemLog-in. Der er allerede et samarbejde mellem Erhvervsstyrelsen og Digitaliseringsstyrelsen om et bedre samspil i administration af NemID og rettigheder i NemLog-in. Der er brug for en fortsat indsats for at skabe bedre sammenhæng for virksomheder og myndigheder.

RMC-ICG anbefaler generelt, at der sker en fortsat tæt koordinering mellem udviklingen af NemID og NemLog-in.

I forhold til målgruppen skal der vælges mellem at begrænse NemLog-in, som det er tilfældet i dag, til kun at betjene offentlige tjenesteudbydere, herunder at give brugerne single sign-on til disse tjenester. Alternativt kan NemLog-in betjene også alle eller udvalgte private tjenesteudbydere, eventuelt med single sign-on. Dette har sammenhæng med de arkitekturmæssige koncepter og med valg vedrørende håndtering af fuldmagter og rettigheder. En sådan udvidelse af målgruppen vil kræve tekniske ændringer i forhold til den forretningsmæssige afregning af private tjenesteudbydere i den eksisterende løsning eller en generel ændring i forretningsmodellen for private tjenesteudbydere.

I forhold til support kan der vælges en samlet support for NemID og NemLog-in (og måske for flere offentlige tjenester).

Der bør være en sammenhæng i servicemål for NemID og NemLog-in, da de sammen betjener offentlige selvbetjeningsløsninger, samt tjenester i sundhedsvæsenet for medarbejdere (fx adgang til sudnhed.dk).

Anskaffelse af NemID og NemLog-in kan principielt ske samlet eller delt, men i praksis betyder kontrakternes løbetider, at det ikke er muligt med en samlet anskaffelse. Det skyldes, at NemID skal udbydes med virkning fra 2017, mens NemLog-in snart skal genudbydes med virkning fra 2019.

6.5 Konklusion

Der er en række facetter i forholdet mellem NemID og NemLog-in, der kræver beslutninger i de kommende faser i arbejdet med næste generation af NemID. RMC-ICG anbefaler generelt, at der sker en fortsat tæt koordinering mellem udviklingen af NemID og NemLog-in.

Mest afgørende er fastlæggelsen af, hvilke opgaver NemID og NemLog-in skal løse i sammenhæng med de forskellige tekniske koncepters forskellige grundlæggende modeller. Desuden anbefaler RMC-ICG, at der etableres et selvstændigt projekt, der dækker håndtering af fuldmagter og rettigheder i den samlede identitetsinfrastruktur.

I Fase 3 vil dette indgå i analyser og løsningsmodeller.

7. NemID og CPR[11]

7.1 Baggrund

Dette kapitel beskriver de vigtigste sammenhænge mellem NemID og CPR.

Baggrunden er de bekymringer, der er udtrykt i høringssvarene og den offentlige debat om de sikkerhedsmæssige udfordringer, der knytter sig til anvendelsen af CPR-nummeret i forhold til NemID.

En del af kritikken af sikkerhed og privacy omhandler dog mere CPR-nummerets centrale rolle i tjenester end selve anvendelsen af CPR i relation til NemID. Således er den danske forvaltningsmodel i overvejende grad bygget op omkring CPR og CPR-nummeret, der af offentlige myndigheder anvendes som nøgle (identifikator) for personer.

I relation til NemID rejses der en kritik af, at NemID og CPR er for tæt bundet sammen, og dette analyseres i det følgende.

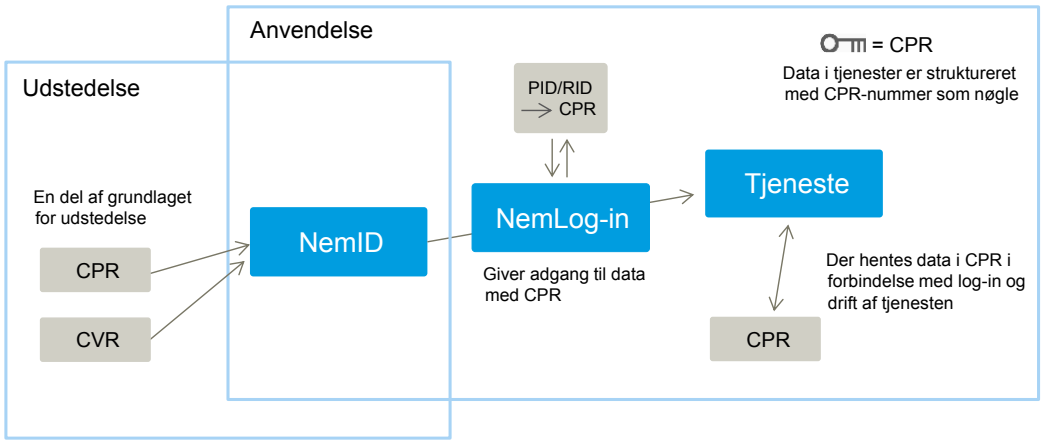
7.2 Den eksisterende løsning

I det følgende tilvejebringes et overblik over, hvordan CPR indgår i udstedelse og anvendelse i den eksisterende NemID-løsning.

Sammenhængene er overordnet set i forhold til:

- Udstedelsen af NemID, hvor data fra CPR-registret indgår som en del af registreringsgrundlaget
- Anvendelsen, hvor data fra CPR indgår i tjenester på forskellig måde. En central faktor er, at CPR-nummeret anvendes som nøgle i de fleste offentlige systemer og i nogle private tjenester.

Figur 13: Sammenhængen mellem udstedelse og anvendelse i den eksisterende løsning



CPR-data indgår kun i begrænset omfang i den eksisterende version af NemID:

[11] NemID og CVR indgår i analysen af virksomhedsområdet.

Nets DanID registrerer indehavers navn, adresse og CPR-nummer og andre oplysninger af hensyn til certifikathåndtering og forsendelse.

Det offentlige certifikat i NemID indeholder *ikke* indehaverens CPR-nummer.

I forbindelse med udstedelsen registreres indehaverens CPR-nummer i et *særskilt* PID/RID>CPR-register (der dog drives for Digitaliseringsstyrelsen af Nets DanID, der også driver NemID).

NemID anvender CPR-nummeret som default-brugernavn, og den enkelte borger har mulighed for selv at vælge et supplerende bruger-id.

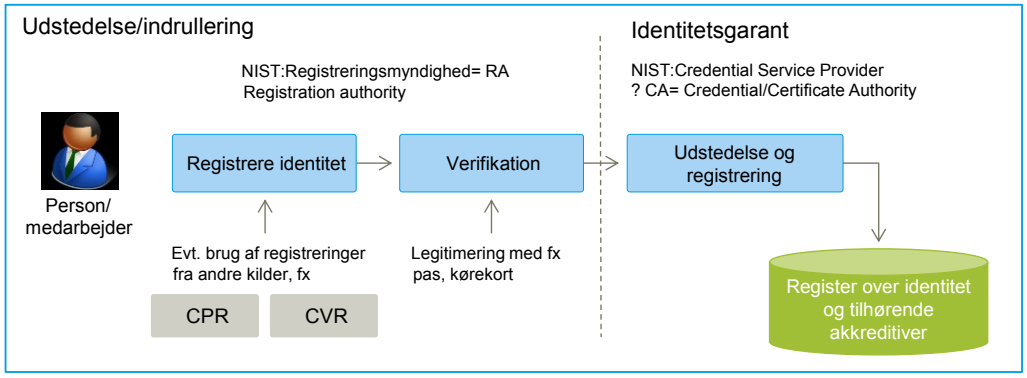
Da NemID ejes og drives af Nets DanID, er NemID underlagt CPR-lovens regler for private tjenester, idet Nets DanID er dataansvarlig. Det betyder, at Nets DanID kun må slå op i CPR efter samtykke. For brugerne betyder det, at de skal afgive samtykke, selvom de måske opfatter NemID som en offentlig tjeneste. Der er desuden udfordringer for personer med adressebeskyttelse, hvor Nets DanID ikke kan få adgang til adresseoplysninger, hvilket betyder at disse personer bliver nødt til at møde personligt frem i forbindelse med udstedelse.

7.2.1 CPR i udstedelsen af NemID

Nedenstående figur illustrerer CPR's rolle under udstedelsen af NemID for borgere og for medarbejdere samt udstedelsens vigtigste processer: registrering af identitet og verifikation (online eller ved hjælp af legitimation) samt den efterfølgende udstedelse og registrering.

Disse processer beskrives i det følgende for NemID for borgere og for NemID til erhverv.

Figur 14: CPR's rolle i udstedelse af NemID



7.2.1.1 NemID til borgere

Udstedelsen af NemID til borgere bygger på registreringen af personen i CPR (jf. Certifikatpolitik for OCES-personcertifikater, afsnit 7.3.1, Registrering af certifikatindehaver"[12]).

Desuden skal personen kunne legitimere sig i forbindelse med udstedelsen, fx med pas eller kørekort, som begge er udstedt på grundlag af registrering af personen i CPR.

[12] https://www.nemid.nu/dk-da/digital_signatur/oces-standarden/oces-certifikatpolitikker/POCES_Certifikatpolitik_version_4.pdf

En del af sikkerheden i NemID er baseret på, at nøglekort (og andre akkreditiver) sendes til personens folkeregisteradresse i CPR-register - ved online udstedelse og når der ikke er billedlegitimation.

Kvaliteten af registreringen i NemID ved disse udstedelser er afgørende afhængig af kvaliteten af registreringer i CPR. I det omfang, registreringerne i CPR kompromitteres (fx ved identitetstyveri), nedsættes troværdigheden af NemID.

Sammenhængen med CPR betyder, at kun personer med et CPR-nummer kan få udstedt et NemID i henhold til Certifikatpolitik for OCES-personcertifikater.

7.2.1.2 NemID-medarbejdersignatur

Udstedelsen af NemID-medarbejdersignatur sker på to måder:

1. Uden registrering af CPR-nummer (de fleste privatansatte og mange offentligt ansatte)
2. Med registrering af CPR-nummer (primært sundhedsområdet og professionelle brugere af tinglysningssystemet).

For medarbejderne på sundhedsområdet skal der registreres CPR-nummer, da dette anvendes i forbindelse med tildeling af rettigheder til tjenester i sundhedsvæsenet.

Da alle ansatte i Danmark skal registreres med CPR-nummer hos deres arbejdsgiver, vil det være muligt at registrere alle medarbejdere med CPR-nummer. Denne mulighed er dog aktivt blevet fravalgt ud fra privacy-hensyn, da en lang række anvendelser af medarbejdercertifikater ikke stiller krav om identificering på CPR-niveau. Desuden er der ikke krav om, at en medarbejder skal være ansat i en given virksomhed eller myndighed for, at der kan udstedes NemID. Certifikatpolitikken for OCES-medarbejdercertifikat stiller udelukkende krav om, at certifikatholder er tilknyttet organisationen.

7.2.2 CPR i anvendelse af NemID

7.2.2.1 Offentlige tjenester

Den offentlige forvaltning i Danmark er i overvejende grad bygget op omkring CPR og CPR-nummeret, der anvendes som nøgle (identifikator) for personer.

Anvendelsen af CPR-nummeret er hovedsageligt reguleret af regler i Persondataloven, Forvaltningsloven og CPR-loven, hvilket betyder, at der er begrænsninger i, hvilke data den enkelte myndighed må få adgang til og give andre adgang til – ligesom der er begrænsninger i mulighederne for samkørsel af registre.

CPR-nummeret som nøgle giver fx borgeren mulighed for at se data om sig selv gennem ”Min side” på borger.dk, hvor data samles ind udelukkende til borgeren. Der er således ikke tale om et samlet register med disse data, men data, der indsamles til og præsenteres for borgeren.

7.2.2.2 Private, der skal bruge CPR

En række private it-systemer og tjenester er pålagt at registrere personer med CPR-nummer, fx banker. Det samme gælder semioffentlige virksomheder og interesseorganisationer som forsyningsselskaber, arbejdsløshedskasser, fagforeninger mv.

For disse gælder mere eller mindre samme forhold som for offentlige tjenesteudbydere, bortset fra at opslag i CPR kræver borgerens samtykke.

7.2.2.3 Andre private

En række private virksomheder anvender CPR-nummer til entydig identifikation af borgere og som nøgle i deres it-systemer.

Enkelte private tjenester anvender CPR-nummeret som både identifikation og autentifikation, et forhold, der er sikkerhedsmæssigt problematisk, og CPR-kontoret anbefaler da også, at CPR-nummeret ikke anvendes til autentifikation, og overvejer løbende skærpelse af vilkårene for anvendelse af CPR-systemet. Senest er det besluttet, at virksomheder og myndigheder på deres

selvbetjeningsløsninger ikke må anvende personnummer som grundlag for autentifikation, men derimod NemID.

7.3 Potentielle løsninger

Da NemID som nævnt ikke indeholder CPR-nummeret, er dette forhold ikke af betydning for muligheden for at anvende løsninger fra andre lande til NemID.

Det vil også være muligt at indføre en afløser for CPR-nummeret uden ændringer i selve NemID, idet et nyt nummer kan håndteres af PID/RID>CPR-registret.

Det forhold, at NemID anvender CPR-nummeret som default bruger-id, kan give borgerne det (forkerte) indtryk, at også tjenesteudbyderne kender CPR-nummeret. Det kan overvejes at fjerne CPR-nummeret som default bruger-id, om end det kan have konsekvenser for brugervenligheden.

7.4 Konklusion

Det er RMC-ICG's anbefaling, at næste generation af NemID skal designes, så den er robust over for en udvikling med supplering eller erstatning af CPR-nummeret.

Det kan ske ved:

1. Fortsat ikke at indlejre CPR-nummer og fremtidig identifikator i NemID
2. Fortsat at have en PID/RID>CPR-tjeneste, som kan udvides til at omfatte nye identifikationer.

Den kommende NemID-løsning skal være robust over for fremtidige ændringer i CPR, også hvis CPR erstattes.

Såfremt en fremtidig NemID-løsning skal ejes af en privat virksomhed, som det er tilfældet i dag, kan det overvejes at gøre det muligt for leverandøren at slå op i CPR på bedre vilkår end i dag ved en eventuel fremtidig lov om en national identitetsinfrastruktur. Det kan mindske eller fjerne de problemer, det i dag giver, at NemID ejes af en privat virksomhed.

8. Håndtering af udenlandsk eID og udlændigeområdet generelt

Den øgede modenhed i digitaliseringen, betyder, at næste generation af NemID skal kunne fungere i forhold til digitalisering over landegrænser. Den netop vedtagne eIDAS-forordning stiller krav om gensidig anerkendelse af anmeldte nationale eID fra andre EU-lande, ligesom den opstiller en juridisk ramme for anerkendelse af tillidstjenester på tværs af grænser.

Ligeledes oplever en række tjenesteudbydere et stigende behov for at kunne betjene såvel danske borgere som udlændinge med bopæl i andre lande.

Disse aspekter analyseres i separate analyser af udlændingeområdet, der udarbejdes af Digitaliseringsstyrelsen. Analyserne vurderer hvilke krav, der er behov for at indarbejde i forhold til næste generation af NemID på baggrund af henholdsvis eIDAS-forordningen og udfordringerne vedrørende NemID for udenlandske borgere i Danmark og danske og udenlandske borgere og virksomheder i udlandet.

Konklusionerne fra de enkelte analyser vil blive indarbejdet i det endelige beslutningsgrundlag på et senere tidspunkt, således at de kan bidrage til kravsætningen for den næste løsning.

9. Migrering

9.1 Baggrund

En migreringsstrategi for næste generation af NemID skal tilrettelægge overgangen fra den nuværende til den nye NemID-løsning, således at den forløber så smertefrit og transparent som muligt - både for brugere og tjenesteudbydere.

Migreringsstrategien skal derfor bygge på entydige krav om størst mulig kontinuitet og bagudkompatibilitet på den ene side i forhold til borgere, medarbejdere og tjenesteudbydere og på den anden side i forhold til at minimere omkostningerne. Samtidigt skal kravene om kontinuitet og bagudkompatibilitet ses i forhold til de gevinster (efterspurgte funktionaliteter), som den næste generation af NemID vil kunne tilbyde.

På baggrund af ovenstående vil RMC-ICG i det følgende foretage en *indledende* vurdering af de krav til migreringsprocessen til den kommende NemID-løsning. Dette vil blive uddybet som del af analysen af de konkrete løsningsscenarier i Fase 3, hvor omfanget og implementeringstakten for de enkelte scenarier for den kommende version af NemID vil blive konkretiseret.

9.2 Migrering af brugere, borgere og medarbejdere

Migrering af brugere fra de eksisterende løsninger skal så vidt muligt etableres som en sømløs proces.

Dette krav gælder både migrering af basisløsningen for borgere (dvs. en nøglekort-baseret NemID) og basisløsninger til erhverv (nøglefil- og nøglekortbaseret) og migrering af og til de supplerende løsninger, og som vil blive leveret af andre leverandører end leverandøren af basisløsningerne.

De supplerende løsninger omfatter bl.a. nøglefilsbaserede løsninger for borgere og signaturservere, som anvendes af sundhedspersonale.

9.2.1 Basisløsninger

Da NemID-klienten effektivt afkobler slutbrugerløsninger fra den underliggende tekniske infrastruktur, vurderes migreringen af basisløsningen *ikke* at være stærkt afhængige af de bagvedliggende tekniske koncepter. Brugernes oplevelse af migreringsprocessen til en ny løsning vil være den samme, uanset hvilket teknisk koncept der ligger bag.

Dog skal det bemærkes, at brugerne vil blive berørt, hvis hovedleverandøren skiftes som konsekvens af udbudsforretningen i forbindelse med overgangen til nye akkreditiver.

9.2.2 Supplerende løsninger

Migrering af en stor del af de supplerende løsninger er ligesom migrering af basisløsninger afgørende afhængig af back-end infrastrukturen og derfor generelt mindre kompliceret og omkostningsfuldt for PKI-baserede koncepter.

Migrering af alle løsninger (både basis og supplerende) kan som det ene yderpunkt foregå *glidende* i forbindelse med brugeres generhvervelse af NemID ved dennes udløb eller – som det andet yderpunkt – *hastig* ved tvungen migrering af brugere inden for en kort periode. Valget af migreringsmodellen er bestemmende for perioden, hvor den nye og den eksisterende løsning skal fungere parallelt, og dette skal afgøres i den videre proces og i leverandørdialogen under anskaffelsesfasen.

For alle tekniske koncepter forudsætter kravet om en sømløs migrering af brugerne et meget tæt samarbejde og koordinering mellem både leverandøren af basisløsningen og eventuelle leverandører af supplerende løsninger og den nuværende leverandør.

Dette samarbejde skal bl.a. omfatte aftaler og processer for udstedelse af nye NemID-løsninger til indehavere af eksisterende NemID (for at kunne benytte den eksisterende certifikatleverandørs valideringstjeneste).

9.3 Migrering af tjenester

Etableringsprocessen for den næste generation af NemID skal understøtte (og motivere) tjenesteudbyderne til at foretage migrering til den nye løsning, samtidigt med at der sikres størst mulig bagudkompatibilitet i overgangsperioden (i relation til den *eksisterende* funktionalitet). Uafhængigt af disse præmisser er det vigtigt at understrege behovet for allokering af tilstrækkelige ressourcer til support for migrering af tjenester.

9.3.1 Bagudkompatibilitet

Det er vurderingen, at bagudkompatibiliteten er størst for de to første PKI-baserede koncepter (dvs. Koncept 1 og 2 i kapitel 4) – både for de offentlige og private tjenesteudbydere. Tjenesterne kan stort set forsætte med at anvende det certifikatbaserede login (eller anvende NemLog-in for det offentlige) - uden store ændringer i eksisterende grænseflader. Koncept 2 stiller dog større krav til migrering af lokale certifikatløsninger.

Det tredje PKI-baserede koncept (Koncept 3) lægger op til, at tjenesteudbydere anvender login-tjenester for autentifikation af brugere (eventuelt med attributter) og vil derfor på sigt kræve en større tilpasning af private tjenester og løsninger, der anvender signaturserveren. Dog giver konceptet mulighed for, at disse i en periode fortsætter med at anvende den direkte login ved hjælp af certifikater og dermed at begrænse behovet for migrering. Det afgørende for dette koncept bliver derfor, hvor lang overgangsperiode der besluttes.

Koncepter, der bygger på IMS-infrastruktur (dvs. Koncept 4 og 5 i kapitel 4), er væsentlig mindre bagudkompatible og derfor forbundet med større migreringsomkostninger, da der fx kan forekomme en længere overgangsperiode, større tilpasninger mv. Dette gør sig specifikt gældende for de fleste private tjenesteudbydere, der ikke - som det offentlige - gør brug af NemLog-in, der afskærmer offentlige tjenester fra direkte kontakt til NemID.

Anvendelse af de *nye* funktionaliteter og muligheder, fx attributter, flere sikringsniveauer og eventuelt en profil for borgere og medarbejdere, i den kommende version af NemID vil dog for alle opstillede koncepter forudsætte ændringer i forhold til de eksisterende indholdstjenester. Disse omkostninger vurderes ikke at være afhængige af de valgte koncepter, da adgang til disse funktionaliteter (attributtet, en profil) forventes at blive afkoblet fra den underliggende teknologi ved hjælp af en TU-pakke. Implementering af flere sikringsniveauer vil for alle koncepter føre til ændringer i indholdstjenesterne.

Også for tjenesternes migrering er tidsfaktoren afgørende, idet en meget lang overgangsperiode vil mindske tjenesteudbydernes omkostninger, mens en meget kort overgangsperiode modsætningsvis vil betyde større omkostninger.

9.4 Konklusion

Brugernes oplevelse af migrering af basisfunktionalitet og de økonomiske omkostninger herved forventes ikke at være afgørende afhængig af det valgte tekniske koncept for basisløsninger for borgere og for erhverv baseret på nøglekortsløsningen. Dette er under forudsætning af, at en eventuel adskillelse af eID og eSignatur implementeres fuldstændig transparent for brugerne (dvs. bliver styret af teknologien og skjult bag brugergrænsefladen). For basisløsningen for erhverv baseret på nøglefil samt supplerende løsninger, herunder signaturserver, sikrer koncepterne, der bygger på PKI-baseret back-end, den største kontinuitet i forhold til eksisterende løsninger og dermed også de mindste migreringsomkostninger.

Den samme konklusion gør sig gældende for migrering af tjenester (specifikt de private tjenester, der ikke anvender fælles login-tjeneste), hvor den største bagudkompatibilitet er for PKI-baserede koncepter. Forhold vedrørende implementeringen af nye funktionaliteter i den næste generation af

NemID skønnes ikke at være afgørende forskellig for de opstillede koncepter - der vil være behov for ændring i brugeroplevelsen i indholdstjenester ved alle koncepter.

En sømløs migrering af brugerne forudsætter, at der stilles præcise krav om samarbejde mellem både leverandøren af basisløsningen og eventuelle leverandører af supplerende løsninger, og den nuværende leverandør. Det er ligeledes afgørende at samarbejdskravene også omfatter en leverandør af den nye TU-pakke.

For en sømløs migrering er det afgørende, at tjenesteudbydere og brugere af supplerende løsninger får tilbudt en fleksibel tidsplan, hvor de ressourcekrævende og komplicerede dele af en migrering kan ske på tider, der i vid udstrækning kan vælges af tjenesteudbydere og brugere selv.

10. Samlet konklusion på delrapport for Fase 2

10.1 Samlet konklusion

10.1.1 Det tekniske grundlag

Analysen i denne fase har skabt grundlaget for en række tekniske koncepter for næste generation af NemID. Det tekniske grundlag er blevet suppleret med særskilte analyser af NemID til erhverv, det fremtidige forhold mellem NemLog-in og NemID, NemID og CPR, håndtering af udenlandsk NemID og migration.

Analysen har omfattet følgende nye tekniske elementer:

A. Adskillelse af eID og eSignatur
B. Flere sikringsniveauer
C. Kontekstafhængig information
D. Fokus på øget privacy
E. En NemID-profil
F. Fuldmagt og rettigheder

RMC-ICG vurderer, at *adskillelse af eID og eSignatur* er et vigtigt element i den næste generation af NemID og en vigtig forudsætning for nye funktionaliteter (fx mere brugervenlig login-funktionalitet med flere sikringsniveauer, kontekstafhængige information om brugere, øget privacy samt styrkelse af den juridisk forpligtende elektroniske signering). Denne adskillelse kan tilvejebringes som en funktionel adskillelse ved at anvende forskellige certifikater til eID og til signering eller som en teknologisk adskillelse, ved opbygning af separate teknologiske løsninger, hvis man vælger at basere eID på ikke-PKI-teknologier.

RMC-ICG vurderer, at der vil være en række fordele ved at understøtte *flere sikringsniveauer* i forbindelse med autentifikation i næste generation af NemID. Det vil kunne dække behov særligt i det private marked, der derved kan bidrage med en større andel af finansieringen. Løsningen bør implementeres med fokus på brugerinddragelse og brugervenlighed og vil i øvrigt kræve klassifikation af data og nødvendig tilpasning af tjenester hos den enkelte tjenesteudbyder for at give det fulde udbytte. Det kan betyde ekstra omkostninger hos de tjenesteudbydere, der har behov for at understøtte forskellige sikringsniveauer.

RMC-ICG vurderer endvidere, at der er behov for, at NemID understøtter *kontekstafhængig information* med mulighed for større brugerkontrol og indblik i, hvilke attributter der videregives til tjenesteudbyderen. I den forbindelse vurderes det at anvendelsen af kontekstafhængige attributter vil sikre en større grad af privacy for borgere og en større fleksibilitet for tjenesteudbyderne, i forhold til hvilke attributter de modtager.

RMC-ICG vurderer, at den næste generation af NemID skal have *fokus på privacy* for at sikre, at brugerne har tillid til systemet. Håndteringen af privacy kan imødekommes med forskellige tekniske løsninger – som ovenævnte kontekstafhængige attributter – leveret gennem login-tjeneste eller ved anvendelse af specialiserede autentifikationsteknologier og protokoller som fx privacy-fokuserede ABC-teknologier (U-Prove og Identity Mixer).

Etableringen af *en NemID-profil* kan løses på flere måder. En løsning i brugergrænsefladen alene (front-end baseret løsning) kan etableres uafhængigt af de underliggende arkitekturer i NemID, mens dannelse af en profil med et NemID forudsætter, at der anvendes samme tekniske koncept til borger og erhverv. Den tekniske analyse viser, at det potentielt er en omfattende og teknisk kompliceret opgave at implementere begge løsningsmodeller.

RMC-ICG vurderer, at NemID fortsat kun skal håndtere autentifikation og signering, og at *fuldmagter og rettigheder* fortsat håndteres i andre dele af den samlede eID-infrastruktur, fx i NemLog-in. Da håndtering af fuldmagter og rettigheder primært ligger i NemLog-in og ikke mindst i de enkelte tjenester, er det en selvstændig stor opgave at afdække behov og løsninger, og RMC-

ICG anbefaler, at dette løses som et selvstændigt projekt – der favner fuldmagter og rettigheder i den samlede e-identitetsinfrastruktur.

Sammenfattende kan det fra en teknisk synsvinkel konkluderes, at der er få tekniske begrænsninger og afhængigheder mellem de enkelte dele af den næste generation af NemID.

10.1.2 Tekniske koncepter

Den næste generation af NemID kan etableres med udgangspunkt i forskellige grundlæggende koncepter (arkitekturer), som ligeledes er blevet analyseret i denne rapport.

Koncepterne bygger på følgende grundlæggende antagelser i forhold til den næste generation af NemID - udover de nye tekniske elementer:

- Understøttelse af eID- og eSigneringsfunktionalitet for borgere
- Understøttelse af eID- og eSigneringsfunktionalitet for medarbejdere
- Udstilling af snitflader, der muliggør supplerende løsninger
- Understøttelse af lokale certifikater og signaturservere for større virksomheder

Analysen af koncepterne viser, at der ikke findes *ét* optimalt koncept, og at kravene om bagudkompatibilitet, minimering af omkostninger og størst muligt fleksibilitet peger på forskellige koncepter.

Hensynet til brugerne og tjenesteudbyderne trækker i retning af en kommende løsning med mange fællestræk med den nuværende løsning. RMC-ICG vurderer i den forbindelse, at to af koncepterne baseret på PKI-teknologi (Koncept 1 og delvist Koncept 3) er dem, hvor omfanget af migreringstilpasninger for tjenesteudbydere vil være generelt mindre end for IMS-baserede koncepter (Koncept 4 og 5). Den samlede økonomi for PKI-baserede løsninger vurderes dermed at være lavere end for IMS-koncepterne, der også skal rumme etablering af to infrastrukturer (IMS til eID og PKI til eSignering). Dog forventes det, at både konceptet med anvendelse af kortidscertifikater og konceptet med adskillelse af rollen som identitetsgarant fra login-tjenesten vil give problemer og behov for tilpasninger i forhold til lokale certifikatløsninger (signaturservere).

RMC-ICG vurderer, at koncepter, hvor man adskiller identitetsgaranten fra login-tjenesten (dvs. Koncept 3 og 5), både er de mest fleksible i forhold til fremtidig understøttelse af nye forretningsbehov og teknologier (protokoller, akkreditiver) og kommercielt mest åbne i forhold til eventuelle nye markedsaktører. Denne afkobling betyder dog øget behov for koordinering, styring og support - og dermed et større omkostningsniveau. Det bemærkes, at implementeringen af Koncept 3 på sigt åbner muligheden for, at man forholdsvist nemt kan skifte til Koncept 5 og anvende andre teknologier – fx privacy-fokuserede ABC-teknologier når disse er teknologisk modne til at kunne bruges til national eID-infrastruktur.

Koncepterne giver forskellige løsningsmuligheder i forhold til et eventuelt samarbejde med private partnere.

Som konsekvens af analysen af de tekniske koncepter kan det endelige valg og udformning af koncepter udsættes til leverandørvurderings-/dialogfasen med de potentielle leverandører for ikke på forhånd at låse leverandørerne til en bestemt løsningsmodel.

10.1.3 Andre analysetemaer

NemID til erhverv

Den foreløbige analyse af erhvervsområdets behov viser, at der er behov for en vifte af løsninger til erhvervsområdet, og at virksomhederne og myndigheder har brug for at kunne anvende forskellige løsninger.

Der kan vælges samme tekniske koncept for basisløsningen baseret på nøglekort for NemID til erhverv som for basisløsningen for NemID til borgere. Basisløsningen baseret på nøglefil for NemID til erhverv og løsninger baseret på signaturservere betyder dog, at der er behov for en direkte PKI-baseret adgang til identitetsgaranten/login-tjenesten. Derfor kan en tilgang, der bygger på *forskellige* teknologiske koncepter (eller deres kombination) for NemID til erhverv og NemID til borgere være en sandsynlig mulighed.

Når analysen af virksomhedsområdet, der gennemføres i et samarbejde mellem Digitaliseringsstyrelsen og Erhvervsstyrelsen og analysen af sundhedsområdet, der gennemføres i samarbejde med Regionerne, er gennemført, skal disse foreløbige konklusioner genvurderes.

I forhold til NemID til erhverv med mange forskellige løsninger og dermed forskellige tidshorisonter i forhold til udvikling, nye versioner m.m. vurderer RMC-ICG, at det er afgørende vigtigt, at de overordnede rammer for, i hvor lang tid der sikres bagudkompatibilitet, og hvornår migreringsperioden skal være afsluttet, meldes ud tidligst muligt. Dette gælder ikke mindst koncepter, hvor der forventes det største migreringsbehov (Koncept 3, 4 og 5).

NemLog-in og NemID

Der er en række facetter i forholdet mellem NemID og NemLog-in, der kræver beslutninger i de kommende faser i arbejdet med næste generation af NemID. RMC-ICG anbefaler generelt, at der sker en fortsat tæt koordinering mellem udviklingen af NemID og NemLog-in.

Mest afgørende er fastlæggelsen af, hvilke opgaver NemID og NemLog-in skal løse i sammenhæng med de forskellige tekniske koncepters forskellige grundlæggende modeller. Desuden anbefaler RMC-ICG, at der etableres et selvstændigt projekt, der dækker håndtering af fuldmagter og rettigheder i den samlede e-identitetsinfrastruktur.

I Fase 3 vil dette indgå i analyser og løsningsmodeller.

NemID og CPR

Det er RMC-ICG's anbefaling, at næste generation af NemID skal designes, så den er robust over for en udvikling med supplering eller erstatning af CPR- (og CVR-)nummeret. Det kan eksempelvis ske for POCES ved, at CPR-nummer og fremtidige personidentifikatorer, som nu, ikke indlejres i NemID. Ligesom der fortsat bør anvendes et unikt ID nummer tilknyttet NemID og en PID/RID-tjeneste, som kan udvides til at omfatte nye identifikatorer.

Såfremt en fremtidig NemID-løsning skal ejes af en privat virksomhed som nu, kan det overvejes at gøre det muligt for leverandøren at slå op i CPR på bedre vilkår end nu i en eventuel fremtidig lov om en national identitetsinfrastruktur. Det kan mindske eller fjerne de problemer det i dag giver, at NemID ejes af en privat virksomhed.

Håndtering af udenlandsk eID og udlændingeområdet generelt

Næste generation af NemID skal kunne fungere i forhold til digitalisering over landegrænser.

Den netop vedtagne eIDAS-forordning stiller krav om gensidig anerkendelse af anmeldte nationale eID fra andre EU-lande, ligesom den opstiller en juridisk ramme for anerkendelse af tillidstjenester på tværs af grænser. Ligeledes oplever en række tjenesteudbydere et stigende behov for at kunne betjene såvel danske borgere som udlændinge med bopæl i andre lande.

Disse aspekter analyseres i separate analyser af udlændingeområdet, der udarbejdes af Digitaliseringsstyrelsen separat. Konklusionerne fra de enkelte analyser vil blive indarbejdet i det endelige beslutningsgrundlag på et senere tidspunkt, således at de kan bidrage til kravsætningen for den næste løsning.

Migrering

Omkostninger og besvær med migrering skal ses i forhold til de gevinster, der opnås ved en løsning med ny funktionalitet. Denne afvejning skal ske overordnet, da gevinsterne kan falde hos andre end dem, der skal afholde omkostningerne.

Brugernes oplevelse af migrering af basisfunktionalitet og de økonomiske omkostninger herved forventes ikke at være afgørende afhængig af det valgte tekniske koncept for basisløsninger for borgere og for erhverv baseret på nøglekortsløsningen - under forudsætning af at en eventuel adskillelse af eID og eSignatur implementeres fuldstændig transparent for brugerne (dvs. bliver styret af teknologien og skjult bag brugergrænsefladen). For basisløsningen for erhverv baseret på nøglefil samt supplerende løsninger, herunder signaturserver, sikrer koncepterne, der bygger på PKI-baseret back-end, den største kontinuitet i forhold til eksisterende løsninger og dermed også de mindste migreringsomkostninger.

I forhold til tjenesteudbyderne er den største bagudkompatibilitet for PKI-baserede koncepter.

En sømløs migrering af brugerne forudsætter, at der stilles præcise krav om samarbejde mellem både leverandøren af basisløsningen, eventuelle leverandører af supplerende løsninger og den nuværende leverandør.

For en sømløs migrering er det afgørende, at tjenesteudbydere og brugere af supplerende løsninger får tilbudt en fleksibel tidsplan, hvor de ressourcekrævende og komplicerede dele af en migrering kan ske på tider, der i vid udstrækning kan vælges af tjenesteudbydere og brugere selv.

På tværs af analysetemaerne

Det er vigtigt allerede nu at sikre den nødvendige koordinering i forhold til en række systemer og projekter, herunder NemLog-in, supplerende erhvervsløsninger, udvikling og fremtidige rolle for CPR og understøttelse af udenlandske eID. Specifikt vil den næste generation af NemID have stor betydning for en række krav, der skal stilles i et udbud af den nye version af NemLog-in. Da udbud af NemLog-in kommer *efter* NemID-udbuddet, vurderer RMC-ICG, at den nødvendige teknologiske og funktionelle koordinering mellem begge infrastrukturer vil kunne blive sikret rent tidsmæssigt.

10.2 Perspektiver til Fase 3

De teknologiske koncepter er kun ét af de forhold, der vil indgå i udformningen af løsningsscenarier i Fase 3.

Afhængigt af de forretningsmæssige behov kan der lægges stor vægt på bagudkompatibilitet for at opnå, at borgere, medarbejdere og ikke mindst tjenesteudbydere får mindst muligt besvær og færrest mulige udgifter ved et skifte til næste generation NemID. Inden for rammerne af dette kan der så laves de mindre ændringer, der forbedrer løsningen.

Lægges der mere vægt på at få dækket flere moderniseringsbehov og sikre en løsning baseret på åbenhed, modularitet og fleksibilitet, vil det stille større krav til forandringer hos brugere og tjenesteudbydere og dermed større omkostninger i dette led.

Analysen i Fase 2 viser, at der teknisk set er rigtig mange muligheder, og da der er mange løsningskombinationer, skal der i Fase 3 ske en afgrænsning af de relevante løsningsmodeller for at fokusere analyserne. Der skal fx tages stilling til følgende parametre forud for opstillingen af de endelige løsningsscenarier:

A. dybden i forhold til opfyldelse af de funktionelle krav og behov (basis vs. supplerende løsninger),

B. bredden i forhold til dækning af brugere (fx unge under 15) og tjenesteudbydere (semioffentlige og private tjenesteudbydere),

De strategiske beslutninger og det økonomiske råderum vedrørende disse parametre er således en forudsætning for udformningen af realistiske scenarier i Fase 3.

I den kommende Fase 3 skal der desuden i dialog med leverandørerne ske en vurdering af, hvilke tekniske løsningsmodeller der er tilgængelige i markedet, og hvor der specifikt skal udvikles til den ønskede løsning.

10.3 Det gennemførte arbejde i Fase 2

Denne delrapport omfatter de emner, som i aftalen mellem Digitaliseringsstyrelsen og RMC-ICG er beskrevet som Fase 2-leverancer, dvs.:

- Afdækning af de teknologiske muligheder
- Analyse af sikkerhedsmæssige forhold med en selvstændig skriftlig konklusion (ikke del af den offentliggjorte rapport)
- Analyse af de markedsmæssige muligheder for at finde egnede leverandører til forskellige løsningstyper (ikke del af den offentliggjorte rapport)
- Internationale relationer
- Udformning af en eller flere løsningsarkitekturer for næste generation af NemID
- Udkast til en migrationsstrategi med det formål at sikre en vellykket overgang til den kommende løsning uden tab af brugere, uden høje tekniske barrierer og med fortsat anvendelse af dele af den eksisterende løsning, hvis dette er teknisk og økonomisk fordelagtigt (færdiggøres i Fase 3)
- Samlet konklusion vedrørende Fase 2.

Da det ikke er aftalt at indsnævre løsningsmulighederne i Fase 1 og 2 har Fase 2-rapporten lagt vægt på at afdække en bredere vifte af teknologiske løsninger end forventet ved kontraktindgåelsen. Ikke alle disse løsninger beskrives derfor lige detaljeret. Det betyder, at der fx ikke beskrives ”en migrationsstrategi”, men at der angives migreringsløsninger i forbindelse med forskellige løsningsmodeller.

For at kvalificere analyserne er der for de mest kritiske dele blevet gennemført workshops med eksterne eksperter samt eksperter fra højere læreanstalter. Desuden er der blevet afholdt en workshop for projektets følgegruppe, der er repræsenteret ved ATP, SKAT, Uni-C, Region Hovedstaden, Region Sjælland, KL, Erhvervsstyrelsen, Region Syddanmark, Region Nordjylland og Region Midtjylland.

Der er i løbet af Fase 2-processen aftalt ændringer i tidsplaner og arbejdsdeling mellem RMC-ICG og Digitaliseringsstyrelsen, der betyder, at følgende opgaver løses i Fase 3:

- Analyse af udlændinge og danske borgere i udlandet, der udarbejdes af Digitaliseringsstyrelsen
- Juridiske analyser
- Funktionsoversigten over de obligatoriske, ikke-obligatoriske og frasorterede funktionelle behov
- Leverandørdialog.

Arbejdet med business casens i Fase 2 har omfattet dataopsamling hos relevante interessenter. Der blev foretaget en analyse af tallene for at sikre, at alle tal er konsistente og kan opdeles efter ensartede kriterier, således at tallene på et senere tidspunkt kan sammenlignes med estimerede omkostninger for de valgte løsningscenarier.

For overblikkets skyld nævnes her opgaver, som løses af Digitaliseringsstyrelsen i forbindelse med foranalysen, og som kan bevirke, at Fase 2-rapporten skal revideres på et senere tidspunkt:

- Analyse af virksomhedernes behov (”Helikopteranalyse”)
- Analyse af regionernes behov.

SUPPLEMENT 1 - FLERE SIKRINGSNIVEAUER

1. STORK2's opdeling af sikringsniveauer

Gennem de senere år er der dannet en vis international konsensus for opdeling i sikringsniveauer. Eksempelvis definerer STORK2, Kantara og NIST alle fire "authentication assurance levels". I det følgende beskrives STORK2's opdeling i sikringsniveauer kort.

STORK2 opererer med en kombination af sikkerhed i to dimensioner til definering af et samlet "Quality Authentication Assurance (QAA)":

- Registration Phase: RP1, RP2, RP3, RP4 (højst)
- Electronic Authentication Phase: EA1, EA2, EA3, EA3 (højst).

RP definerer niveauerne for registrering af brugerne gående fra ingen eller meget lav verifikation til meget høj sikkerhed for brugeres identitet. POCES vurderes at ligge minimum på RP3.

EA definerer niveauerne for anvendelse gående fra ingen eller meget lav sikkerhed til meget høj sikkerhed baseret på en multifaktor løsning.

Det endelige QAA-niveau udregnes som ved følgende matrix:

Tabel 18:Matrix for udregning af QAA niveau

		Assurance level for electronic authentication phase (EA)			
		EA1	***EA2***	***EA3***	***EA4***
Assurance levels for registration phase (RP)	RP1	QAA1	QAA1	QAA1	QAA1
	RP2	QAA1	QAA2	QAA2	QAA2
	RP3	QAA1	QAA2	QAA3	QAA3
	RP4	QAA1	QAA2	QAA3	QAA4

NemLog-in

NemLog-in er en væsentlig part i den danske autentifikationsinfrastruktur for offentlige myndigheder, og derfor er det væsentligt at analysere, i hvilket omfang denne komponent understøtter brug af differentierede sikringsniveauer.

NemLog-in og de tilhørende API er allerede designet og specificeret til håndtering af fire autentifikationsniveauer gående fra level 1 (lav) til level 4 (høj) med den eksisterende NemID med 2-faktor autentifikation indplaceret som level 3. Under antagelser af, at der i en kommende NemID-løsning benyttes de fire definerede sikringsniveauer (eller en delmængde heraf), vil NemLog-in således relativt simpelt kunne håndtere differentierede sikringsniveauer inklusiv håndtering i forhold til single sign-on og step-up, hvor en bruger skal løftes i autentifikationsniveau, eksempelvis fra 1-faktor til 2-faktor autentifikation.

BILAG 2 – AUTENTIFIKATIONSTEKNOLOGIER OG PROTOKOLLER

2. Autentifikationsteknologier

I det følgende beskrives to grundlæggende mekanismer til autentifikation af brugere, der er relevante for den næste generation af NemID. Mekanismerne er en PKI-baseret autentifikation, som anvendes i NemID-infrastrukturen i dag, og en nyere metodik, der i det følgende betegnes attributbaserede autentifikation eller ABC-teknologi. "ABC"-begrebet dækker i det følgende "klassiske" attribut protokoller som SAML og OpenID Connect og privacy ABC-løsninger som U-Prove eller Identity Mixer.

2.1 PKI

Public Key-teknologi blev i Diffie og Hellman's oprindelige videnskabelige artikel "New Directions in Cryptography"[13] beskrevet som en mekanisme til nøgleudveksling og elektronisk signatur, men har efterfølgende også været anvendt i protokoller til ren autentifikation. Public Key-certifikater i standardformatet X.509v3 er statiske af natur, men kan anvendes ved dynamisk udstedelse i form af såkaldte korttidscertifikater, der anvendes i forbindelse med en session.

PKI til brug i elektronisk signatur er moden og gennemstandardiseret fra kryptografiske primitiver til applikationslag (S/MIME og PAdES). Derimod er der ikke den samme konsensus for standarder, når PKI anvendes som autentifikationsmekanismer for slutbrugere dog med visse undtagelse (fx SSL, SSH). XMLDSig tokens i NemID-regi er givetvis specificeret og implementeret meget forskelligt fra andre PKI-baserede eID-schemes.

I den eksisterende NemID-infrastruktur er autentifikation og elektronisk signatur historisk set teknisk tæt knyttet sammen. Autentifikation er grundlæggende baseret på en mekanisme, hvor brugerne "skriver under på", at de ønsker at logge ind hos en tjenesteudbyder.

PKI-baserede løsninger lægger ikke i sin grundlæggende form op til anvendelse af flere autentifikationsniveauer. Hvis dette ønskes, vil der typisk være behov for flere forskellige certifikater pr. bruger.

Grundet den høje modenhed i X.509-baserede PKI findes der er lang række produkter og udviklingsværktøjer, der understøtter teknologien. Men da PKI anvendes forskelligt på applikationslaget, vil der stadig skulle laves en væsentlig egen udvikling.

Med NemID's store udbredelse vil et skifte væk fra denne grundlæggende metodik have konsekvenser for tjenesteudbyderne. Udfordringerne i denne sammenhæng vil have begrænset indflydelse på løsninger, der ligger bag en centraliseret login-tjeneste som NemLog-in, men vil påvirke tjenesteudbydere, der anvender NemID som autentifikationsmekanisme direkte, hvilket primært er de private organisationer.

2.2 ABC-teknologi

I begyndelsen af dette årtusind blev der på internationalt plan erkendt et behov for standardiseret elektronisk identitetshåndtering med fokus på brugercentrering og privacy. Især personer som Kim Cameron og Dick Hardt har været med til at definere behovene i en åben eID-infrastruktur, og i 2011 blev en række af tankerne direkte inkluderet i den amerikanske regerings strategi for

[13] http://www-ee.stanford.edu/~hellman/publications/24.pdf

elektronisk identifikation "National Strategy for Trusted Identities in Cyberspace"[14]. De grundlæggende ideer har ligeledes influeret Storbritanniens nye eID-initiativ "Digital Assurance Programme"[15].

En af grundtankerne er, at de såkaldte attributter, som brugerne identificeres ved, er forskellige afhængigt af den valgte løsning/tjeneste. Dette svarer til situationen i den analoge verden, hvor vi er identificeret ved forskellige karakteristika afhængig af kontekst. Eksempelvis sker identifikation i forhold til offentlige myndigheder gennem CPR, mens identifikation i forbindelse med besøg på et diskotek typisk forgår ved at se, hvorvidt en person er over 18 år.

Den gennemgående ide i alle ABC-teknologier er brugen af en eller flere identitetsgaranter, som udsteder attribut-tokens, der kan anvendes til identifikation af brugeren over for en Service Provider i den givne kontekst.

Der udvikles løbende teknologier, protokoller og standarder, der specifikt er rettet mod at adressere denne type autentifikationshåndtering. Af væsentlige eksisterende mulige produkter og protokoller kan nævnes:

- SAML
- Microsoft Cardspace (discontinued)
- OpenID Connect
- IBM Identity Mixer
- Microsoft U-Prove.

Der er meget forskellige modenhedsgrader og grader af støtte fra industrien og Open Source-samfundet, men grundlæggende er alle disse teknologier baseret på kontekstafhængig information om brugerne.

Der er en række fordele ved at anvende åbne, standardiserede løsninger med bred accept fra industrien:

- Designet specifik til elektronisk autentifikation
- Indbygger forskellige grader af privacy-by-design
- Stor grad af sikkerhedsreview på specifikation
- Konsensus og vilje til at udvikle konkurrencedygtige og interoperable produkter.

Den internationale trend er således at adskille elektronisk autentifikation og elektronisk signatur. eIDAS-forordningen er det seneste eksempel på denne opdeling.

Der sker stadig udvikling og forskning inden for kontekstbaseret autentifikation. Således deltager Alexandra Instituttet i et forskningsprojekt på området kaldet ABC4Trust. Der er således risiko for, at et teknologiskift fra PKI-baseret autentifikation til ABC-teknologi vil betyde hyppigere ændringer i protokoller i infrastrukturen.

2.3 Vurdering

Samlet vurderer RMC-ICG, at den reneste løsning og den fulde udnyttelse af de nye muligheder bedst opnås gennem anvendelse af teknologier designet til håndtering af elektronisk autentifikation frem for fortsat at benytte PKI. Et teknologiskifte fra PKI-baseret autentifikation til attributbaseret

[14] http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[15] https://identityassurance.blog.gov.uk/

identifikation vil have effekt på eksisterende løsninger og vil derfor kræve en migreringsfase med information og hjælpeværktøjer. Det skal bemærkes, at konsekvenserne ved et eventuelt skifte vil vokse med udbredelsen af infrastrukturen.

Som nævnt er der forskellige modenhedsgrader af de forskellige teknologier. Ved et eventuelt skift til attributbaseret autentifikation er det derfor væsentligt, at der vælges en teknologi og protokol, der er tilpas moden og har en bred støtte i industrien for at sikre fremadrettet kontinuitet i infrastrukturen.

Forskellene på PKI- og ABC-teknologierne kan opsummeres kort i følgende tabel:

Tabel 19: Forskellene på PKI- og ABC-teknologierne

	PKI	ABC
Bagudkompatibilitet	✓	
Modenhed	Høj	Stadig under udvikling
Designet specifikt til eID		✓
Differentierede sikringsniveauer	Kræver flere certifikater pr. bruger	✓
Kontekstafhængig information om brugerne	Vil typisk kræve korttidscertifikater	Del af design
Privacy-by-design*		✓
International trend for eID		✓
Fremadrettet ”off-the-shelf” produkter	(✓)	✓

BILAG 3 – AUTENTIFIKATIONSTEKNOLOGIER OG PROTOKOLLER

3. Specifikke teknologier og produkter

Der findes en række teknologier, som giver en tjenesteudbyder identifikationsinformation om en autentificeret bruger. I det følgende vil potentielle muligheder analyseres. Det er væsentligt at bemærke, at de forskellige muligheder ikke ekskluderer hinanden. Det er således muligt at understøtte flere interfaces parallelt, hvis man ønsker større valgfrihed hos tjenesteudbyderne.

3.1 Privacy-egenskaber

De forskellige teknologier kan understøtte privacy-egenskaber. I det følgende listes mulige privacy-egenskaber, der indgår i den efterfølgende analyse.

Det skal bemærkes, at de beskrevne privacy-egenskaber er vurderet på det relevante protokolniveau. Det tages således ikke hensyn til, at identitetsudbyder (IdP), tjenesteudbyder eller andre tredjeparter får information om brugeren gennem andre mekanismer eksempelvis gennem logning af IP-adresser.

3.1.1 Untraceability by IdP

Angiver, at identitetsudbyder ikke har mulighed for at afgøre, hvor en given bruger logger ind. Fra et privacy-perspektiv kan dette være en ønskelig egenskab, men det kan samtidig være en ulempe i forbindelse med efterforskning af misbrug, hvor brugeren måske ønsker, at en central part logger anvendelsen

3.1.2 Selective disclosure

Angiver, at brugeren i forbindelse med et login kan vælge, hvilke attributter en given tjenesteudbyder kan få adgang til.

3.1.3 Unlinkability

Angiver, at to forskellige tjenesteudbydere ikke kan forbinde en given bruger, der anvender begge tjenesteudbydere ud fra identitetsattributter. Dette sikres typisk ved anvendelse af pseudonymer. Det er oplagt, at hvis der anvendes CPR eller lignende generelle ID'er som attribut for to forskellige tjenesteudbydere, vil der ikke være "unlinkability".

3.1.4 Conditional disclosure

Angiver, at en bruger som udgangspunkt er anonym hos en tjenesteudbyder, men at brugeren kan identificeres under givne forudsætninger. Dette kunne eksempelvis være en bruger, der i forhold til en online-spiludbyder er anonym, indtil der opstår mistanke om hvidvask. Herefter kan en dommer stille krav om, at brugeren identificeres til retsforfølgelse. I det efterfølgende vil "Conditional disclosure" typisk ikke være en integreret del af protokollen, men være en mulighed, som kan implementeres i en konkret anvendelse.

3.2 X.509-langtidscertifikater

Anvendelse af konventionelle certifikater kan enten ske ved, at brugeren laver en digital underskrift på et token. Men skriver så at sige under på, at man gerne vil logges ind på tjenesten. Alternativt kan man anvende en veldefineret X.509-baseret protokol med mulighed for bruger-autentifikation som eksempelvis SSL og TLS.

Teknologien er moden og velkendt, og der findes en række produkter og værktøjer, der understøtter udvikling af løsninger baseret på X.509. Udviklere bør have en vis indsigt i teknologien for at undgå typiske implementeringsfejl, som har indflydelse på sikkerheden.

Løsninger baseret på X.509-langtidscertifikater er som udgangspunkt "untraceable" for udstederen, men ved anvendelse af centralt opbevarede nøgler og ved anvendelse af tjenester som OCSP kan brugers anvendelse spores.

Brugeren har ikke mulighed for at bestemme, hvilke attributter i certifikatet som tjenesteudbyderen skal have adgang til, så ”selective disclosure” skal implementeres med et anonymt certifikat og med attributhåndtering uden for X.509-teknologien.

Det er umiddelbart muligt for tjenesteudbydere at linke brugere gennem sammenligning af de anvendte certifikater.

Med et neutralt og anonymt certifikat er det muligt at implementere ”conditional disclosure”.

3.3 X.509-korttidscertifikater

Anvendelser af certifikater, der bliver udstedt i forbindelse med anvendelse, har mange af de samme egenskaber som konventionelle certifikater, men er dog mere dynamiske og kan derfor anvendes til at sikre ”selective disclosure”.

Der findes ikke mange løsninger, som er direkte rettet mod korttidscertifikater, men løsninger, der er udviklet til langtidscertifikater bør relativt nem kunne anvendes til korttidscertifikater.

3.4 SAML

SAML er en forkortelse for Security Assertion Markup Language. Protokollen er udviklet som en XML-baseret mekanisme til at udveksle autentifikations- og autorisationsdata mellem en identitets- og en tjenesteudbyder.

SAML findes i en stabil version; SAML2.

SAML og anvendes i dag blandt andet i NemLog-in mellem NemLog-in og de offentlige sites, der anvender løsningen, som er koblet til NemLog-in. Desuden arbejdes der på europæisk plan på en fælles sammenbinding af nationale eID-infrastrukturer. Dette projekt, STORK2, er baseret på udveksling af identitetsdata gennem SAML.

Det er umiddelbart muligt at understøtte kontekstafhængige identitetsdata (attributter) og differentierede sikringsniveauer.

SAML understøtter ikke umiddelbart untraceability for IdP.

Det er muligt at understøtte ”unlinkability” mellem tjenesteudbydere ved anvendelse.

Det er muligt at implementere en løsning med ”conditional disclosure”, hvis attributterne, der videregives, ikke identificere brugeren direkte.

3.5 OpenID Connect

OpenID Connect er en autentifikationsprotokol bygget over OAuth2. Protokollen er specificeret af OpenID Foundation og erstatter OpenID 2.0.

OpenID Connect understøtter ikke untraceability for IdP. ”Selective disclosure” og “unlinkability” er integrerede elementer i protokollen, og det er muligt at implementere “conditional disclosure”.

OpenID Connect er implementeret til både at fungere i webapplikationer og native apps på mobilplatforme.

OpenID Connect har fået momentum den seneste tid. Således er en række store organisationer, herunder Microsoft, Google, PayPal, Salesforce og Deutsche Telecom i gang med at udrulle OpenID Connect-løsninger. Desuden er der implementeret understøttelse CMS’er som eksempelvis Drupal.

3.6 U-Prove og Identity Mixer

U-Prove, der er udviklet af Microsoft, og Identity Mixer, der er udviklet af IBM, er relativt nye teknologier, der er designet med meget høj fokus på privacy. Det er ikke undersøgt, i hvilket omfang brugere og markedet vil efterspørger disse udvidede privacy-egenskaber.

Som nævnt er teknologierne meget nye. Det må således forventes, at der i en årrække vil frigives væsentlige ændringer og opdateringer i specifikationerne. Desuden findes der meget få værktøjer, der understøtter teknologierne.

Både U-Prove og Identity Mixer understøtter "untraceability for IdP", "unlinkability", "selective disclosure" og "conditional disclosure".

3.7 Oversigt

I det følgende præsenteres en samlet vurdering af specifikke mulige teknologier, der kan være relevante arkitekturkoncepter i forhold til privacy-egenskaber samt produktets funktionalitet og markedsmæssige karakteristika.

3.7.1 Privacy-egenskaber

Tabel 20: Opfyldelse af privacy-egenskaber for udvalgte teknologier

	X.509 (langtid)	X.509 (korttid)	SAML	OpenID Connect	U-Prove og Identity Mixer
Untracebility	(✓)				✓
Selective disclosure		✓	✓	✓	✓
Unlinkability		✓*	✓*	✓*	✓
Conditional disclosure	✓	✓	✓	✓	✓

*) Kan linkes gennem IdP

3.7.2 Funktionalitet

Tabel 21: Produktets funktionalitet og markedsmæssige karakteristikker

	X.509 (langtid)	X.509 (korttid)	SAML	OpenID Connect	U-Prove og Identity Mixer
Udviklet primært som eID protokol			✓	✓	✓
Designet til webunderstøttelse			✓	✓	✓
Designet til native app understøttelse				✓	
Bagudkompatibilitet	✓	(✓)	✓[1]		

	X.509 (langtid)	X.509 (korttid)	SAML	OpenID Connect	U-Prove og Identity Mixer
Modenhed[2]	Høj	Medium	Høj	Høj	Lav
Softwarekrav til klient	Medium	Medium	Lav	Lav	Høj

1) Gælder kun offentlige tjenesteudbydere, der anvender NemLog-in

2) Vurdering af niveauet af stabilitet af specifikationer og den generelle markedsaccept

3.8 Konklusion

De forskellige protokoller har forskellige modenhedsgrader og funktionelle egenskaber. Derfor bør det overvejes at stille krav om understøttelse af flere protokoller.

X.509 har en række begrænsninger i forhold til ønskelig funktionalitet. X.509 som login-mekanisme bør kun videreføres, hvis man har et stort ønske om bagudkompatibilitet.

SAML har vist sig effektiv i NemLog-in og bør forsat understøttes over for offentlige tjenesteudbydere. Bør i højere grad understøtte ”selective disclosure” for løsninger, der ikke har behov for identifikation på CPR-niveau.

OpenID Connect bør med sit store momentum og simple implementering være et understøttet interface. Særligt over for private tjenesteudbydere.

U-Prove og Identity Mixer mangler modenhed, og det er uklart, i hvilket omfang markedet vil understøtter disse løsninger. Man bør dog sikre sig, at der ikke vælges modeller, der begrænser muligheden for at implementere U-Prove eller Identity Mixer interfaces på et senere tidspunkt.

Gartner Group anbefaler i en rapport (”2013 Gartner Magic Quadrant for User Authentication”) understøttelse af både SAML og OpenID Connect:

”*Undoubtedly, federation will become the norm in the midterm to long term, but it is likely that the RESTful "O-protocols" (OAuth and the nascent OpenID Connect) will be preferred by many cloud providers (OAuth now and OpenID Connect within one to three years as it matures), so user authentication vendors (and others) will need to support these in addition to SAML.”*