Næste generation NemID
Foranalyse: Oplæg til beslutninger

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

09. april 2015

Indholdsfortegnelse

Bilag

Bilag 1: Afdækning af relevant funktionalitet i den eksisterende NemID for næste generation NemID.

Bilag 2: Til Scenarie 2 – Virksomhedsområdet.

Bilag 3: Fase 1-rapport med bilag (vedlægges ikke).

Bilag 4: Fase 2-rapport med bilag (vedlægges ikke).

Bilag 5: NemID – Juridiske kontekst.

Bilag 6: NemID – Lovanalyse – gennemgang af lovgivning.

1. Ledelsesresumé

1.1 Rammer for næste generation NemID

En række forhold sætter rammen for næste generation NemID, enten i form af udefrakommende krav og begrænsninger, eller beslutninger af overordnet karakter i projektet.

Det gælder NemID's juridiske kontekst, hvor EU's forordning om elektronisk identifikation og tillidstjenester betyder en begrebsmæssig opdeling i eID og digital signering, som kan få indflydelse på næste generation NemID.

Næste generation NemID vil være bestemt af de mål og gevinster, der prioriteres for løsningen, herunder afvejninger mellem brugervenlighed, økonomi, finansieringsforhold og hensyn til sikker migrering til den ny løsning.

1.2 Scenariernes indhold

Næste generation NemID skal som den nuværende dække behovet for at administrere identiteter (for borgere og virksomheder) og autentificere[1] brugerne samt understøtte digital signering.

De overordnede forretningsmæssige behov, der er afdækket i Fase 1 og prioriteret af styregruppen med henblik på at udarbejde beslutningsgrundlag for næste generation NemID, er en meget sikker NemID-løsning, der dækker de nuværende behov, samt sikrer kontinuitet og bagudkompatibilitet for interessenterne.

Alle scenarierne har dækningen af disse overordnede behov som grundlag.

Scenarierne er opbygget efter drøftelse mellem Digitaliseringsstyrelsen og *Rambøll Management Consulting* og *Implement Consulting Group* (der i det følgende benævnes RMC-ICG), således at de løsningselementer, der er drøftet i styregruppen for NemID, er fordelt på tre scenarier og et særskilt løsningselement.

Scenarie 1 viser en løsning baseret på nuværende arkitektur og grundlæggende teknologi, med minimale ændringer i forhold til nu.

Scenarie 2 har fokus på forbedringer for borgerne (1-faktor-login) og for erhvervsområdet (brug af *NemID privat* i erhvervssammenhæng) samt bedre administrative løsninger.

Scenariet indeholder samme funktioner som nu, men med en ny arkitektur og teknologier, der muliggør flere sikkerhedsniveauer og adskillelse af autentifikation og signering – dog uden at brugerne må opleve denne opdeling.

Desuden dækkes de følgende forretningsmæssige behov, primært med fokus på at imødekomme virksomheders og myndigheders behov som arbejdsgivere:

- Bredere anvendelsesmuligheder for NemID privat til erhvervsformål.
- Bedre administrative løsninger til erhverv.

Scenarie 2 er grundlag for Scenarie 3, som yderligere indeholder dækning af følgende forretningsmæssige behov:

- Brugernes behov for øget privacy og tjenesteudbydernes behov for kontekstafhængig information.

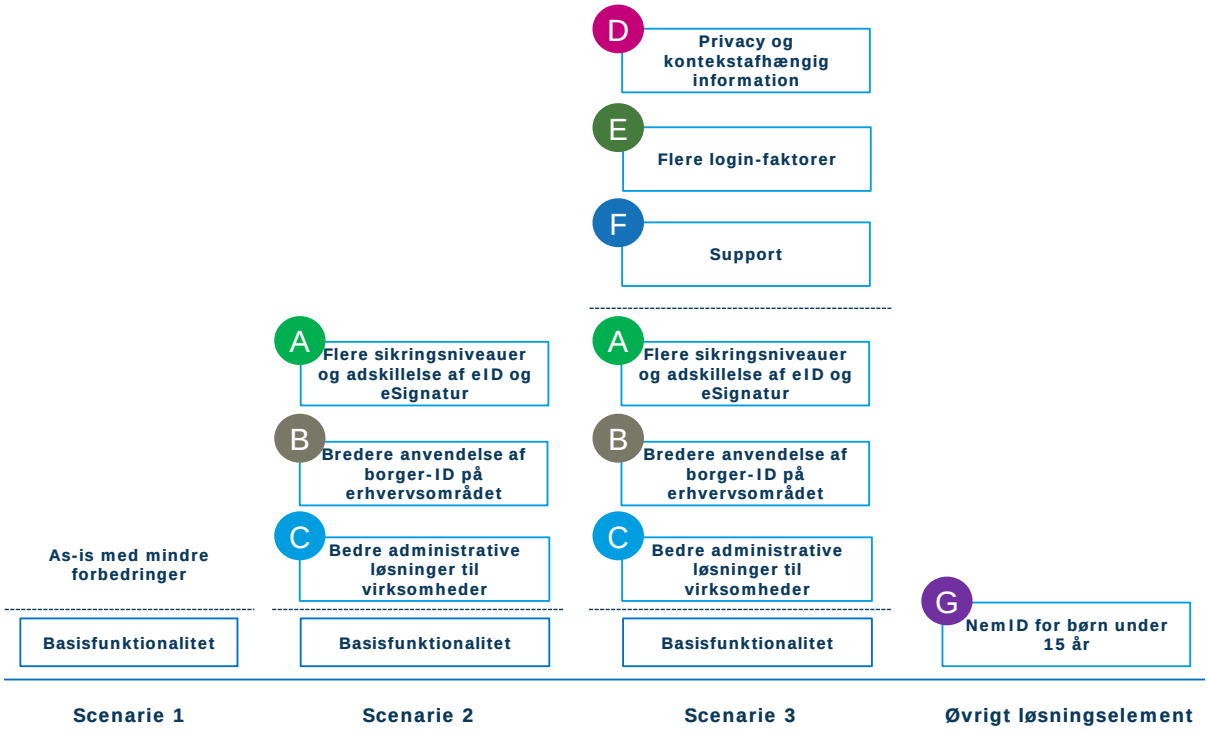
[1] At autentificere brugere vil sige at kontrollere, at brugeren er den, vedkommende udgiver sig for at være.

- Flere login-faktorer for at dække brugernes behov for flere valgmuligheder og mere brugervenlige og situationsrelevante login-faktorer.
- Bedre og billigere support primært for erhverv, men også for borgere.

Løsningselementet *NemID til børn under 15 år* er beskrevet og vurderet i afsnit 15 og indgår ikke som en del af scenarierne, da analysen har vist, at dette er for omkostningstungt i forhold til de opnåede gevinster. Desuden mangler juridiske og digitaliseringsstrategiske afklaringer.

Det vil være muligt at flytte på løsningselementerne mellem scenarierne, idet det fx er muligt at give bedre og billigere support i både Scenarie 1 og 2.

Figur 1: Oversigt over scenarierne og løsningselementerne



1.3 Grundlæggende principper og forudsætninger

Den kommende løsning skal have et højt sikkerhedsniveau og skal være brugervenlig. Det er et grundlag for alle tre scenarier.

Desuden er et fælles grundlag for alle scenarierne, at håndtering af autentificering sker med udgangspunkt i en central registrering af identitets- og login-faktorer, således at hovedparten af brugerne ikke skal installere nøglefiler, klientsoftware eller lignende på eget udstyr.

Ligeledes bygger scenarierne på central lagring af privatnøgler til signering hos leverandøren. Dette sker på grundlag af erfaringerne med digital signatur fra 2003 (OCES1) i Danmark, der viste store problemer for brugerne med at håndtere nøglefiler. Det betød negative brugeroplevelser, høje supportudgifter, og at anvendelsen blev hæmmet. Til gengæld har erfaringerne med NemID (OCES2) med central lagring af privatnøgler været en stor succes, og det har været muligt at udbrede løsningen til 90 % af den voksne befolkning.

Det er ligeledes et fælles grundlag, at virksomheder og myndigheder fortsat skal have mulighed for en nøglefilsløsning, idet de har udtrykt et meget stærkt behov for, at denne løsning fortsætter.

Desuden er scenarier og løsningselementer baseret på det grundlæggende princip, at NemID håndterer autentificering (login) og signering, mens forhold vedrørende fuldmagter og rettigheder håndteres andre steder i infrastrukturen, fx i NemLog-in.

1.4 Konklusioner om scenarierne

1.4.1 Scenarie 1

Scenarie 1 indebærer, at den nuværende løsning fortsætter med kun få ændringer. Det vil betyde en høj grad af kontinuitet og bagudkompatibilitet. Der er dog risiko for, at scenariet ikke vil imødekomme ønsker om fremtidssikring af teknologien.

Desuden vil scenariet ikke imødekomme alle behov og ønsker for forbedringer, der er indkommet i høringsfasen og i de fællesoffentlige parters arbejde med NemID.

Endelig er der også risiko for, at leverandørerne i markedet vil opfatte et udbud af 'samme løsning' som et signal om, at den nuværende leverandør foretrækkes, og det kan medføre, at færre vil byde.

1.4.2 Scenarie 2

Gevinster

Samlet set betyder Scenarie 2 mere brugervenlige løsninger for borgere og erhvervsliv. Dette i form af mulighed for 1-faktor-login, bredere muligheder for at anvende NemID privat i erhvervssammenhæng samt bedre og mere differentierede løsninger til administration af NemID i forbindelse med virksomheder og myndigheder og deres medarbejdere.

Scenarie 2 medfører øget brugervenlighed for borgerne, idet de får mulighed for en lettere anvendelse af løsningen i kraft af 1-faktor-login.

Virksomhederne vil få tilbud om en mere enkel anvendelse og dermed tidsbesparelser som følge af muligheden for at anvende NemID privat i erhvervssammenhæng.

Det er RMC-ICG's anbefaling, at der stiles efter en styret udbredelse af NemID privat til erhverv, idet det er afgørende for brugerne, at de kan vælge at anvende NemID privat i *alle* sammenhænge. Hvis blot en enkelt udbredt løsning stiller krav om NemID medarbejdersignatur, skal virksomheden have både NemID privat og NemID medarbejdersignatur.

Virksomheder og myndigheder vil få betydelig bedre administrationsmuligheder end i den nuværende løsning.

Tjenesteudbydere (både private og offentlige) vil kunne drage fordel af muligheden for 1-faktor-login, hvilket kan betyde, at der vil blive flere tjenester, der anvender NemID, og det kan gavne brugeroplevelsen.

Scenariet vil imødekomme flere af de mange krav og behov for forbedringer, der er indkommet i høringsfasen og i de fællesoffentlige parters arbejde med NemID, særligt fra virksomhedsområdet.

Udgifter

Teknisk set kan et scenarie, der giver mulighed for 1-faktor-login og adskillelse af autentifikation og signering, bygge på en bredere vifte af tilgængelige løsninger i markedet. Det vil også være attraktivt for flere leverandører at byde, og samlet set kan det efter RMC-ICG's vurdering betyde, at der kan opnås større kvalitet i løsningen, uden at det betyder øgede udgifter.

Hvor Scenarie 1 kun indebar fællesoffentlige udgifter til NemID, betyder Scenarie 2 udgifter flere steder i det samlede NemID-økosystem, som omfatter brugere, login-tjenester og tjenesteudbydere.

Set i forhold til de gevinster, der opnås for borgere og erhvervsliv i dette scenarie, i form af tidsbesparelser ved login og administration, vurderes de fællesoffentlige merudgifter (i forhold til Scenarie 1) at være begrænsede.

Her omfatter fællesoffentlige udgifter udgiften til leverandøren/leverandørerne af NemID og udgifter til bedre administrative løsninger for virksomheder og myndigheder.

Der vil derudover være udgifter til informationstjenester, der knytter NemID privat til CVR-numre.

Desuden vil understøttelse af bredere brug af NemID privat kræve, at primært offentlige tjenesteudbydere skal gennemføre ændringer for at gøre det muligt at anvende NemID privat i erhvervssammenhæng. Det gælder fx Digital Post og NemRefusion. Det skønnes, at forholdsvis få tjenesteudbydere skal gennemføre ændringer for at give mulighed for bredere anvendelse af NemID privat til erhvervsformål.

Det præcise antal vil i høj grad afhænge af, om tjenesteudbyderne selv bestemmer, om de vil understøtte anvendelse af NemID privat i erhvervssammenhæng, eller om det er et mål at sikre en styret, sammenhængende og koordineret (og dermed tvunget) anvendelse af NemID privat i erhvervssammenhæng. For virksomhedsbrugere betyder det forskellen på, om de som nu skal have to NemID eller i fremtiden kan nøjes med én.

Muligheden for, at virksomheder kan anvende NemID til borgere med en CVR-tilknytning, analyseres nærmere af Digitaliseringsstyrelsen og Erhvervsstyrelsen i andet regi. Konklusioner fra dette analysearbejde vil spille ind i det videre arbejde med genudbud af NemID.

Leverandørforhold

Et udbud af en løsning, der afviger fra den nuværende, vil gøre det mere attraktivt for andre leverandører end den nuværende leverandør. Det har dermed betydning for konkurrencesituationen og i sidste ende for den samlede pris på løsningen.

1.4.3 Scenarie 3

Gevinster

Scenarie 3 dækker de samme behov som Scenarie 2 og giver desuden mulighed for gevinster på yderligere tre områder, som uddybes herunder.

Scenariet kan betyde en styrkelse af borgernes høje tillid til løsningen i kraft af styrkelsen af privacy. For tjenesteudbyderne betyder scenariet mulighed for mere målrettet (kontekstafhængig) information om brugerne.

Desuden kan løsningen give lettere anvendelse for borgere i kraft af mulighed for flere login-faktorer. Hvilke login-faktorer, der kan komme på tale og på hvilke betingelser, vil dog først blive afklaret i forbindelse med det videre arbejde primært i kravspecificerings- og anskaffelsesfasen.

Endelig indebærer scenariet mulighed for bedre supportløsninger for borgere i sammenhæng med tiltag for øget brugervenlighed. For erhvervslivet vil der dels være bedre support, dels mulighed for adgang til billigere eller helt gratis support.

Hvor Scenarie 2 gav mulighed for gevinster i form af tidsbesparelser for borgere, virksomheder og myndigheder, betyder de yderligere elementer i Scenarie 3 gevinster i form af øget brugertilfredshed og øget tillid til løsningen.

Udgifter

Udgifterne for Scenarie 3 bygger på den samlede økonomi for Scenarie 2 med tilføjelse af udgifterne til elementerne fra Scenarie 3.

Som Scenarie 2 indebærer også Scenarie 3 fællesoffentlige udgifter samt udgifter i det øvrige økosystem. Det er ikke muligt at beregne udgifterne til login-faktorer uden at have valgt en konkret faktor.

De samlede fællesoffentlige udgifter til Scenarie 3 er væsentligt højere end for Scenarie 2, hvilket skyldes øgede nettoudgifter til bedre og billigere support. Det omfatter først og fremmest udgifter til delvist frikøb af support for erhvervslivet. Der indregnes også besparelser på supporten som følge af stærkere krav til øget brugervenlighed. Der knytter sig dog en vis usikkerhed til omfanget af support på sigt, idet supportudgifterne muligvis vil falde som følge af en øget brugervenlighed og bedre kendskab til løsningerne blandt brugerne. Da de samlede supportudgifter udgør en stor del af udgifterne til NemID, anbefaler RMC-ICG, at der sættes fokus på, hvordan supporten kan optimeres og effektiviseres.

Kontekstafhængig information og øget privacy forventes at føre til udgifter hos login-tjenester til at indhente relevant information og videresende den til tjenesterne. Det forventes dog, at de kan få indtægter fra tjenesterne for at levere dette.

Leverandørforhold

Som Scenarie 2 er Scenarie 3 en løsning, der afviger fra den nuværende både i forhold til funktionalitet, arkitektur og teknologi. Et udbud af en sådan løsning vil som nævnt gøre det mere attraktivt for andre leverandører end den nuværende leverandør og dermed have betydning for konkurrencesituationen og i sidste ende for den samlede pris på løsningen.

1.4.4 Øvrigt løsningselement – NemID til børn under 15 år

Analysen af gevinster, udgifter og ulemper ved at udbrede NemID til børn under 15 år viser, at udgifter til udvikling af specialtilpassede løsninger, samt udstedelse, drift og support, vil beløbe sig til et tocifret millionbeløb.

Det bemærkes, at de samlede udgifter skal betragtes som *merudgifter*, da de eksisterende UNI•Login og TastSelv-infrastrukturer ikke vil kunne fjernes. Denne merudgiftsbetragtning gælder i høj grad også andre tjenester, hvor det er en forventning, at eksisterende login-mekanismer i lang tid vil fungere ved siden af NemID til børn under 15 år.

Sammenfattende anbefaler RMC-ICG på nuværende tidspunkt, at NemID *ikke* udvides til også at omfatte børn under 15 år, da business-casen for det offentlige for denne udvidelse *ikke* er positiv.

1.5 Overordnede konklusioner

Analyserne peger på to grundlæggende veje for næste generation NemID: en fortsættelse af den nuværende løsningsmodel eller fornyelse.

En fortsættelse af den nuværende løsningsmodel bygger på Scenarie 1.

En fornyelse bygger på Scenarie 2 eller 3.

Valget mellem fortsættelse og fornyelse forudsætter en række beslutninger om de tekniske løsningsmodeller, men også om ønsket funktionalitet, leverandørstrategi, migrering osv.

Det har afgørende betydning, hvilke leverandører og hvor mange det lykkes at få til at deltage i det kommende udbud. Der er således risiko for, at der kun vil være én leverandør, der vil byde på opgaven, som det også var tilfældet ved sidste udbud. Det vil trække i retning af en fortsættelse af den nuværende løsningsmodel. Det har således stor betydning, at der etableres mulighed for, at andre leverandører får reel mulighed for at bidrage til den samlede løsningsportefølje.

Foranalysen viser endvidere, at beslutningerne om næste generation NemID har konsekvenser ikke kun for løsningen selv, men også andre steder i NemID-økosystemet og dermed digitaliseringen af Danmark.

Interessenternes behov og ønsker har ikke kun vedrørt selve NemID, men også anvendelsen i tjenester og forbedringer i andre dele af NemID-økosystemet, herunder ikke mindst NemLog-in. Nogle af disse behov er behandlet i denne foranalyse, mens andre, fx vedrørende fuldmagter og rettigheder, er videreformidlet til andre parter. Der foregår samtidig en tæt koordination mellem NemID-projektet og de parter, hvor andre projekter løftes.

Det forhold, at der indgår mange elementer og parter i det samlede NemID-økosystem, betyder, at gevinster som fx brugervenlighed er afhængig af, at flere parter gennemfører ændringer. Det betyder behov for at vurdere, om styringsmæssige tiltag er nødvendige for at opnå de ønskede gevinster, fx i forbindelse med udarbejdelse af ny digitaliseringsstrategi.

En samlet vurdering af udgifter og gevinster i scenarierne viser, at Scenarie 1 vil have de mindste påvirkninger på både gevinst- og udgiftssiden i det samlede økosystem. De fællesoffentlige udgif-

ter til løsningen forventes at være højere end til den nuværende løsning, da der er flere identiteter og transaktioner, end det er forudsat i den nuværende kontrakt.

Scenarie 2 vil betyde et mindre tocifret millionbeløb i fællesoffentlig merudgift, mens der vil være gevinster i form af sparet tid for erhvervslivet og borgerne.

Scenarie 3 vil betyde fællesoffentlige merudgifter til især frikøb af erhvervssupport. Gevinsterne vil primært være større brugertilfredshed og tillid til løsningen.

2. Introduktion til analysen

2.1 Indledning og formål

Analysen af næste generation NemID og nærværende rapport er udarbejdet af Rambøll Management Consulting og Implement Consulting Group (RMC-ICG) for og i tæt samarbejde med Digitaliseringsstyrelsen.

Baggrunden for analysen er, at der skal genudbydes og implementeres en ny NemID-løsning, idet kontrakten for den eksisterende løsning udløber i november 2017.

Formålet med analysen er at bistå de fællesoffentlige parter med at forberede et beslutningsgrundlag forud for anskaffelsen af næste generation af den nationale infrastruktur for e-identitet og digital signatur (næste generation NemID).

Denne rapport beskriver først rammerne for næste generation NemID og derefter tre løsningsscenarier og et tilhørende øvrigt løsningselement, der vurderes på baggrund af analyserne udført i projektets Fase 1 og Fase 2.

2.2 Rapportens opbygning

Rapporten består overordnet set af fire dele, jf. nedenstående samt Figur 2:

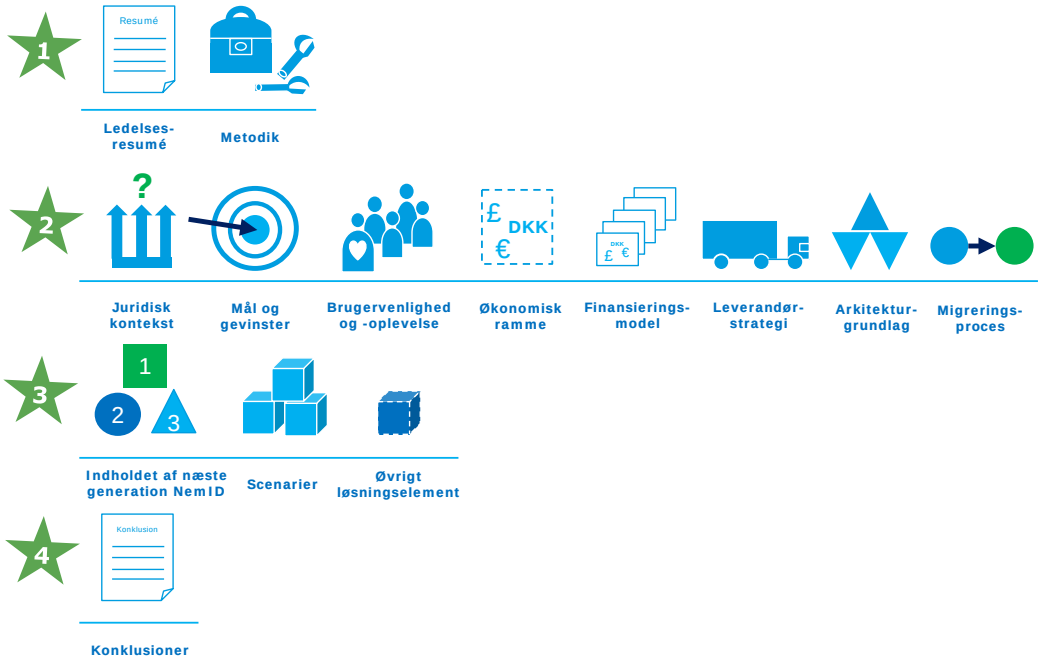
Del I (kapitel 1-2) indeholder ledelsesresumé og præsenterer foranalysen og dens metodik.

Del II (kapitel 3-10) redegør for de forhold, der sætter rammen for næste generation NemID, enten i form af udefrakommende krav og begrænsninger eller beslutninger af overordnet karakter, som styregruppen måtte træffe.

Del III (kapitel 11-15) beskriver tre scenarier og tilhørende løsningselementer for næste generation NemID.

Del IV (kapitel 16) består af de overordnede vurderinger og konklusioner.

Figur 2: Oversigt over rapportens elementer



Mere specifikt har rapporten følgende opbygning:

Kapitel 1: Ledelsesresumé

Kapitel 2: Introduktion til analysen og dens metodik, herunder proces, data, afgrænsning og begrebsafklaring

Kapitel 3: NemID's juridiske kontekst

Kapitel 4: Mål og gevinster

Kapitel 5: Brugervenlighed og brugeroplevelse

Kapitel 6: Økonomisk ramme

Kapitel 7: Forretningsmodeller

Kapitel 8: Leverandørstrategi

Kapitel 9: Arkitekturgrundlag

Kapitel 10: Migreringsproces

Kapitel 11: Indholdet af næste generation NemID

Kapitel 12: Scenarie 1

Kapitel 13: Scenarie 2

Kapitel 14: Scenarie 3

Kapitel 15: Øvrigt løsningselement

Kapitel 16: Overordnede konklusioner

2.3 Grundlag for foranalysen

Foranalysen har til formål at udarbejde scenarier og løsningselementer, der skal danne udgangspunkt for den efterfølgende beslutningsproces og anskaffelsesforløb for den næste generation NemID.

Fase 1 og Fase 2 er helt centrale grundlag i forhold til foranalysen, jf. nedenstående Figur 3. Desuden har RMC-ICG og Digitaliseringsstyrelsen gennemført en teknisk dialog med virksomheder vedrørende næste generation NemID. Denne dialog giver væsentlige input til foranalysen.

De følgende afsnit opsummerer de input fra Fase 1 og Fase 2, som indgår i analysearbejdet i foranalysen.

Figur 3: Grundlaget for foranalysen

2.3.1 Fase 1 – Brugerne

I Fase 1 blev der gennemført analyser af interessenternes behov og ønsker i forhold til næste generation NemID.

Resultatet af interessentanalysen var kortlægning af en række ønsker og behov, hvoraf der hersker udbredt enighed blandt interessenterne om nogle, mens der er divergerende meninger om andre. Endelig er der ønsker, der er fremkommet som kreative ideer i brugeranalysen, og som kan fungere som inspiration til det videre arbejde.

De registrerede ønsker og behov er:

Sikkerhed. Alle interessenter lægger stor vægt på sikkerheden i udstedelsen og anvendelsen af NemID.

Brugervenlighed. De adspurgte brugergrupper lægger stor vægt på brugervenlighed og ønsker, at tilgængelighed skal være en del af løsningens design. Virksomheder og erhvervsorganisationer ønsker en forenkling af oprettelse og anvendelse af NemID.

Behov for differentierede løsninger til virksomheder og myndigheder. Virksomheder og myndigheder ønsker løsninger, der tager højde for de meget forskellige behov i forhold til organisationernes størrelse og anvendelse af NemID.

En sammenhængende og fremtidssikret it-arkitektur. Fremtidens NemID ønskes baseret på åbne standarder samt en fleksibel og modulær løsning, der kan integreres med andre systemer.

Adskillelse af digital autentifikation (login) og digital signatur. Nogle interessenter ønsker adskillelse af eID (autentifikation) og digital signatur (signering). Dette antages at styrke sikkerheden og skabe grundlag for øget konkurrence. Andre interessenter ser en risiko for, at en adskillelse skaber kompleksitet for it-svage brugere.

Rettighedshåndtering. Mange interessenter ønsker bedre håndtering af rettigheder og fuldmagt i næste generation NemID.

NemID som brugerprofil. Nogle interessenter ønsker, at NemID indeholder en brugerprofil med forskellige identiteter. Andre har betænkelighed ved at lade den private identitet og medarbejderidentiteten smelte sammen i en enkelt profil.

Virksomhedspakker. Det ønskes, at der tages hensyn til forskellige virksomhedstypers særlige behov i forbindelse med oprettelse og administration af NemID medarbejdersignatur.

Fleksibilitet. Der er ønsker om fleksibilitet i antallet og arten af attributter tilknyttet NemID (fx navn og adresse), blandt andet af hensyn til privatlivets fred (privacy).

2.3.2 Fase 2 – Teknikken

Fase 2 fokuserede på relevante it-teknologiske løsningsmodeller, både grundlæggende løsningsmodeller i form af tekniske koncepter og løsningsmuligheder for flere af den samlede løsnings delkomponenter.

Den tekniske analyse tog udgangspunkt i de identificerede behov og ønsker fra Fase 1. De vigtigste konklusioner opsummeres i det nedenstående:

I Fase 2-analysen blev det konkluderet, at **adskillelse af autentifikation og signering** er en vigtig forudsætning for nye funktionaliteter, fx mere brugervenlig login-funktionalitet med flere sikringsniveauer, kontekstafhængig information om brugere og øget privacy. Ud fra et teknisk perspektiv er dette muligt at implementere.

Der er en række fordele ved, at næste generation NemID understøtter **flere sikringsniveauer** ved autentifikation. Det er dog en teknisk samt juridisk forudsætning, at der foretages en klassifikation af data og en nødvendig tilpasning af tjenester hos den enkelte tjenesteudbyder for at sikre fuldt udbytte. Konsekvensen af dette er, at tjenesteudbydere med behov for at understøtte forskellige sikkerhedsniveauer får ekstra udgifter. Til gengæld må det dog forventes, at det vil tiltrække nye tjenesteudbydere, der således kan bidrage til finansieringen af NemID-infrastrukturen.

Den næste NemID-løsning bør baseres på teknologi, der som den nuværende NemID **ikke kræver særlig software installeret** på brugerens udstyr (fx kræver den eksisterende nøglekortsløsning ikke særlige drivere eller software).

For næste generation NemID skal det desuden overvejes at understøtte mere målrettet information om brugeren til tjenesteudbyder ved login – **kontekstafhængig information**. Det betyder, at mindst mulig information videresendes til tjenesteudbyder, at brugerne får større kontrol over egne data og eventuelt får indblik i, hvilke informationer der videregives til tjenesteudbyderen. Dette vil øge muligheden for god privatlivsbeskyttelse (privacy) for borgere og større fleksibilitet for tjenesteudbydere i forhold til, hvilke informationer de modtager.

Fokus på **privacy** i næste generation NemID kan sikre brugertillid til systemet. Privacy kan ud fra et teknisk perspektiv leveres gennem en broker (login-tjeneste) eller ved at anvende specialiserede autentifikationsteknologier og protokoller.

Etableringen af **en NemID-profil** kan teknisk implementeres alene i brugergrænsefladen (front-end/'glasplade'-baseret løsning) og dermed uafhængig af de underliggende arkitekturer i NemID. Derimod forudsætter dannelsen af en profil med ét NemID pr. person (hvor NemID kan bruges til rollen som borger og rollen som medarbejder), at der anvendes samme tekniske koncept til borger- og erhvervsløsninger. Den tekniske analyse viser, at det potentielt er en omfattende og teknisk kompliceret opgave at implementere begge løsningsmodeller.

Fuldmagter og rettigheder i næste generation NemID foreslås fortsat håndteret i andre dele af den samlede nationale eID-infrastruktur såsom NemLog-in. Det skyldes, at det er en stor opgave at afdække behov og løsninger, hvorfor dette bør adresseres i et selvstændigt projekt.

Sammenfattende kan det fra en teknisk synsvinkel konkluderes, at der er få tekniske begrænsninger og afhængigheder mellem de enkelte dele af næste generation NemID. En afgørende begrænsning er dog hensynet til bagudkompatibilitet i forhold til brugere og tjenester.

2.3.3 Teknisk dialog – Leverandørerne

Der har været gennemført teknisk dialog med ni danske og internationale leverandører. Dialogen har været gennemført på en måde, der sikrer en overholdelse af udbudsretslige regler og retningslinjer for afholdelse af teknisk dialog. Hovedpointerne fra dialogen er samlet i det følgende:

2.3.3.1 Udbud og udbudsproces

Centralt for de virksomheder, der deltog i den tekniske dialog, var et ønske om størst mulig grad af gennemsigtighed i udbudsprocessen i forhold til kontraktforhandlingerne, forretningsmodellen og de juridiske regler.

Dialogen viste tydeligt, at der så vidt muligt bør skabes incitamenter for nye tilbudsgivere til at deltage i et kommende udbud. Det væsentligste incitament for deltagelse vurderes at være en bevidsthed i markedet om, at der er etableret en åben konkurrence, som størstedelen af leverandører har mulighed for at vinde. Dette kan fx styres ved en opdeling af ydelsen i separate dele, der kan bydes på individuelt. Herudover vil der fx være mulighed for at kompensere for leverandørers deltagelse i et udbud, fx ved at betale leverandørerne for afgivelse af et endeligt tilbud efter deltagelse i en konkurrencepræget dialog.

2.3.3.2 Sikkerhed

Leverandørerne kan levere løsninger med den ønskede sikkerhed og løsninger med høj sikkerhed, uden at løsningen er baseret på certifikater til brugere.

2.3.3.3 Identifikation og autentifikation

Enkelte virksomheder viste interessere for at tilbyde enten en autentifikations- eller signeringsløsning. For at dette kan lade sig gøre, skal den eksisterende NemID-løsning adskilles i separat autentifikation og signering.

Alternativt skal leverandører gå sammen i konsortier eller fungere som komponentleverandører til en hovedleverandør.

2.3.3.4 Funktionalitet

På især erhvervsområdet påpegede flere virksomheder et behov for at operere med flere brugersegmenter, fx enkeltmandsvirksomheder, mellemstore virksomheder og meget store virksomheder. Der kunne også være mulighed for at skelne mellem forskellige juridiske typer af virksomheder som foreninger, udenlandske virksomheder eller aktieselskaber. Det skal give mulighed for at tilpasse løsningen til brugernes behov.

Derudover blev muligheden for at levere flere login-faktorer, herunder SMS, biometri m.m., drøftet. Det blev anbefalet, at en kommende løsning som minimum er åben nok til, at der kan leveres flere login-faktorer, når teknologien er moden.

2.3.3.5 Brugervenlighed

Dette område var af væsentlig betydning for alle leverandører. Alle virksomheder påpegede, at de har løsninger, der kan give brugeren en god brugeroplevelse.

Flere virksomheder fremhævede desuden en stor erfaring med at levere løsninger tilpasset borgere med særlige behov.

2.3.3.6 Signering

Dette område blev drøftet i forbindelse med muligheden for at levere flere sikkerhedsniveauer eller adskille autentifikation og signering. En adskillelse skal give brugeren mulighed for at anvende sit eID uden signering og give flere leverandører mulighed for at levere en autentifikations- eller en signeringsløsning.

En enkelt virksomhed beskrev en løsning, hvori der indgik en online-signeringsplatform, der kan erstatte eller supplere den eksisterende løsning.

2.3.4 Proces og data

Grundlaget for foranalysen er den viden, der er indsamlet og opbygget i Fase 1 og Fase 2, jf. nedenstående Figur 4.

Desuden har den tekniske dialog med leverandørerne også tilvejebragt information til foranalyse-arbejdet, ligesom eksterne eksperter løbende har været involveret. RMC-ICG har undervejs i hele processen haft tæt dialog og sparring med Digitaliseringsstyrelsen og styrelsens eksperter.

Digitaliseringsstyrelsen har ligeledes inddraget eksterne eksperter, der har reviewet udkast til denne foranalyse, og deres kommentarer er indarbejdet. De eksterne eksperter er fra Alexandra Instituttet, Danmarks Tekniske Universitet – Center for Cybersikkerhed samt Oslo Universitet.

Derudover har projektets følgegruppe, der er repræsenteret ved ATP, Styrelsen for IT og Læring (tidligere Uni-C), Danske Regioner, SKAT, Kommunernes Landsforening (KL), Erhvervsstyrelsen, Nationalt Sundheds-it og Region Midtjylland været involveret gennem flere workshops og møder.

Foranalysens datagrundlag illustreres af Figur 4.

Figur 4: Datagrundlaget for foranalysen

2.3.5 Afgrænsning

Foranalysen har som formål at danne beslutningsgrundlag for næste generation NemID, og det betyder, at der er lagt vægt på at analysere forhold, der har den største betydning for beslutningstagere i denne fase.

Interessenterne har desuden bidraget med meget input, der i højere grad har betydning for udformningen af udbudsmateriale (konkrete krav til løsningens udformning) eller implementering og drift af den kommende løsning (fx krav til oppetid). Disse bidrag indgår i det samlede baggrundsmateriale, som Digitaliseringsstyrelsen kan anvende i det videre arbejde.

En række forhold vil således kræve yderligere analyser i forbindelse med de kommende faser, når der er truffet beslutninger om den kommende løsnings indhold.

2.3.6 Begrebsafklaring/ordforklaring

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

- Autentifikation og signering benyttes om de to anvendelser af NemID. Begreberne anvendes som udtryk for ”elektronisk identifikation” og ”elektronisk signatur” fra EU’s eIDAS-forordning (Electronic Identification and Signature).
- Identitet – elektronisk eller digital identitet – anvendes om den digitale repræsentation af en person eller virksomhed. Dette svarer til eID.
- Autentifikation anvendes om den proces, hvor det gennem kontrol af personens login-faktorer (akkreditiver) sikres, at personen/virksomheden er den, vedkommende udgiver sig for at være.
- Signatur anvendes som udgangspunkt om en avanceret elektronisk signatur som defineret i eIDAS-forordningens artikel 3, styk 11.
- For de engelske begreber ”Level of assurance” og ”Assurance level” anvendes begrebet ”autentitetssikringsniveau” eller den korte form ”sikringsniveau” svarende til den danske oversættelse fra eIDAS-forordningen. Ofte anvendes ordet ”sikkerhedsniveau”.

Tabel 1: Generelle begreber om nuværende og næste generation NemID

Begreb	Bruges til/hvorfor
NemID	Bruges både om den nuværende og kommende/næste generation NemID, uanset navnet på en kommende NemID-løsning.
NemID medarbejdersignatur	Bruges både om den nuværende og kommende NemID medarbejder-signatur, uanset om en kommende løsning kun omfatter eID eller både autentifikation og signering.
NemID til erhverv	Bruges om de løsninger, der omfatter virksomheder bredt, dvs. MO-CES, VOCES, FOCES osv. MOCES= medarbejderOCES. VOCES=virksomhedsOCES. FOCES= funktionsOCES. OCES= Offentlige certifikater til elektroniske services.
NemID privat	Bruges om de løsninger, der retter sig specifikt til private borgere.

Tabel 2: Tekniske begreber om nuværende og næste generation NemID

Begreb	Bruges til/hvorfor
Akkreditiver Login-faktorer	Repræsentation af en identitet. Eksempel: Et akkreditiv/en login-faktor kan være et brugernavn, et brugernavn og adgangskode, en PIN-kode, et SmartCard, et token, et fingeraftryk, et pas osv.
Nøglefil	Angiver en af de specifikke løsninger for NemID til erhverv, hvor certi-fikat og tilhørende private nøgle gemmes i en fil beskyttet med bruge-rens 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 kommerciel central løsning valgt af kunden. 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 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 angi-ver lav kvalitet, 4 høj kvalitet. Begreb i STORK2.
Autentifikationsniveau	Angiver sikkerheden ved login (autentifikation), hvor 1 angiver lav sikkerhed, 4 høj sikkerhed (fx brug af flere login-faktorer). Begreb i STORK2.
Sikringsniveau Autentitetssikringsniveau	Teknisk betegnelse i eIDAS-forordningen for den samlede vurdering af registrering, validering af identitet, udstedelse, udlevering, autentifika-tion og håndtering af sikkerhed i løsningen. Ofte blot omtalt som sik-kerhedsniveau. 1 angiver lav sikkerhed, 4 høj sikkerhed. Assurance Level anvendes i eIDAS-forordningen og NemLog-in. I STORK2 anvendes ”Quality Authentication Assurance (QAA)”.

Tabel 3: Begreber i mulige tekniske koncepter

Begreb	Forklaring
Identitetsgarant	Den organisation, der udsteder login-faktorer (akkreditiver) og på

Begreb	Forklaring
	anmodning (ved login) garanterer, med et givent sikringsniveau, at de fremviste akkreditiver tilhører den entitet, de er udstedt til. Credential Service Provider eller Certificate Authority kan varetage rollen som identitetsgarant.
Login-tjeneste Broker	De tjenester, der indestår for brugeres identitet over for tjenesteudbydere og herunder leverer identitetsrelaterede informationer.
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	Bruges til/hvorfor
eIDAS-forordning	Europa-Parlamentets og Rådets Forordning (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.
Den kommende persondataforordning	Der arbejdes på en persondataforordning i EU. Indholdet er p.t. ikke fastlagt endeligt.
STORK 2	Secure idenTity acrOss boRders linKed 2.0. Et EU-projekt, der har til formål at skabe et fælles elektronisk identifikations- og autentifikationsområde.

3. NemID's juridiske kontekst

Grundet den store udbredelse af NemID og den strategiske betydning af NemID-infrastrukturen er det væsentligt, at de juridiske rammer er klare og veldefinerede. I dette afsnit foretages en kort gennemgang af de væsentligste juridiske forhold, der har relevans for infrastrukturen, herunder lovgivning, sikkerhedsmæssige forhold samt retsvirkninger.

Som bilag til rapporten er vedlagt en mere detaljeret redegørelse, der også rummer henvisninger til relevante kilder (Bilag 5: NemID – Juridiske kontekst).

Der eksisterer ikke gældende lovgivning, der regulerer NemID og den underliggende OCES-standard[2]. Fx adresserer Lov om elektroniske signaturer en specifik type digital signatur (kvalificerede signaturer) og ikke andre (ikke kvalificerede, men avancerede) digitale signaturer som fx NemID. Den i 2014 vedtagne forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner mv. indeholder derimod en vis regulering af såkaldte "ikke-kvalificerede" tillidstjenester, der vil omfatte NemID (den offentlige digitale signatur). Som en markant nyskabelse introducerer forordningen krav om anerkendelse af eID på tværs af grænser. Det vurderes, at næste generation NemID skal kunne opfylde forordningens krav til anmeldelse som nationalt eID til Europa-Kommissionen og således skal kunne anvendes på tværs af Europas grænser.

NemID skal også fremover dække behovet for en løsning til log-in (autentifikation) til internetbaserede tjenester, både i den offentlige og private sektor. Den private sektor omfatter i høj grad, men ikke udelukkende, den finansielle sektor. NemID skal desuden i relevante tjenester løse behovet for digital signering. Fx udgør NemID i dag en forudsætning for gennemførelse af digital tinglysning.

Der er ingen direkte lovgivningsmæssige forpligtelser for borgere og virksomheder til at erhverve NemID. Som følge af lovgivningen om obligatorisk digital kommunikation med det offentlige, herunder obligatorisk Digital Post og obligatorisk digital selvbetjening, er NemID dog i praksis obligatorisk at anvende for alle med bopæl i Danmark, som kan få NemID. Der er i lovgivningen fastlagt visse muligheder for at undtage borgere fra forpligtelsen til at kommunikere digitalt med det offentlige. Den enkelte borger skal søge om sådanne undtagelser. Digitaliseringsstyrelsen undersøger i øjeblikket, om der er behov for yderligere lovgivning på området.

Digital signatur-infrastrukturen er adresseret i en lang række love, hvilket betyder, at en ændring af NemID eller den underliggende OCES-standard kan forudsætte ændringer heri. Det må bero på en nærmere vurdering af de enkelte lovbestemmelser, i hvilket omfang der alene eksisterer et behov for at sikre autentifikation (der kan etableres uden digital signatur), og i hvilket omfang der ligeledes er behov for en underskrift, der kan sikre integritet og uafviselighed (forudsætter en digital signatur).

Da NemID giver borgerne adgang til fortrolige data om sig selv, er anvendelsen af og sikkerheden i NemID i høj grad underlagt bestemmelserne i Persondataloven og Datatilsynets bekendtgørelser, vejledninger og afgørelser, som stiller krav til niveauet af sikkerhed for adgang til og transport af persondata via det åbne internet.

Dansk offentlig forvaltning er tæt bundet op på registreringer baseret på CPR-nummeret. Udstedelse af NemID baseres blandt andet på indhentning af oplysninger fra CPR-registret, som bidrager til validering af brugerens identitet. Selvom NemID rent teknisk ikke indeholder et CPR-nummer (men kun navn, e-mail og et teknisk løbenummer kaldet PID), etableres der i praksis ved udstedelsen af NemID en tæt sammenhæng mellem CPR og NemID. Tilsvarende er tilfældet for

[2] OCES = Offentlige Certifikater til Elektronisk Service.

udstedelse af NemID til virksomheder, som er baseret på CVR-registeret, og hvor certifikatet indeholder virksomhedens CVR-nummer.

NemID kan anvendes både i privat og erhvervsmæssig sammenhæng. NemID privat kan i dag med få undtagelser for enkeltmandsvirksomheder alene anvendes til private formål. Datatilsynet har indtil nu forholdt sig skeptisk over for en generel anvendelse af NemID privat i erhvervsmæssige sammenhænge, særligt i forhold til adgang til virksomhedens fortrolige og følsomme oplysninger, der må forudsætte tilstedeværelsen af et virksomhedskontrolleret login.

I perioden 2000 til 2010 har der, i regi af Justitsministeriet, været gennemført et større analysearbejde for at afklare de juridiske rammer for anvendelse af digitale signaturer. På baggrund af Justitsministeriets delbetænkning om e-signatur og formkrav i lovgivningen fra 2000 har der været stort fokus på at fjerne formkrav i lovgivningen, der forhindrer anvendelse af digital kommunikation. Betænkningen resulterede i et krav om, at alle ministerområder gennemgik lovgivningen under eget ressort med henblik på at fjerne unødige formkrav. Betænkningen vurderes ligeledes at have sikret et efterfølgende fokus på området, således at ny lovgivning ikke indeholder unødige formkrav.

Efterfølgende har Justitsministeriet i 2004 afgivet en betænkning om e-signaturs retsvirkninger, hvori det blev fastslået, at retsvirkningerne af en digital signatur ikke adskiller sig fra retsvirkningerne af en traditionel underskrift. Endelig afgav Justitsministeriet i 2010 en afsluttende beretning om elektronisk aftaleindgåelse og handel, hvori det konkluderes, at gældende aftaleretlige regler giver domstolene et tilstrækkeligt grundlag for på tilfredsstillende måde at løse de spørgsmål, som elektronisk aftaleindgåelse og handel giver anledning til.

Samlet betyder dette, at digital signatur bør behandles som en traditionel papirbaseret underskrift, og at anvendelsen af dansk rets almindelige formueretslige regler og principper fører til tilfredsstillende resultater i relation til digitale signaturer, hvilket var baggrunden for Justitsministeriets konklusioner i ovennævnte beretning. Af det gennemførte arbejde følger det således, at NemID (i praksis den indeholdte signaturfunktionalitet) kan erstatte fysisk underskrift og således kan anvendes som grundlag for forpligtende aftaler.

Disse konklusioner er i overensstemmelse med bestemmelser i direktivet om elektroniske signaturer samt forordningen om elektronisk identifikation og tillidstjenester, hvoraf det følger, at en kvalificeret elektronisk signatur har samme retsvirkning som en håndskreven underskrift. Tilsvarende fastslår både direktivet og forordningen, at elektroniske signaturer ikke må afvises i en retssag alene af den grund, at de er elektroniske.

4. Mål og gevinster

4.1 Vision for fremtidens nationale infrastruktur for e-identitet og digital signatur

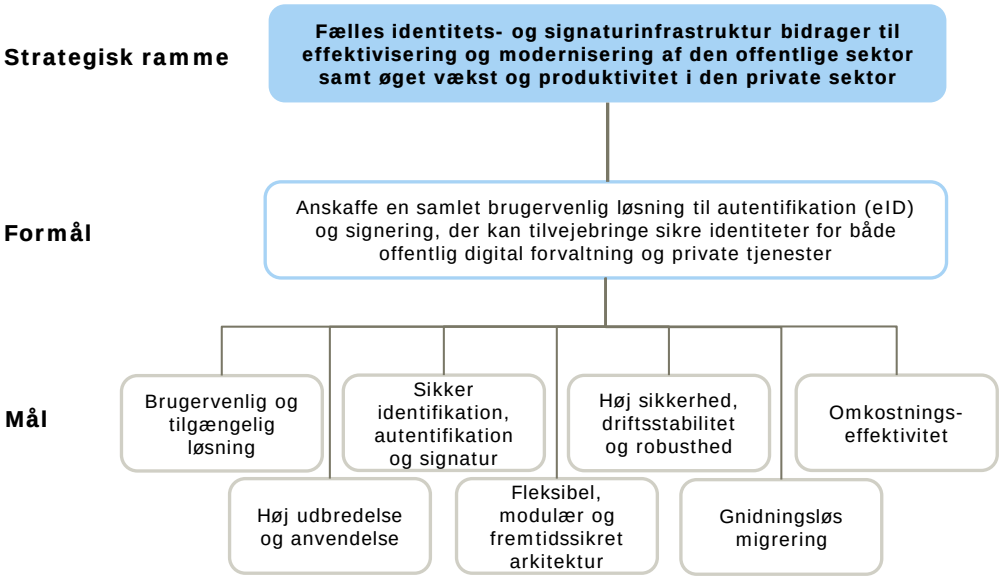
Fremtidens nationale infrastruktur for e-identitet og digital signatur for borgere, myndigheder og private virksomheder er forudsætningen for en fortsat effektiv, brugervenlig og sikker digital offentlig sektor. Én fælles identitets- og signaturinfrastruktur med høj anvendelse og stor udbredelse bidrager til effektivisering og modernisering af den offentlige sektor samt øget vækst og produktivitet i den private sektor. Med næste generation NemID skal brugerne derfor kunne få adgang til offentlige og private digitale services på en brugervenlig og sikker måde, og de skal fortsat kunne signere.

Næste generation NemID skal ligeledes understøtte effektiv digital kommunikation med borgerne, således at borgerne kan anvende forskellige platforme, herunder mobile platforme, til kommunikation med det offentlige.

Den fællesoffentlige indsats betyder sammen med samarbejdet med bankerne, at mere end 4,4 millioner borgere har NemID, og mere end 1 millioner medarbejdere og personer med tilknytning til virksomheder og myndigheder har en NemID medarbejdersignatur. Der foretages cirka 50 millioner transaktioner om måneden. Den høje udbredelse og anvendelse skal videreføres i en fremtidig løsning, således at gevinsterne ved at investere i en ny løsning bliver så høje som muligt.

Figur 5 viser visionen for den kommende løsning, selve formålet med udbuddet og de enkelte delmål for løsningen. Hvor visionen er en overordnet samfundsvision, er selve formålet med projekt "Næste generation NemID" at anskaffe en samlet løsning til autentifikation (eID) og signering, der kan tilvejebringe sikre identiteter for både offentlig digital forvaltning og private tjenester.

Figur 5 Oversigt over formål og mål for projekt Næste generation NemID



Det overordnede formål indebærer, at den samlede løsning skal dække behov for sikker autentifikation og signering for både borgere, virksomheder, myndigheder og deres medarbejdere. De sikre identiteter skal ikke alene kunne anvendes i forhold til det offentlige, men også i forhold til digitale tjenester, som tilbydes private.

Da NemID er en del af grundlaget for it-sikkerheden i offentlige og private tjenester, er det en grundlæggende forudsætning, at NemID fortsat har meget høj sikkerhed både i design og drift.

Samtidig skal sikkerheden kunne styrkes i takt med øgede behov for fortrolighed og for at imødegå fremtidige trusler mod sikkerheden.

4.2 Mål

Målene for løsningens indhold er:

- Brugervenlig og tilgængelig løsning (for mange brugere med forskellige forudsætninger og typer af brugerudstyr).
- Sikker identifikation, autentifikation og signatur.
- Høj sikkerhed, driftsstabilitet og robusthed.
- Høj udbredelse og anvendelse.
- Fleksibel, modulær og fremtidssikret arkitektur.
- Gnidningsløs migrering.
- Omkostningseffektivitet.

En *brugervenlig og tilgængelig løsning for mange brugere med forskellige forudsætninger og typer af brugerudstyr* indebærer, at næste generation NemID bedst muligt skal dække behovene hos en meget bred brugerskare med mange forskellige behov og forudsætninger. Det gælder mere end fire millioner borgere med meget forskellig it-parathed, meget forskellige anvendelsesmønstre og mange forskellige typer udstyr som Pc'er, tablets og smartphones. Det gælder mere end en million medarbejdere i virksomheder dækkende både administrative funktioner og funktioner i sundhedsvæsenet. Det gælder desuden de medarbejdere, der skal administrere disse medarbejdere og mere end en halv million virksomheder, myndigheder mv., som anvender NemID.

Sikker identifikation, autentifikation og signatur indebærer, at næste generation NemID skal leve op til krav i EU's forordninger (fx eIDAS) og dansk lovgivning samt dække behovene i offentlige og private digitale tjenester for sikker identifikation, autentifikation og signering.

Næste generation NemID skal fortsat have *høj sikkerhed, driftsstabilitet og robusthed* for at kunne dække behovene hos tjenesteudbyderne. Digitale tjenester, der forudsætter NemID, anvendes til så mange livsvigtige (fx i sundhedsvæsenet) og samfundskritiske formål (fx økonomiske transaktioner), at der skal være tilstrækkelig kapacitet og oppetid døgnet rundt, året rundt.

Høj udbredelse og anvendelse dækker over, at løsningen skal anvendes af mange forskellige brugergrupper og i mange forskellige sammenhænge, både offentlig og privat.

En *fleksibel, modulær og fremtidssikret arkitektur* indebærer, at løsningen kan udvikles i takt med nye funktionelle og sikkerhedsmæssige behov, at der kan anvendes tidssvarende og økonomisk attraktive komponenter, og at disse komponenter forholdsvis let kan udskiftes.

En *gnidningsløs migrering* indebærer, at borgernes migrering til en ny løsning tager højde for borgernes kompetencer. Ligeledes indebærer det, at virksomheders og myndigheders meget store investeringer i it-udstyr og personalekompetencer i videst muligt omfang kan anvendes i forbindelse med næste generation NemID. Endelig indebærer det, at migreringen sker med fokus på høj sikkerhed og driftsstabilitet.

Omkostningseffektivitet betyder, at næste generation NemID skal kunne anskaffes og drives med færrest mulige omkostninger både for det offentlige og for de borgere og virksomheder, der skal anvende NemID.

I projektet vil der være behov for løbende at vælge bedst mulig balance mellem disse krav.

4.3 Gevinster

De gevinster, der ønskes opnået med projektet, er:

- Høj tillid til løsningen.
- Lettere anvendelse for borgere.
- Lettere anvendelse for virksomheder.

- Lettere administration for virksomheder.
- Flere offentlige tjenester anvender det nye NemID.
- Flere private tjenester anvender det nye NemID.
- Mere fleksible udviklingsmuligheder og fremtidssikring af løsningen

Set i sammenhæng med statens business case-model har projektet i sig selv således primært kvalitetsløftsgevinster og kun i begrænset omfang effektiviseringsgevinster. NemID muliggør dog effektiviseringsgevinster på mange andre måder, da NemID understøtter digitalisering generelt.

Høj tillid til løsningen betyder, at brugerne har tillid til, at NemID fungerer tilfredsstillende og med høj sikkerhed. NemID skal bidrage til at sikre, at fortrolige data om borgerne forbliver fortrolige.

Lettere anvendelse for borgere og for virksomheder betyder, at brugerne har lettere ved at autentificere sig og signere digitalt. Det betyder også, at der er hjælp at hente, når der opstår problemer, fx i form af support.

Lettere administration for virksomheder betyder, at virksomhederne skal administrere mindst muligt, og at administrationsløsningerne er tilpassede de forskellige virksomhedstypers behov.

At *flere offentlige tjenester anvender det nye NemID*, er primært bestemt af aftaler om, at offentlige tjenester med følsomme personoplysninger skal anvende NemID og NemLog-in. Med en mulighed for 1-faktor-login kan der dog muligvis tiltrækkes flere offentlige tjenester.

At *flere offentlige private tjenester anvender det nye NemID* betyder, at det nuværende antal tjenester stiger fx som følge af mulighed for 1-faktor-login.

Mere fleksible udviklingsmuligheder og fremtidssikring af løsningen betyder, at den kommende løsning løbende kan tilpasses interessenternes behov, og at nye tekniske og sikkerhedsmæssige løsninger lettere kan implementeres i løbet af den kommende kontraktperiode.

I vurderingen indgår ikke en gevinst i form af et stigende antal brugere (borgere og medarbejdere), da antal brugere dels bestemmes af lovgivning, regler og aftaler om obligatorisk digital selvbetjening, dels indirekte følger af, at flere tjenester anvender NemID.

Scenarier og løsningselementer vurderes i forhold til de ovennævnte gevinster.

5. Brugervenlighed og brugeroplevelse

Brugervenlighed dækker som begreb, at et produkt eller en given brugergrænseflade er nem at betjene. I digital kontekst betegner brugervenlighed en egenskab ved et system med en grænseflade, der er relevant, overskuelig og let at navigere i fra et brugerperspektiv. Et brugervenligt system tager højde for målgruppens behov og adfærd. Det forventningsafstemmer i forhold til den opgave, der skal udføres, giver meningsfuld feedback til brugeren og giver fornemmelsen af kontrol.

Brugeroplevelse dækker som begreb brugerens samlede løbende oplevelse både før, under og efter interaktionen med et produkt.

For at opnå et højt niveau af tilfredshed hos brugere skal udviklerne være i stand til at supplere forretningsmål med indsigt i målgruppens behov samt have den fornødne teknologi til rådighed.

Rapporten vil overvejende behandle brugervenligheden i de beskrevne løsningselementer, selvom brugernes oplevelser ikke er begrænset til anvendelsen af NemID. Øget brugervenlighed i NemID brugergrænsefladen vil dermed kun delvist påvirke en samlet brugeroplevelse.

Med næste generation NemID er der mulighed for at øge brugervenligheden ved at designe og udvikle løsningselementerne med vægt på et brugercentreret perspektiv, og ikke udelukkende fokusere på de teknologiske muligheder. Næste generation NemID kan dermed af brugerne opfattes som forbedret. Dette sikres bl.a. ved at fokusere på den værdi, brugerne oplever, når de anvender NemID. Hvis næste generation NemID bliver lettere at anvende, er der også større chance for, at det anvendes korrekt og bliver mere sikkert.

Værdi for slutbrugere er fx, når slutbrugeren er i stand til at gennemføre digitale selvbetjeningsløsninger uden at støde på teknologiske eller designmæssige barrierer og samtidig betragter oplevelsen som overvejende positiv.

Brugervenlighed er også at tilvejebringe løsninger, der dækker brugerens forskellige behov i hverdagen. Et nøglekort er eksempelvis god til brug ved et bord i hjemmet, men ofte ikke en optimal løsning for den, der skal logge ind fra en smartphone i et S-tog.

5.1 Forudsætninger for gode brugeroplevelser

I Fase 1 var en af de tydeligste indsigter fra brugeranalysen, at slutbrugerne ikke forstår, hvad NemID er og ikke er. De forstår til gengæld godt, hvad de skal bruge det til. En egentlig systemforståelse for NemID-økosystemet er ikke udbredt blandt brugerne og er næppe nødvendig. Et eksempel på denne manglende forståelse er bl.a., at den almindelige bruger ikke ved, hvad forskellen på NemID og NemLog-in er.

Brugere behøver ikke kunne forstå, hvordan et system fungerer for at være i stand til at interagere med det. De brugergrænseflader, hvori man anvender sit NemID, er mangeartede og ofte komplicerede, digitale tjenester. Til trods for at de i mange brugeres øjne er del af en sammenhængende brugeroplevelse, er der ikke sammenhæng mellem brugergrænsefladerne til tjenester og NemID. Af samme årsag kan næste generation NemID ikke i sig selv løse alle de udfordringer, der vil findes omkring brugeroplevelse i disse usammenhængende systemer.

Det har afgørende betydning for helhedsopfattelsen, hvordan brugeren er kommet i gang med at anvende en service. For nogle har anskaffelsen af NemID været forbundet med besværligheder, der er svære at abstrahere fra, og som efterfølgende præger opfattelsen af NemID-løsningen.

En anden og stor indflydelse på brugeroplevelsen af NemID er brugernes helhedsopfattelse af NemID, som hele tiden kan og bliver påvirket af bl.a. medier og brugernes umiddelbare omgangs-

kreds. De historier, en slutbruger hører om eller læser i pressen om andres oplevelser med NemID, må forventes at være overvejende negative og kan i større eller mindre grad påvirke brugerens egen oplevelse af interaktionen med en NemID-brugergrænseflade.

Rapporten tager udgangspunkt i brugeroplevelser, der relaterer til Scenarie 2 og 3, og inkluderer de indsigter, der er fundet på baggrund af brugeranalysen i Fase 1.

5.2 Metodisk arbejde med brugercentreret design for NemID

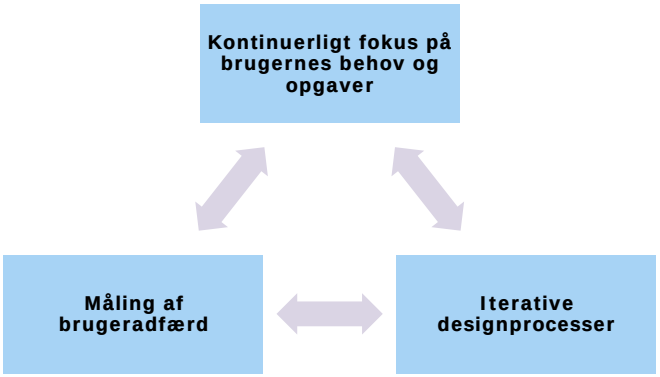
Et fundamentalt princip er kontinuerligt fokus på brugerens behov og opgaver.

Det kan ske gennem en metodisk tilgang, hvor der oparbejdes en kvalitativ forståelse for slutbrugeres anvendelse af et system, for deres adfærd, frustrationer, behov og ønsker. Dette med henblik på at sikre høj grad af brugervenlighed og brugertilfredshed. Tilgangen skal give udviklingsteamet – informationsarkitekter, designere og udviklere – en grundig forståelse for det, de udvikler til.

Der skal være løbende måling af brugeradfærd med analyser og tests af både kvalitativ og kvantitativ karakter.

Der skal være iterative designprocesser, hvor der er løbende forventningsafstemning med inddragelse af interessenter og slutbrugerne.

Figur 6: Fokuspunkter i processen for brugercentreret design

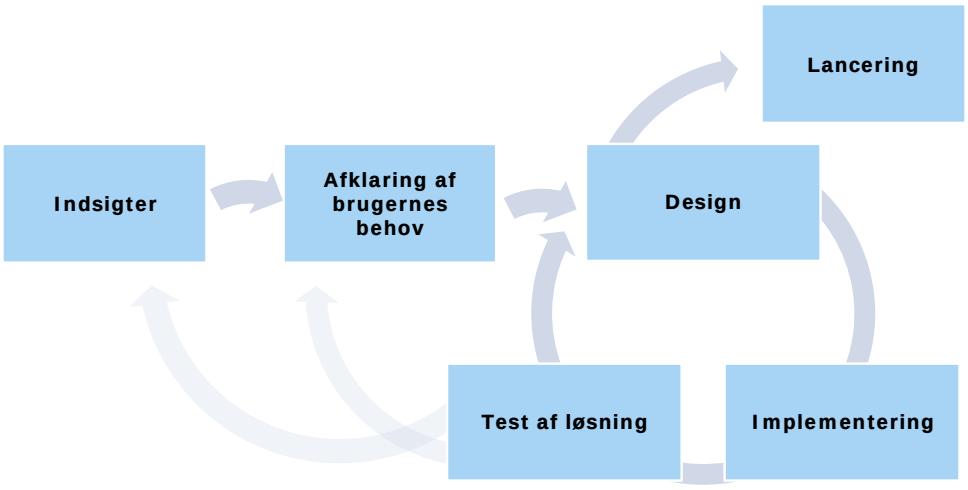


En grundlæggende mekanisme i et metodisk arbejde med brugervenlighed er at inkludere den erfaring og viden, der er indhentet i tidligere faser af løsningens liv og inddrage disse i den iterative designproces.

Den viden, der indhentes gennem involvering af brugere i alle løsningens faser, inddrages i designarbejdet og er med til at forme en løsning, der er let at anvende, og som opfylder brugernes behov. En del af processen er at validere løsningen gennem en evaluerende analyse, hvor brugerne igen er centrale for at afdække, hvorvidt ønsker og krav til anvendelse og oplevelse er indfriet. Indsigterne inddrages i efterfølgende designarbejde, og på den måde gentages analyse og design i en iterativ proces.

Det er i høj grad relevant at se på den samlede brugeroplevelse på tværs af løsninger, hvortil NemID anvendes og arbejde med processerne omkring brugercentreret design i samlede brugerforløb i offentlige digitale løsninger. Det kunne eksempelvis være at optimere hele brugeroplevelsen omkring indberetning af sygdom i NemRefusion eller rettighedsstyring af medarbejdersignaturer.

Figur 7: Model for metodisk arbejde med brugercentreret design



Figurens processer kan illustreres ved, at der allerede nu er sket en afdækning af brugernes behov flere gange i foranalysen, bl.a. ved en offentlig høring og ved flere brugerworkshops. De offentlige parter har desuden aktivt medvirket i analysefasen ved at udarbejde dele af analysegrundlaget. Det kan bæres ind i designfasen af næste generation NemID.

RMC-ICG anbefaler, at disse processer benyttes som konsekvent fremgangsmåde i udviklingsprocessen for at opnå brugbare, anvendelige brugergrænseflader og høj brugertilfredshed.

5.3 Brugervenlighedsmålinger

I tråd med principperne bag iterative designprocesser er det muligt at måle effektiviteten, den forretningsmæssige værdi og brugervenligheden af NemID-løsningen. For at opnå det bedst mulige vurderingsgrundlag bør man sammensætte to eller flere testmetoder i en samlet undersøgelse. Denne metodetriangulering styrker validiteten af undersøgelsen, idet de valgte metoder kompenserer hinandens styrker og svagheder.

Hver metode har særlige styrker, som kan analysere de kriterier, der opstilles for undersøgelsen. Tre supplerende metoder kan eksempelvis være:

- Kvantitativ undersøgelse: Hvor hurtigt kan brugerne gennemføre en defineret opgave, og hvor falder de fra?
- Kvalitativ undersøgelse: Hvilke udfordringer oplever brugeren og hvorfor?
- Ekspert-evaluering: Hvordan vurderer en ekspert i brugervenlighed en brugergrænseflade?

RMC-ICG anbefaler, at der metodisk gennemføres brugervenlighedsmålinger for at tilvejebringe objektive begrundelser for ændringer i brugergrænsefladen.

5.4 Konklusion

Det er ikke muligt at beskrive rammerne for, hvordan den gode brugeroplevelse bør se ud for NemID, da oplevelsen som helhed rummer langt flere faktorer end dem, det er muligt at påvirke med næste generation NemID.

RMC-ICG anbefaler, at der i arbejdet med næste generation NemID er et kontinuerligt fokus på brugernes behov både i forbindelse med kravspecifikation, udvikling af den ny løsning og løbende i hele kontraktperioden.

RMC-ICG anbefaler, at der arbejdes med iterative designprocesser for at sikre, at brugervenligheden for NemID bliver bedst mulig og udvikler sig i takt med fremtidige behov.

6. Økonomisk ramme

Som grundlag for at skønne udgifterne til næste generation NemID beskrives i det følgende økonomien i den nuværende løsning samt forhold, der har betydning for, hvor store udgifter der kan forventes til den kommende løsning.

6.1 Den nuværende økonomi

Den nuværende NemID-løsning er fastlagt i Aktstykke 205, godkendt af Finansudvalget den 18. juni 2008, vedrørende etablering af en fælles digital signatur med finanssektoren samt at sikre et sikkerhedsløft.

Ifølge aktstykket er de samlede udgifter til det nuværende NemID 850 millioner kroner, hvoraf bankerne forventes at betale 485 millioner kroner, og indtægter fra virksomheder og offentlige myndigheder udgør 160 millioner kroner for ydelser leveret af den nuværende leverandør.

De resterende 205 millioner kroner til udvikling og drift (herunder support) af NemID er finansieret fællesoffentligt med en tredjedel fra henholdsvis staten, kommunerne og regionerne.

Dette kapitel afdækker alene de fællesoffentlige udgifter.

6.1.1 Fællesoffentlige udgifter 2008-2015

Udvikling og videreudvikling

Af de 205 millioner kroner i Aktstykke 205 er 50 millioner kroner afsat til udvikling af den nuværende NemID-løsning.

I perioden frem til nu er der desuden anvendt yderligere 34 millioner kroner til videreudvikling af fx JavaScript-klienten, håndtering af DDoS-angreb og mobile løsninger.

I alt har den nuværende løsning kostet knap 90 millioner kroner at udvikle.

Drift og support

Af de 205 millioner kroner i Aktstykke 205 er 155 millioner kroner afsat til drift og support, i kontrakten fordelt med halvdelen til drift, halvdelen til support.

Der er yderligere tilført 14 millioner kroner til drift (i forbindelse med drift af JavaScript-klienten) og 20 millioner kroner til frikøb af support til virksomheder i forbindelse med obligatorisk Digital Post.

I alt har den nuværende løsning kostet knap 200 millioner kroner i drift og support (inkl. skønnede udgifter på 39 millioner kroner for 2015).

De samlede fællesoffentlige udgifter i perioden 2008-2015 er summen af ovenstående og forventes at være knap 300 millioner kroner (inkl. skønnede udgifter for 2015).

6.1.2 Andre offentlige udgifter

Stat, kommuner og regioner har afholdt yderligere udgifter i forbindelse med NemID. Det omfatter udgifter til support i forbindelse med NemID, udgifter som tjenesteudbydere og udgifter som arbejdsgivere (til NemID medarbejdersignaturer).

6.2 Fremskrivning af nuværende økonomi i udbudsperioden

Det har stor betydning for fremskrivningen af den fremtidige økonomi, at NemID overgår fra en periode med kraftig vækst i antal identiteter til en periode med mere afdæmpet vækst i dette antal.

Samtidig er der i perioden også sket en kraftig vækst i antallet af transaktioner med NemID for både banker, offentlige tjenester og private tjenester, hvilket også har stor indflydelse på fremskrivningen.

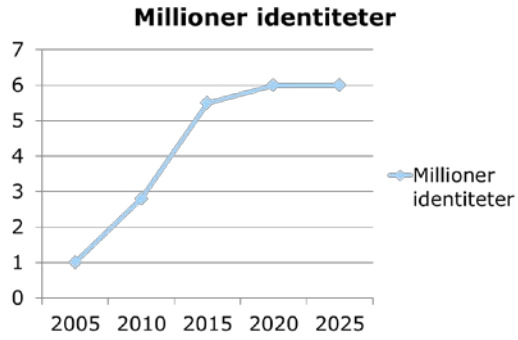
De foregående år har været præget af en omfattende omlægning til digitale løsninger og deraf følgende stigning i transaktioner både i banker og det offentlige. Den generelle tendens forventes at være, at antallet af både banktransaktioner og transaktioner på offentlige tjenester fortsat vil stige, omend mere afdæmpet end hidtil. Derimod vil antallet af transaktioner hos øvrige private tjenesteudbydere i høj grad afhænge af, hvordan den næste generation NemID designes, og på hvilke betingelser den stilles til rådighed for private tjenesteudbydere.

Tabel 5 NemID transaktioner 2014[3]

Transaktioner	Antal i millioner
NemID-banktransaktioner	480
NemID OCES private	88
NemID OCES offentlige (NemLog-in)	42
Nøglefils-transaktioner (skøn)	25

Nedenfor vises derfor en skønnet udvikling i det samlede antal NemID (både borgere og medarbejdere). Figur 8 viser, hvordan der fra 2005 og frem til 2015 er sket en kraftig stigning i antallet af NemID, og at der fremover kan forventes en langt svagere stigning, dels fordi 90 % af borgere over 15 år nu har et NemID, dels fordi omkring 40 % af arbejdsstyrken har en NemID medarbejdersignatur.

Figur 8: Fremskrivning af den fremtidige udvikling af identiteter



Denne ændring i udbredelsen af NemID markerer også overgangen fra et papirbåret samfund til et digitalt samfund, hvor fx brugernes kendskab til digitale værktøjer kan forventes at medføre, at behovet for support ligeledes har nået et plateau og måske vil blive reduceret i de kommende år.

Det nuværende niveau for udgifter til drift og support på cirka 40 millioner kroner om året forventes derfor at stige i den ny kontraktperiode. Driftsudgifterne vil være påvirket af de flere transaktioner, mens det er vanskeligt at vurdere det fremtidige supportbehov.

6.3 Vurdering af påvirkninger i NemID-økosystemet

Gennemførelsen af scenarierne vil have forskellig påvirkning på interessenterne i økosystemet.

Både for gevinster og udgifter gennemføres analysen opdelt på de forskellige aktører i NemID-økosystemet, som består af følgende:

Registreringsopgaven: Denne udføres i dag af kommunerne, bankerne og borgerne på selvbetjeningsløsninger. Desuden udføres opgaven af virksomheder og myndigheder i forskellige løsninger. Registreringsopgaven forventes at være uændret i næste generation NemID og analyseres ikke.

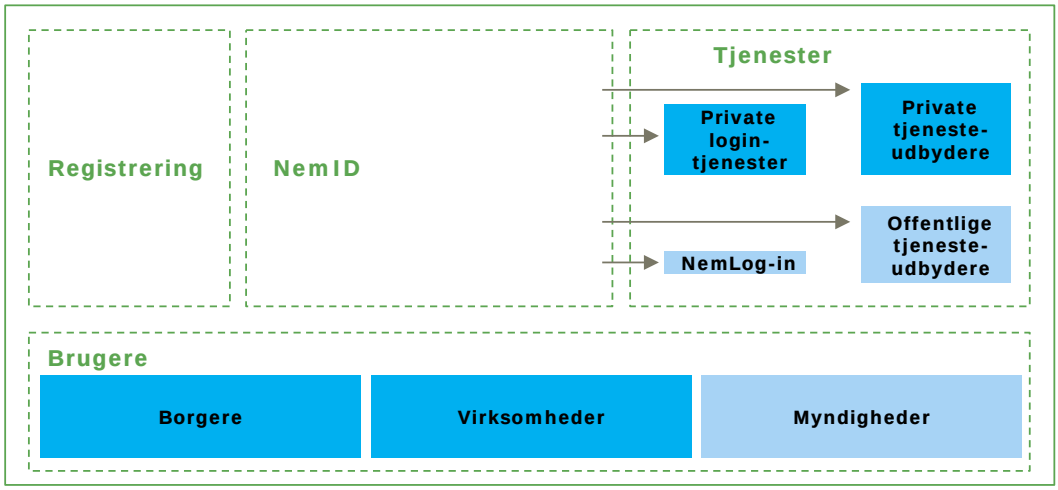
[3] Opgjort pr. ultimo september 2014. Der har ikke været adgang til tal for NemID medarbejdersignatur med nøglekort.

NemID: Denne del af opgaven omfatter udbud af næste generation NemID og udgifterne til anskaffelse og drift af den nye løsning i perioden 2018-2022. Udgifterne hertil afholdes af stat, kommuner og regioner, og beskrives som fællesoffentlige udgifter.

Brugere: NemID udsteder digitale identiteter til borgere, virksomheder, myndigheder og deres medarbejdere. Analysen afdækker påvirkningen på borgerne og på virksomheders og myndigheders rolle som arbejdsgiver (brugerorganisation) samt på disses medarbejdere.

Tjenester: Brugerne anvender NemID til at få adgang til meget forskellige digitale tjenester. Tjenesternes forhold er meget varierende, afhængigt af, om de er offentlige eller private. For sidstnævntes vedkommende er forholdende afhængige af, om de anvender en login-tjeneste eller selv har opbygget en løsning til login-funktionen, eventuelt med brug af den tjenesteudbyderpakke, som den nuværende leverandør stiller til rådighed. Analysen afdækker påvirkningen på private tjenesteudbydere og login-tjenester og på offentlige tjenesteudbydere og NemLog-in.

Figur 9: Overblik over interessenterne i NemID-økosystemet



6.4 Udgiftsdrivere i den kommende løsning

På grundlag af udgiftsanalysen af den nuværende løsning og tal for transaktioner og support kan der identificeres nedenstående væsentlige udgiftsdrivere.

Udviklings- og videreudviklingsudgifter

Udgiftsdrivende for udviklingsudgifter er krav til funktionalitet og brugervenlighed. Især kræver brugervenlighed som vist i foregående afsnit en stor indsats med inddragelse af brugere og sikring af sammenhæng i brugeroplevelsen, hvilket også øger udgifterne. Hertil kommer høje udgifter som følge af, at der arbejdes med krypterede data og med høje sikkerhedskrav. Det betyder blandt andet store krav til tests af løsningen.

Udviklingsomkostningerne kan reduceres, hvis det er muligt i høj grad at anvende standardløsninger. Særlige nationale krav, der afviger fra internationale standardløsninger, er således udgiftsdrivende.

Udgifter til tilgængelighed (”24*7”)

NemID er en afgørende infrastrukturkomponent for anvendelsen af en række centrale tjenester som offentlige selvbetjeningsløsninger.

Der er derfor store krav til tilgængelighed i form af:

- Korte svartider for alle transaktioner – stiller krav til høj kapacitet også ved spidsbelastning.
- Tilgængelig løsning døgnet rundt, året rundt (24*7) – stiller krav til dublerede installationer og mandskabskrævende overvågning døgnet rundt.

- Tilgængelig løsning også i beredskabs-/katastrofesituationer – som stiller krav til dublerede installationer og eventuelt reserveudstyr.

Disse krav er alle udgiftsdrivende for driftsudgifterne.

Transaktioner

Det nuværende NemID har haft 600 millioner transaktioner pr. år (både banktransaktioner og PO-CES-transaktioner).

Den nuværende nøglekortsløsning koster op til 20-40 øre pr. transaktion[4] i udgifter til trykning og forsendelse af nøglekort, hvilket betyder meget i de samlede udgifter.

Support

Ifølge kontrakten med den nuværende leverandør går cirka halvdelen af den samlede betaling for drift til support. Support udgør derfor en væsentlig del af de fællesoffentlige udgifter.

[4] Den nuværende leverandørs pris for et nøglekort er 76 kroner (http://www.nets.eu/dk-da/Produkter/Sikkerhed/medarbejdersignatur/Pages/Priser-uden-Pro-pakken.aspx). Der er 148 nøgler på nøglekortet. Det er en pris på 51 øre pr. nøgle. Anslås leverandørens avance til 20 %, svarer det til 40 øre pr. nøglekort.

7. Forretningsmodeller

I dette kapitel foretages en analyse af finansieringsmuligheder ved etablering og drift af næste generation NemID i Danmark. Fokus er i afsnittet på at undersøge muligheder og konsekvenser af en ændret egenbetaling af NemID-løsninger for slutbrugere (borgere, virksomheder og myndigheder) samt de private og offentlige tjenesteudbydere.

Afsnittet behandler ikke fordelingen af finansieringen mellem stat, kommuner og regioner. Ligeledes er fordelingen mellem det offentlige og eventuelle private partnere uden for afsnittets fokus. Begge aspekter behandles særskilt af Digitaliseringsstyrelsen.

7.1 Udstedelse og anvendelse af NemID

7.1.1 Borgere

Da NemID til borgere *de facto* er en forudsætning for digital kommunikation med det offentlige, er det en forventning, at udstedelsen og anvendelsen af løsningen fortsat er gratis.

Den eksisterende model, hvor NemID til borgere er gratis, har vist sig at have meget stor og positiv effekt i forhold til udbredelsen af den nuværende version af NemID. Set i lyset af erfaringer fra andre lande kan det betragtes som en af hovedårsagerne til løsningens store succes. En alternativ model, der bygger på en højere grad af egenbetaling, vil være vanskelig at indføre og vil uden tvivl blive negativt modtaget.

Modviljen mod egenbetaling for NemID privat tager udgangspunkt i en argumentation om, at det offentlige (og bankerne), der høster de direkte økonomiske gevinster ved anvendelsen af NemID, også skal afholde omkostningerne for løsningen. Denne argumentation gælder basisløsningen baseret på nøglekort og i mindre grad tillægsprodukter, hvor der er større accept af, at borgerne selv betaler.

De samme forhold er i princippet også gældende for supportydelsen. Dog kan man forestille sig nogle betalbare supportservices, fx med henblik på at begrænse antallet af telefonhenvendelser.

På lidt længere sigt kan højere grad af egenbetaling føre til, at borgerne vil søge at fravælge NemID-løsningen. Borgernes betalingsvillighed er afgørende afhængig af, hvilke tjenester en egenbetalt NemID vil give adgang til. Således vurderes det, at fx de studerende fortsat vil anvende NemID for at få SU, uanset om NemID til borgere vil være frikøbt (skattefinansieret) eller ej. Hvis der er mulighed for at anvende analoge kanaler, vil borgere sandsynligvis øge anvendelsen af disse.

7.1.2 Virksomheder

Den nuværende betalings- og finansieringsmodel bygger på et frikøb af de første tre NemID medarbejdersignaturer. Modellen dækker på nuværende tidspunkt primært behovet for medarbejdersignaturer hos enkeltmandsvirksomheder og små virksomheder, der ikke ønskes belastet med ekstra udgifter. Også mange større virksomheder anvender de gratis medarbejdersignaturer som en tilstrækkelig løsning for at kunne tilgå de offentlige tjenester. Således er cirka 80 % af medarbejdersignaturerne udstedt til virksomheder med 1-3 medarbejdersignaturer.

Ligesom for borgere er NemID i praksis obligatorisk for virksomheder, der skal anvende en række offentlige tjenester. Det er således en udbredt forventning, at anskaffelse og anvendelse af NemID-løsninger til erhvervsformål skal være mulig uden at påføre virksomhederne ekstra omkostninger. Forventningen bygger på rationalet om, at dem, der høster gevinster, også afholder omkostningerne.

Det er vurderingen, at behovet for gratis medarbejdersignaturer for virksomheder er betydeligt mindre i den kommende generation af NemID, hvis man vælger at udvide mulighederne for, at NemID privat også skal kunne bruges til erhvervsformål.

Der vil således være en mulighed for at fjerne gratis anskaffelse af de første medarbejdersignaturer, og for at mange virksomheder 'migrerer' til en gratis NemID privat til erhvervsformål. Denne ændring muliggør også differentieret prisniveau for en basisløsning (dvs. de første tre medarbejdersignaturer) og tillægsprodukter (øvrige certifikater ud over de første tre).

Overvejelserne vedrørende finansiering af medarbejdersignaturer er i store træk også gældende for support. Argumentationen er tilsvarende, at myndighedernes digitale tjenester er obligatoriske, og supporten for at kunne anvende dem skal være gratis (eller i hvert fald med reducerede priser).

Et frikøb af erhvervssupport vurderes således at have en positiv indflydelse på brugertilfredsheden og indgår derfor som et element i Scenarie 3.

7.1.3 Myndigheder

Myndighedernes anskaffelse og brug af medarbejdersignaturer omfattes i den eksisterende NemID- løsning af samme betalingsregler som de private virksomheder. Dvs. at myndighederne skal betale for udstedelse af hvert certifikat ud over de første tre.

En ændring af denne model til et frikøb af alle medarbejdersignaturer til det offentlige ville have store konsekvenser for løsningens forretningsmodel, primært på grund af regionernes store anvendelse af NemID.

Samtidig vil den kræve, at leverandøren af medarbejdersignaturer nemt skal kunne sondre mellem NemID, der skal udstedes til de private virksomheder, og dem, der skal udstedes til myndighederne, fx med udgangspunkt i en komplet liste over myndigheder. Etablering af en sådan liste skal dække mere end 500.000 virksomheder og mange tusinde offentlige organisationer. Det vil være en stor og kompleks opgave, som vil kræve en stor løbende indsats, da konstellationen af myndigheder ændrer sig.

På den anden side kan der være økonomiske gevinster ved et samlet frikøb af medarbejdersignaturer til brug hos det offentlige, både i form af lavere priser pr. NemID og i form af indirekte gevinster på grund af større udbredelse af løsningen på tværs af myndigheder og dermed større brugervenlighed.

7.1.4 Private tjenesteudbydere

Den nuværende leverandør opkræver betaling hos private tjenesteudbydere, hvor der er to afregningsmodeller at vælge imellem:

- Pris pr. session, dvs. for hver anvendelse, login og/eller signering på en eller flere af tjenesteudbydernes applikationer. Modellen anbefales, hvis kunderne anvender tjenesten hos en privat udbyder en til tre gange om året.
- Pris pr. unik bruger, dvs. at der afregnes pr. unik bruger (pr. kalenderår), som anvender løsningen hos den private tjenesteudbyder. Den unikke bruger kan anvende tjenesten ubegrænset. Modellen anbefales til private tjenesteudbydere, hvor kunderne anvender deres tjenester mere end tre gange om året.

NemID blev i 2014 anvendt til 88 millioner transaktioner hos private tjenesteudbydere. Med en pris pr. session på 1,01 kroner betyder det en omsætning på 89 millioner kroner til den nuværende leverandør. Sandsynligvis betyder pris pr. unik bruger, som vælges af tjenesteudbydere med mange transaktioner, at tallet er noget lavere.

De private tjenesteudbyderes brug af den kommende NemID-infrastruktur kan enten betales af det offentlige, dvs. frikøbes eller fortsat indgå som en service, virksomhederne selv skal betale for.

En skattefinansieret model (et frikøb af anvendelsen af NemID-infrastrukturen for de private tjenesteudbydere) kan have positive effekter, herunder bl.a. en øget udbredelse og anvendelse af løsningen. Det medfører øget brugervenlighed gennem samme og konsistente brugeroplevelser og

en øget sikkerhed. På den negative side kan det fremhæves, at et frikøb af NemID i forhold til private tjenesteudbydere vil bidrage til at fjerne konkurrencen på markedet for autentifikations- og signeringsløsninger. En skattefinansieret model (eventuelt i et partnerskabssamarbejde) i forhold til private tjenesteudbydere vil trække endnu mere i retning af monopollignende tilstande i et længere perspektiv.

Der er to grundlæggende varianter for private tjenesteudbyderes betalinger:

I den første variant er det leverandøren af løsningen, der fortsat står for salg af ydelser i forbindelse med private tjenesteudbyderes brug af NemID.

I den anden variant overtager det offentlige (eventuelt i en partnerskabskonstruktion) salg af ydelserne, og overtager som konsekvens også direkte indtægterne. Dette vil svare til implementering af en 'CPR-model' og vil begrænse usikkerheder og nødvendige kontrolmekanismer vedrørende leverandørens prisfastsættelse, indtjeningsmargin m.m. Dog skal man være opmærksom på, at implementering af CPR-modellen kan betyde krav om overtagelse af ejerskabet. Kravene omkring åbenhed om økonomien ('åbne bøger') vil stadig være gældende mellem parterne i en eventuel partnerskabskonstruktion.

7.1.5 Offentlige tjenesteudbydere

Anvendelse af NemID-løsningen er på nuværende tidspunkt frikøbt for de offentlige tjenesteudbydere. De offentlige tjenesteudbydere skal derfor ikke betale for, at brugerne anvender NemID i deres tjenester. Modellen har vist sig at have nogle positive effekter i form af besparelser ved et samlet indkøb af retten til at kunne anvende NemID-infrastrukturen. Den har også givet forretningsmæssige og organisatoriske gevinster ved at fastholde de offentlige myndigheders fokus på effektivisering gennem digitalisering.

En ændring fx til at indføre en betalingsmodel, der følger modellen for de private virksomheder, kan bidrage til at fjerne disse effekter.

7.2 Anskaffelse og anvendelse af tillægsprodukter og -ydelser

En fremtidig NemID-infrastruktur vil indeholde en række tillægsprodukter og -ydelser, som kan tilvejebringe et øget finansieringsgrundlag.

Både på virksomhedsområdet og på borgerområdet er der allerede etableret tillægsydelser, fx i form af forskellige ekstra medarbejdersignaturer, supportydelser eller NemID-nøglevisere, USB kryptotoken m.m.

I praksis har det dog vist sig, at efterspørgslen efter disse produkter og ydelser er ret begrænset, og som en konsekvens er der sandsynligvis ringe finansieringsmuligheder. Det forventes ikke at ændre sig, selvom der skulle komme nye og smartere produkter, da brugerbetaling stadig vil udfordre efterspørgslen.

7.3 Konklusion

Mulighederne for at øge egenbetalingen af anvendelse af NemID synes at være ret begrænsede. Både borgere og de private virksomheder har en forventning om, at det offentlige gratis stiller de løsninger til rådighed, der skal anvendes i forbindelse med den i praksis obligatoriske brug af digitale tjenester.

En udvidelse af de ydelser, der er skattefinansierede, kan have utilsigtede konsekvenser, herunder ikke mindst en dårligere konkurrencesituation på længere sigt, idet det begrænser mulighederne for andre leverandører i markedet.

8. Leverandørstrategi

I dette afsnit behandles leverandørstrategi for næste generation NemID. Det omfatter muligheder for flere leverandører af løsningen og konkurrencefremmende incitamenter og tiltag for at sikre, at leverandører vil byde på den kommende løsning og dermed skabe den nødvendige konkurrencesituation.

8.1 Flerleverandørstrategi

En flerleverandørstrategi i den kommende NemID kan i princippet implementeres i forhold til både back-end og front-end af den fremtidige infrastruktur.

I forhold til back-enden kan en flerleverandørstrategi enten implementeres ved en reel *dublering* af back-end løsningen eller ved at opdele NemID back-enden, så *adskilte funktioner* vil kunne leveres af forskellige leverandører. Begge opdelinger forudsætter, at markedsaktører finder det attraktivt, ikke mindst økonomisk, at byde på en *del* af næste generation NemID-løsningen.

Som konkluderet i Fase 2 rapporten er det yderst tvivlsomt, om det er realistisk at etablere parallelle back-end infrastrukturer, der retter sig mod at opfylde *samme* brugerbehov, idet det vil være meget dyrt at etablere parallelle løsninger. Det understreges dog, at løsninger, der rettes mod *specifikke* behov, fuldt ud understøttes af rammerne for den foreslåede arkitektur for den kommende NemID (se afsnit 9) og for det fællesoffentlige trust framework.

En flerleverandørstrategi for back-end med udgangspunkt i funktionsopdeling (fx gennem adskillelse af leverance af eID og eSignering-funktionalitet) vil bestemt være mulig, ikke mindst som følge af kravet til åbenhed i den kommende løsning. Opdelingen vurderes samtidig at bringe øget teknisk kompleksitet i det samlede projekt med større styringsmæssige krav for at sikre det nødvendige samspil mellem de forskellige dele af løsningen.

En eventuel flerleverandørstrategi i forbindelse med front-end elementer forudsætter ligeledes, at de nødvendige grænseflader er veldefinerede og tilgængelige for andre leverandører (som fx forskellige login-faktorer).

8.2 Potentielle tilbudsgivere for den kommende NemID-løsning

Den tekniske dialog med de potentielle danske og internationale leverandører, der blev gennemført i efteråret 2014, giver sammen med resultaterne af den tidligere udførte markedsanalyse, en indikation af det fremtidige felt af mulige tilbudsgivere. Samtidig har dialogen været med til at afdække leverandørernes præferencer og ønsker til den kommende udbudsproces.

Den vigtigste konklusion på den gennemførte dialog er, at det vil være en forholdsvis stor udfordring at få leverandører til at byde, givet markedets størrelse og den eksisterende leverandørs meget dominerende position.

Samtidig kan det konstateres, at ingen af de undersøgte leverandører og løsninger udgør et samlet alternativ til den danske NemID-løsning, hverken i deres nuværende form og indhold eller fremadrettet.

NemID er et teknisk avanceret koncept, som omfatter både elekronisk identifikation og digital signering, og der er meget få leverandører, der har tilstrækkelige erfaringer (og/eller kompetencer) til at kunne løfte denne opgave. Denne vurdering gælder både for de meget få mulige danske og for internationale leverandører.

Det er derfor en afgørende præmis for udbudsforretningens succes at være opmærksom på konkurrencefremmende tiltag, der kan være med til at øge antallet af tilbudsgivere og dermed skabe en reel konkurrencesituation.

8.3 Konkurrencefremmende tiltag

8.3.1 Rammer og præmisser for udbudsforretning

Den tekniske dialog med potentielle leverandører har vist, at det er centralt at sikre størst mulig grad af gennemsigtighed i udbudsprocessen i forhold til kontraktforhandlingerne, forretningsmodellen og de juridiske regler.

Den internationale interesse for den kommende udbudsforretning kan fremmes gennem en række forskellige generelle tiltag. Disse tiltag kan fx omfatte anvendelse af engelsk som sprog i udbudsforretningen, betaling for deltagelse i udbudsprocessen eller for at afgive endeligt tilbud efter deltagelse i en konkurrencepræget dialog.

De mere specifikke vilkår og krav kan fx omfatte kontraktvilkår tilpasset internationale standarder (herunder bodsbestemmelser og servicemål), afklarede vilkår og snitflader vedrørende samarbejde med den eksisterende leverandør, realistisk tidsplan, begrænset antal af mindstekrav m.m.

Man må dog forvente, at den eksisterende leverandørs meget stærke position også vil blive taget i betragtning ved en beslutning om eventuel deltagelse i en ressourcekrævende udbudsforretning, uagtet krav om ligebehandling, åbenhed m.m.

8.3.2 Opdeling af udbudsforretning

Den tekniske dialog har ligeledes vist, at de væsentligste incitamenter for deltagelse i en udbudsforretning vil være at etablere en reel markedsdynamik og konkurrence, som en flerhed af leverandører har mulighed for at vinde. Dette kan fx styres ved en opdeling af ydelsen i mindre og derved også mere håndterbare dele, der kan bydes på individuelt. Det vil i praksis være implementering af flerleverandørstrategi for den kommende løsning.

NemID forventes også i fremtiden at bestå af en række moduler og funktionelle elementer, hvor der principielt er stor valgfrihed med hensyn til, om modulerne skal leveres af en eller af flere leverandører, og hvorvidt og hvordan disse elementer skal samles i eventuelle 'leverancepakker'.

Fordelene ved en flerleverandørstrategi skal naturligvis opveje de negative konsekvenser, hvis løsningen leveres af flere leverandører. Det er ulemper som lavere brugertilfredshed, øget teknisk kompleksitet i den samlede løsning, større styringsbehov for at sikre en sammenhængende og stabil drift samt større udgifter til integrationer, m.m.

En opdeling af udbudsforretningen kan bygge på at målrette 'leverancepakkerne' i forhold til målgrupperne fx gennem adskillelse af borger- og virksomhedsrettede løsninger. Løsningen til virksomheder kan yderligere opdeles. En leverancepakke kan dække medarbejdere ansat i private virksomheder, der primært anvender medarbejdersignaturer til kommunikation med det offentlige. En anden leverancepakke kan dække medarbejdere i de store offentlige virksomheder, som fx regionerne, der primært anvender medarbejdersignaturer til autentifikation over for sektorens fagspecifikke systemer.

Denne opsplitning kan kombineres med en funktionel adskillelse, hvor eID og eSignering udbydes separat. Denne tilgang vil lægge op til, at markedets aktører vil kunne foreslå den mest velegnede teknologi til autentifikation, der opfylder de stillede krav til løsningen, og som derfor ikke nødvendigvis skal være PKI-baseret.

8.4 Konklusion

Det er RMC-ICG's vurdering, at leverandørfeltet i den kommende udbudsforretning kan vise sig at være meget begrænset, givet markedets størrelse samt den eksisterende leverandørs meget do-

minerende position. Det er derfor afgørende, at der aktivt arbejdes både med rammerne og eventuelt opdeling af de efterspurgte leverancer for derved at skabe tilstrækkelig kommerciel interesse, ikke mindst blandt de internationale leverandører.

9. Arkitekturgrundlag

9.1 Indledning

I dette afsnit beskrives det arkitekturgrundlag, som på en hensigtsmæssig måde kan understøtte de gevinster og mål, som er beskrevet i afsnit 4. Arkitekturgrundlaget bygger på analyser og modeller fra Fase 2.

Arkitekturgrundlaget ligger til grund for Scenarie 2 og 3, mens Scenarie 1 ikke umiddelbart efterlever grundlaget.

9.2 Den nuværende arkitekturmodel

I den eksisterende model er arkitekturen designet med udgangspunkt i, at tjenesteudbyder indgår aftale direkte med identitetsgaranten (leverandøren af NemID).

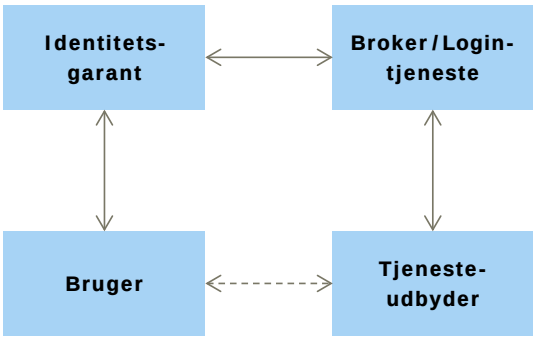
Denne arkitekturmodel er egnet i en situation med kun en identitetsgarant, fordi den er enkel og ikke kræver styring i større omfang.

Modellen er blevet suppleret med login-tjenester, som en funktion mellem identitetsgarant og tjeneste. Bl.a. har det offentlige etableret en fælles login-tjeneste, NemLog-in.

9.3 Forslag til en ny arkitekturmodel

I dette afsnit analyseres en arkitektur med en løsere kobling mellem tjenesteudbyder og identitetsgarant ved at introducere en broker (login-tjeneste, svarende til NemLog-in), som illustreret i Figur 10.

Figur 10: Broker-baseret arkitekturmodel



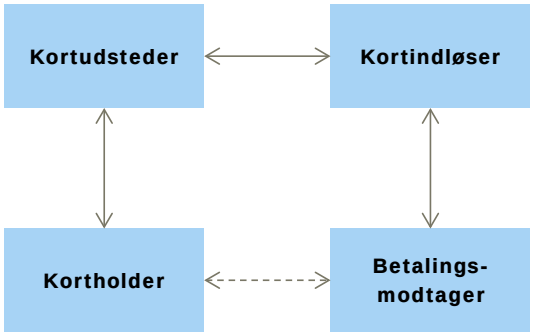
Modellen er behandlet som et muligt arkitekturmæssigt koncept som led i den forudgående tekniske analyse[5] og i den sammenhæng vurderet som den mest fleksible i forhold til fremtidig understøttelse af nye forretningsbehov og teknologier og kommercielt mest åbne i forhold til eventuelle nye markedsaktører.

En broker – login-tjeneste – er en enhed, der indsætter et ekstra abstraktionslag og sikrer en løsere kobling mellem identitetsgarant og tjenesteudbyder.

Denne model svarer til modellen for betalingskort-infrastrukturen som vist på Figur 11, hvor kortholderen (svarende til brugeren) forbindes til betalingsmodtager (svarende til tjenesteudbyder)

[5] Næste generation af NemID. Fase 2 – Teknisk analyse. November 2014. Indgår som Bilag 4: Fase 2-rapport med bilag.

gennem kortudsteder (svarerende til identitetsgarant) og kortindløser (svarende til broker). Modellen har vist sig meget skalerbar i praksis, både i forhold til antallet af aktører og transaktioner.



Figur 11: Arkitektur til betalingskort-infrastruktur

Som nævnt anvender langt hovedparten af offentlige tjenesteudbydere allerede denne model, med NemLog-in som broker. Ligeledes fungerer sundhedsområdets SOSI STS'ere som brokere.

Det er væsentligt for den samlede sikkerhed, at både identitetsgaranter og brokere har et højt sikkerhedsniveau. Dette kan sikres gennem en række mekanismer. Certifikat-politikker kan som nu stille krav til certifikatudstedere (identitetsgaranter). Derudover vil der være behov for at gennemføre supplerende regulering af både identitetsgaranter og brokere eventuelt gennem et trust framework for de dele af infrastrukturer, der ikke er dækket af traditionel PKI. Sikkerhedskrav kan fastlægges gennem lovmæssig regulering eller via akkrediteringsordninger. Krav bør i videst mulig omfang være funderet på åbne og anerkendte internationale standarder. RMC-ICG vurderer, at en offentlig løsning som NemID nyder så stor tillid, at man med fordel kan etablere en attraktiv akkreditering, der over for brugerne signalerer, at en given identitetsgarant eller broker er "NemID-godkendt".

Ved understøttelse af både identitetsgarant og broker i en akkrediteringsordning vil det være muligt at tilknytte tiltag, der bidrager til den samlede sikkerhed. Således kan man stille krav om anvendelse af de såkaldte EV-certifikater i forbindelse med browserbaserede login hos brokeren, og man kan introducere et samlet domæne, som brugere kan genkende, hvorunder akkrediterede brokere lægger deres login- og signeringstjenester. Eksempelvis kan Digitaliseringsstyrelsen registrere domænet "nemidgodkendt.dk"[6], og i forbindelse med en akkreditering kan broker X få brugsretten til "brokerX.nemidgodkendt.dk" eller lignende.

9.3.1 Fordele

Der er en række fordele med denne arkitekturmodel, særligt når udviklingen går i retning af, at der er flere identitetsgaranter. Det sker bl.a. som følge af eIDAS-forordningens krav om, at borgere fra andre EU-lande skal kunne anvende deres lokale eID i Danmark. Derfor skal danske offentlige tjenesteudbydere kunne modtage udenlandske eID. I stedet for at hver enkelt tjenesteudbyder implementerer dette, er der planer om at etablere nationale eID-gateways (PEPS[1]). Sådanne gateways kan umiddelbart implementeres ved at indarbejde funktionalitet hos en broker til at modtage eID fra andre EU-medlemsstater. Der er i Digitaliseringsstyrelsen igangsat en række analyser af juridiske og tekniske forhold i relation til eIDAS-forordningen, som skal afdække dette mere konkret.

Arkitekturmodellen åbner for – som for betalingskort – at brugerne kan anvende flere forskellige eID fra flere identitetsgaranter. For tjenesterne betyder det, at de kun skal have forbindelse til én

[6] Der bør vælges et simpelt domænenavn, der let genkendes af brugerne, og som ikke oplagt kan misbruges ved typosquatting og lignende.
[1] PEPS = Pan European Proxy System.

broker, som så håndterer forbindelsen til forskellige identitetsgaranter. Tjenesteudbyder behøver således ikke have kendskab til de enkelte identitetsgaranter, men skal blot definere en politik for et ønsket veldefineret sikkerhedsniveau.

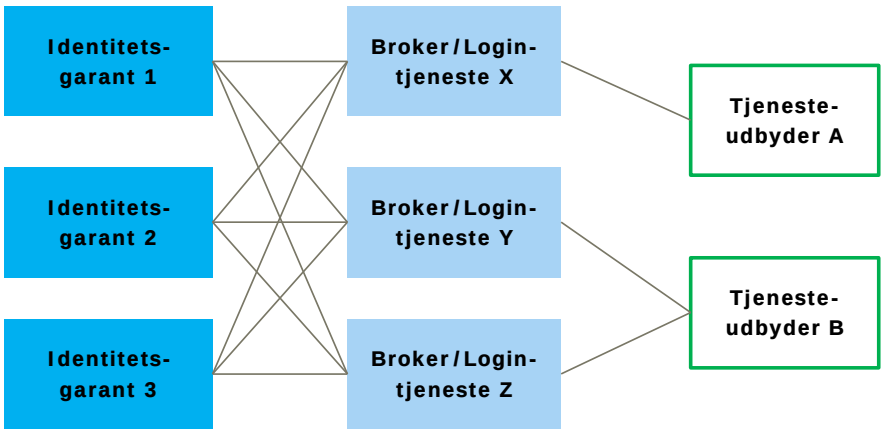
Anvendelse af en broker-baseret arkitektur åbner desuden mulighed for, at tjenesteudbydere kan få mere relevante og branchespecifikke identitetsdata for den konkrete kontekst, uden at identitetsgaranten skal akkumulere en lang række informationer om brugerne. Dette kendes allerede i dag fra sundhedssektoren, hvor SOSI STS'erne fungerer som brokere og tilfører information om brugerne fra eksempelvis Sundhedsstyrelses autorisationsregister.

I forhold til en infrastruktur med flere identitetsgaranter vil anvendelse af brokere skjule kompleksiteten for den enkelte tjenesteudbyder. Anvendelse af en broker vil således minimere påvirkning af tjenesteudbyder ved ændringer i den bagvedliggende infrastruktur mellem identitetsgaranter og broker. Dette kan være ændringer i form af teknologiskift hos de eksisterende identitetsgaranter og etablering af nye identitetsgaranter.

Samtidig vil en tjenesteudbyder have mulighed for at indgå aftale med flere brokere med henblik på at sikre størst mulig oppetid.

Det skal bemærkes, at en identitetsgarant kan operere som broker, ligesom en større tjenesteudbyder kan etablere egen broker-funktion.

Figur 12: Arkitektur med flere identitetsgaranter og brokere



Som tidligere nævnt vil en af de væsentligste fordele ved anvendelse af brokere være en løsere kobling mellem tjenesteudbydere og identitetsgaranter. RMC-ICG vurderer, at dette kan understøtte en flerleverandørstrategi, da adgang til markedet vil være væsentligt lettere for identitetsgaranter og brokere, således at det bliver lettere at skifte dele af løsningen på sigt. For de enkelte parter vil der være væsentligt færre integrationspunkter, og en del kompleksitet bliver skjult.

Desuden kan den løsere kobling mellem tjenesteudbyder og identitetsgarant betyde større agilitet i NemID-økosystemet, idet ændringer hos identitetsgaranten i mindre grad påvirker tjenesteudbyderne direkte. Skiftet i den eksisterende løsning fra Java-klient til JavaScript-klient illustrerer dette. En række private tjenesteudbydere har været nødt til at foretage ændringer i deres løsning for at understøtte JavaScript-klienten. Offentlige tjenester, der benytter NemLog-in som broker, har derimod kunnet fortsætte uden ændringer, da opdateringen udelukkende påvirkede NemLog-in.

Der er mulighed for, at brugerne kan vælge løsninger fra forskellige identitetsgaranter og dermed opnå større redundans. Ligeledes kan tjenesteudbydere vælge at integrere til flere brokere. Hvis der bliver etableret flere identitetsgaranter og flere brokere, kan modellen dermed sikre en mere robust infrastruktur med færre 'single-points-of-failure'.

RMC-ICG vurderer, at anvendelse af akkrediterede brokere vil øge den samlede sikkerhed i infrastrukturen. Brugeren vil i højere grad anvende deres akkreditiver (login-faktorer) hos få brokere med stor fokus på it-sikkerhed frem for mange forskellige større og mindre tjenesteudbydere med fokus på kerneforretning, og som ikke nødvendigvis har et højt it-sikkerhedsniveau. Dette bliver

yderligere udtalt ved introduktion af flere sikkerhedsniveauer, da det må forventes at øge udbredelsen til endnu flere tjenesteudbydere. Hvis angriberen får kontrol over en tjenesteudbyders hjemmeside, har angriberen mulighed for at erstatte NemID-klienten med en klient, der ligner NemID-klienten, men som i stedet sender brugerens indtastede data til angriberen. RMC-ICG vurderer, at introduktion af brokere således kan mitigere risikoen for 'man-in-the-middle-angreb'.

En broker-baseret arkitektur kan indføres fleksibelt og gradvist, hvor tjenesteudbydere kan vælge at understøtte login og signering som en integreret del af egen hjemmeside eller at benytte en broker.

Introduktionen af brokere kan baseres på frivillighed og med tiltag, der fremmer overgang til brug af brokere, herunder markedsføring af akkrediterings-/mærkningsordning af brokere. Alternativt kan der stilles krav om, at der benyttes en godkendt broker.

9.3.2 Ulemper

Modellen kan øge den samlede kompleksitet og dermed omkostninger for den samlede infrastruktur. RMC-ICG vurdere dog, at modellen er mere åben for konkurrence, og at de samlede fællesoffentlige udgifter ikke vil overstige en model uden brokere.

I forhold til en model, hvor tjenesteudbydere er koblet direkte til identitetsgaranter, er der med introduktion af brokeren endnu en part, der kan påvirke den samlede oppetid for tjenesteudbyderen i negativ retning. Den enkelte tjenesteudbyder kan mitigere risikoen ved at indgå aftale med flere brokere som illustreret for tjenesteudbyder B i Figur 12.

9.3.3 Udfordringer

Der er en række udfordringer, som skal håndteres i forbindelse med anvendelse af brokere.

Der skal etableres en forretningsmodel, der understøtter anvendelse af broker-funktion. Forretningsmodellen skal gerne gøre det fordelagtigt for identitetsgaranter og brokere at indgå aftaler og minimere risikoen for udnyttelse af en dominerende stilling på markedet for henholdsvis identitetsgarant og broker. Det bør overvejes, om der skal introduceres regler, eventuelt som led i en akkrediteringsordning, som kan regulere markedet. Det vil have negativ indflydelse på brugeroplevelsen, hvis ikke alle brokere understøtter alle identitetsgaranter. I den eksisterende løsning oplever brugere af "NemID på hardware" et tilsvarende problem, hvor det ikke er alle tjenesteudbydere, der understøtter denne variant af NemID. Dermed får brugerne ikke den fulde udnyttelse af løsningen.

Det skal sikres, at der som minimum er en identitetsgarant og en broker for både offentlige og private tjenesteudbydere. Det bemærkes i den sammenhæng, at der allerede i dag findes kommercielle brokere på det danske marked:

- DSI-Next (SikkerAdgang).
- KMD (NemAdgang).
- Nets (E-Ident).
- Signicat (Signicat eID).

Der er en række problemstillinger i forhold til sikring af brugernes privatliv, der skal håndteres. Eksempelvis bør det vurderes, om der skal udvikles et interface, der sikrer, at brokere ikke har adgang til signeringsdata i forbindelse med, at de fungerer som signeringstjenester. Ved introduktion af tjenesteudbyderspecifikke pseudonymer bør det vurderes, om pseudonymerne skal være ens på tværs af brokere for at understøtte tjenesteudbyderes anvendelse af flere brokere. Visse brugere vil finde dette naturligt og brugervenligt, mens andre vil finde denne funktionalitet kompromitterende for deres beskyttelse af privatlivet i forhold til kobling på tværs af systemer. Tjenesteudbydere vil foretrække samme tjenesteudbyderspecifikke pseudonym på tværs af brokere. I visse sammenhænge vil dette være et krav, eksempelvis ved udelukkelse af brugere fra en tjeneste efter brud på regler for anvendelse af tjenesten.

For at sikre en sikker og omkostningseffektiv integration for tjenesteudbydere og for at støtte konkurrence på markedet skal broker som minimum udstille en eller flere veldefinerede åbne og stan-

dardiserede interfaces til tjenesteudbydere. Dette kan typisk være et SAML 2.0, som det kendes fra NemLog-in og OpenID Connect, som anvendes af Google+ Sign-in. Tilsvarende bør der stilles veldefinerede interfaces til rådighed for digital signering.

9.3.4 Migrering

Den broker-baserede model anvendes som nævnt allerede hos alle offentlige tjenesteudbydere, der er koblet til NemLog-in. Desuden anvender en række private tjenesteudbydere ligeledes brokere gennem kommercielle login-løsninger. I denne situation vil migreringen primært handle om at sikre, at brokere, herunder NemLog-in, lever op til besluttede krav i trustmodellen for at opnå en akkreditering.

De tjenesteudbydere, der i dag har integreret NemID direkte på egen side, og som dermed ikke anvender en broker, bør ændre løsningen til at kunne tilgås af en broker.

9.4 Konklusion

RMC-ICG anbefaler, at en kommende NemID-infrastruktur baseres på anvendelse af en arkitektur med broker-funktionalitet.

RMC-ICG anbefaler, at brokere med tilhørende funktionelle og sikkerhedsmæssige krav beskrives som en national standard med tilknytning til et trust framework, og at der etableres en akkrediteringsordning, der markedsføres som en del af de offentlige standarder over for brugere og tjenesteudbydere.

10. Migreringsproces

I dette afsnit behandles de risici, som vurderes relevante i forhold til at sikre, at der kan migreres til næste generation NemID som beskrevet i scenarierne uden afbrydelser i borgeres, virksomheders og myndigheders anvendelse af NemID. NemID's rolle som grundlag for digital forvaltning og andre digitale løsninger betyder, at kravene til kontinuerlig drift og til at undgå problemer ved overgangen til nye løsninger og eventuel ny leverandør er meget høje.

Analysen behandler risici i forbindelse med migreringsproces samt behandler, hvordan risici kan minimeres.

10.1 Migreringsalternativer og risikoanalyse

Der er flere migreringsmuligheder, afhængigt af hvilken leverandør der vælges.

Migreringsforløb 1:

I dette forløb vinder den nuværende leverandør det kommende udbud og kan derfor fortsætte med drift af den nuværende løsning, indtil nye løsninger kan supplere eller tage over.

Dette migreringsforløb har lav risiko for manglende tilgængelighed, idet den nuværende installation kan driftes videre, indtil nye løsninger supplerer og erstatter den.

Migreringsforløb 2:

I dette forløb udvikler en ny leverandør (her og i det følgende: eller nye *leverandører*) nye løsninger. Brugerne og tjenesteudbyderne migreres til den nye løsning *på én gang* eller over en meget kort periode (fx en måned).

Dette forløb indebærer risiko for, at den næste leverandør ikke kan nå at have en velfungerende løsning klar til det aftalte tidspunkt. Det kan afhjælpes ved at have mulighed for, at den nuværende leverandør kan drive den nuværende løsning, indtil den nye løsning er klar.

Selve migreringen af mere end 4,5 millioner NemID-nøglekortsbrugere, mere end 500.000 nøglefilsbrugere og tilslutningen af mere end 275 tjenesteudbydere og login-tjenester vil være ressourcekrævende. Udsendelsen af løsning til engangskode (fx nøglekort eller nøgleviser) vil kræve tid, da der skal udsendes mere end 4 millioner breve, hvis der vælges en løsning, der kræver udsendelse med postvæsenet i forbindelse med migreringen. Supportbehovene i forbindelse med et skift vil være store, hvilket taler for at sprede skiftet over så lang tid, at supportfunktionen kan dække behovene med en rimelig ressourceindsats.

Sandsynligheden for manglende teknisk tilgængelighed eller funktionel tilgængelighed (brugerne kan ikke få en ny løsning til at fungere) vil være stor med en kort periode til et skifte.

Migreringsforløb 3:

I dette forløb indgås der aftale med den nuværende leverandør om betingelserne for at videreføre nuværende installation, indtil den kan udfases. Det giver en ny leverandør tid til parallelt at udvikle og idriftsætte nye løsninger og dermed mulighed for en *glidende overgang* til nye løsninger.

Dette forløb betyder lav risiko for manglende tilgængelighed, og migreringsforløbet er robust over for længere leveringstid hos ny leverandør. Forløbet kan indebære, at den nuværende leverandør skal drive den nuværende løsning i flere år med deraf følgende omkostninger for det offentlige.

Migreringsforløb 4:

I dette forløb bygger en ny leverandør en ny bagudkompatibel installation, hvortil den nuværende løsning migreres fra den nuværende leverandør og drives i en længere periode.

En ny leverandør udvikler parallelt nye løsninger og idriftsætter disse.

Da en ny leverandør skal opbygge en ny løsning på grundlag af dokumentation af den nuværende løsning, er sandsynligheden for driftsproblemer ved skiftet eller i perioden derefter stor.

Tabel 6: Samlet risikovurdering vedrørende migrering

Fremtidig leverandør	Samlet risikovurdering – manglende tilgængelighed
1: Den nuværende leverandør, som fortsat driver nuværende installation, indtil den udfases og parallelt udvikler og idriftsætter nye løsninger.	Lav
2: Ny leverandør udvikler ny løsning, som over en kort periode eller på én gang erstatter den nuværende løsning.	Høj
3: Den nuværende leverandør 3A: Driver fortsat nuværende installation, indtil den udfases. Ny leverandør 3B: Udvikler og idriftsætter nye løsninger parallelt.	Lav
4: Ny leverandør 4A: Bygger ny, bagudkompatibel installation, hvor nuværende migreres fra den nuværende leverandør. 4B: Udvikler og idriftsætter nye løsninger parallelt.	Høj

Set ud fra målsætningen om kontinuerlig høj driftssikkerhed er det RMC-ICG's anbefaling, at der arbejdes med en migreringsløsning som ovennævnte migreringsforløb 3. I kombination med den anbefalede arkitekturmodel (se afsnit 9), som afkobler tjenester fra identitetsgaranter, vil denne migreringsløsning give lav risiko for afbrydelser i NemID og give robusthed i forhold til eventuelle forsinkelser.

Der vil i alle migreringsforløb være fællesoffentlige udgifter til migreringen, dels til fortsat at drive den eksisterende løsning i en periode, dels til bl.a. support i forbindelse med skiftet.

Hertil kommer, at borgere, virksomheder og myndigheder vil have udgifter i forbindelse med migreringen (virksomheder og myndigheder både som arbejdsgivere og som tjenesteudbydere).

10.2 Konklusion

Migrering fra nuværende til ny løsning indebærer risici for manglende tilgængelighed ved migreringen og i en periode herefter.

Det kan helt eller delvist håndteres ved at indgå aftaler med den nuværende leverandør om betingelserne for fortsat drift af den nuværende løsning i en periode efter kontraktens udløb.

Det skal desuden håndteres ved at gennemteste løsningen før idriftsættelse og ved at planlægge en trinvis indførelse af den ny løsning.

11. Indholdet af næste generation NemID

11.1 Overblik over scenarierne

De overordnede forretningsmæssige behov er afdækket i Fase 1 og prioriteret af styregruppen med henblik på at udarbejde beslutningsgrundlag for næste generation NemID. Behovene er en meget sikker NemID-løsning, der dækker de nuværende anvendelsesområder samt sikrer kontinuitet og bagudkompatibilitet for interessenterne.

Alle scenarierne har dækningen af disse overordnede behov som grundlag.

Scenarierne er opbygget efter drøftelse mellem Digitaliseringsstyrelsen og RMC-ICG, således at de løsningselementer, der er drøftet i styregruppen, er fordelt på tre scenarier og et særskilt løsningselement.

Scenarie 1 viser en løsning baseret på samme arkitektur og ny teknologi, med minimale ændringer i forhold til nu.

Scenarie 2 har fokus på forbedringer for borgere (1-faktor-login) og for erhvervsområdet (brug af NemID privat i erhvervssammenhæng) samt bedre administrative løsninger. Scenariet indeholder samme funktioner som nu, men med en ny arkitektur samt mulighed for at anvende udbredte teknologiske løsninger. Dette muliggør flere sikkerhedsniveauer samt adskillelse af autentifikation og signering – dog uden at brugerne må opleve denne opdeling. Desuden dækkes de følgende forretningsmæssige behov, primært med fokus på at imødekomme virksomheders og myndigheders behov som arbejdsgivere:

- Brede anvendelsesmuligheder for NemID privat til erhvervsformål.
- Bedre løsninger til udstedelse og administration af NemID medarbejdersignatur.

Scenarie 2 er grundlag for Scenarie 3, som yderligere indeholder dækning af følgende forretningsmæssige behov:

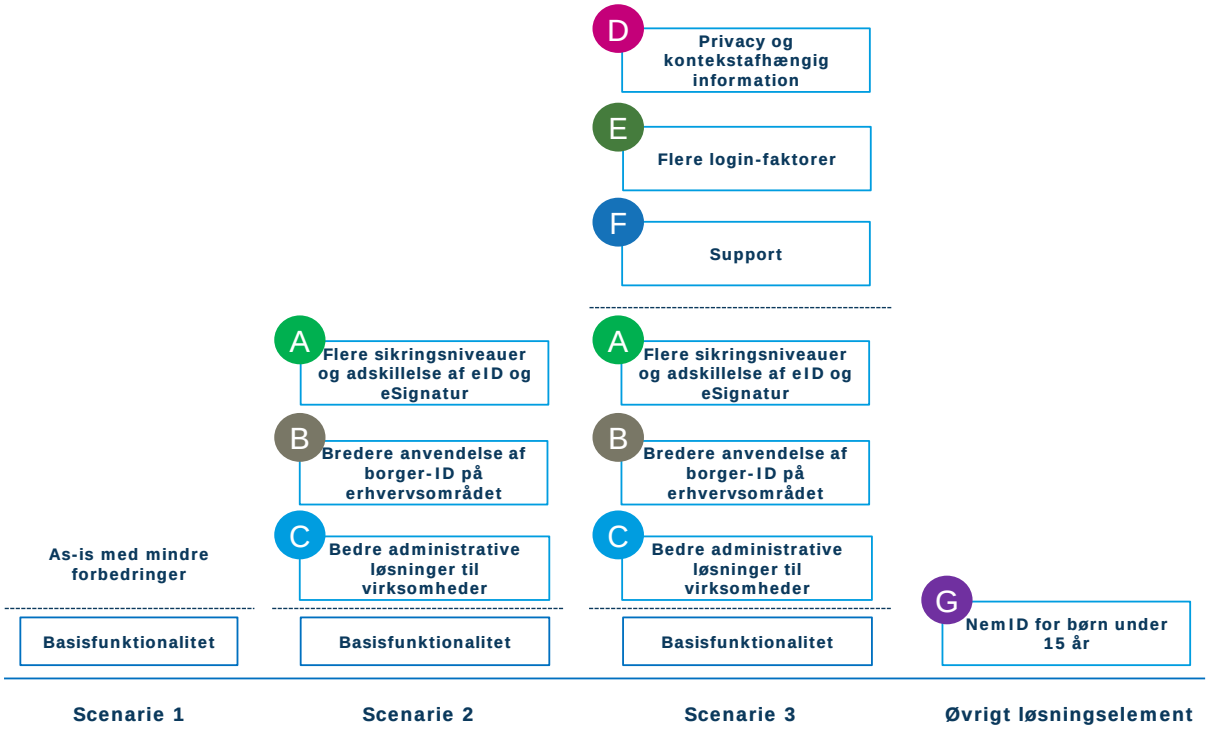
- Brugernes behov for øget privacy og tjenesteudbydernes behov for kontekstafhængig information.
- Mulighed for flere login-faktorer for at dække brugernes behov for flere valgmuligheder og mere brugervenlige og situationsrelevante login-faktorer.
- Bedre og billigere support primært for erhverv, men også for borgere.

Løsningselementet *NemID til børn under 15* er beskrevet under afsnit 0 og indgår ikke som en del af scenarierne, da analysen har vist, at dette er for dyrt i forhold til de opnåede gevinster.

Opdelingen i scenarier og scenarieelementer er sket for at kunne fremstille og analysere de mange løsningsmuligheder og kombinationer af løsningsmuligheder på en overskuelig måde. Hvert enkelt element rummer i sig selv en række teknologiske valg og muligheder. Der er generelt ikke stærke teknologiske bindinger mellem løsningselementerne i sin helhed, der afgørende begrænser udfaldsrummet for beslutninger vedrørende næste generation NemID. I gennemgangen af scenarier og scenarieelementer beskrives eventuelle bindinger.

Dette betyder, at det er muligt at flytte på løsningselementerne mellem scenarierne, idet det fx er muligt at give bedre og billigere support i både Scenarie 1 og 2. Det betyder også, at der i arbejdet frem mod implementering af næste generation NemID skal træffes beslutninger om den konkrete udmøntning af indholdet i de valgte løsningselementer.

Figur 13: Oversigt over scenarierne og løsningselementerne



11.2 Grundlæggende principper og forudsætninger

Det er et fælles grundlag for alle tre scenarier, at håndtering af autentificering sker med udgangspunkt i en central registrering af identitet og login-faktorer, således at hovedparten af brugerne ikke skal installere nøglefiler, klientsoftware eller lignende på eget udstyr. Ligeledes bygger scenarierne på central lagring af privatnøgler til signering hos leverandøren.

Det sker på grundlag af erfaringerne i Danmark med digital signatur fra 2003 (OCES1), som viste store praktiske og sikkerhedsmæssige udfordringer for brugerne i håndteringen af nøglefiler. Dette betød store supportudgifter, og at anvendelsen blev hæmmet. Til gengæld har erfaringerne med NemID (OCES2) med central lagring af privatnøgler været en stor succes, og det har været muligt at udbrede løsningen til 90 % af den voksne befolkning.

Andre lande, der enten baserer sig på nøglefiler på brugerens udstyr eller på SmartCards, har også erfaringer med ringe udbredelse og lav anvendelseshyppighed. Både Tyskland og Belgien baserer sig på SmartCards, som har ringe udbredelse og anvendes meget lidt.

Det er ligeledes et fælles grundlag, at der fortsat skal være mulighed for en nøglefilsløsning til virksomheder og myndigheder, som har udtrykt et meget stort behov for, at denne løsning fortsætter.

Scenarier og løsningselementer baserer sig alle på det grundlæggende princip, at NemID håndterer autentificering (login) og signering, mens forhold vedrørende fuldmagter og rettigheder håndteres andre steder i infrastrukturen, fx i NemLog-in.

Der indgår følgende i løsningen:

En central lagring af privatnøgler hos leverandøren samt 2-faktor-login med kodeord og engangskode (fx nøglekort) til NemID privat og NemID medarbejdersignatur

En central lagring af privatnøgler fortsætter som nu, omfattende både autentifikation og signering. Teknisk set indebærer det autentifikation og signering som en service og med engangskodeord (OTP) i form af nøglekort eller tilsvarende løsninger. Der skal også være mulighed for andre login-faktorer som hardware tokens og nøglefiler.

Borgere og virksomheder vil fortsat have mulighed for at anvende forskellige løsninger som almindeligt nøglekort, nøglekort med stor skrift og telefonservice til blinde (eller tilsvarende løsninger).

Central lagring og anvendelse af privatnøgler hos leverandøren er i overensstemmelse med eIDAS- forordningen. I forordningens bilag II stk. 3 og stk. 4 behandles eksplicit krav til løsninger, hvor generering og forvaltning af private nøgler (benævnt "elektroniske signaturgenereringsdata") udføres af en tillidstjenesteudbyder.

Nøglefil (virksomheder og myndigheder)

Nøglefilsløsningen fortsætter som nu. Virksomheder og myndigheder vil fortsat have mulighed for at anvende forskellige løsninger som i dag, herunder nøglefil som nu.

Andet

Virksomhederne vil fortsat have mulighed for at anvende virksomheds- og funktionscertifikater. Desuden skal løsningen kunne etableres i samarbejde med en privat partner.

11.3 Arkitektur og teknologi

De tre scenarier bygger på to forskellige arkitekturer og teknologiske platforme.

Det er primært to scenarieelementer – "flere sikringsniveauer" og "privacy" – der har den største betydning for arkitekturen og den konkrete teknologiske implementering af den kommende NemID-infrastruktur.

Understøttelse af flere sikringsniveauer bygger på en adskillelse af eID og eSignatur – som konsekvens af at have *flere autentifikationsniveauer*, men kun *ét* signeringsniveau.

Dette betyder, at "flere sikringsniveauer" og "adskillelse af eID og eSignering" betragtes som *ét* samlet scenarieelement.

Med en adskillelse af eID og eSignering følger, at eID-funktionalitet i løsningen – og dermed Scenarie 2 og Scenarie 3 – skal baseres på andre autentifikations-teknologier og interfaces end PKI, fx SAML 2.0 eller forskellige PKI-løsninger. Det betyder, at arkitekturen vil bygge på en kombination af *identity-management*-systemer og PKI.

Scenarie 1 lægger derimod op til en arkitektur, hvor PKI fortsat vil anvendes som den grundlæggende teknologi og som samme grænseflade – både for autentificering og signering.

Understøttelse af scenarieelementet om øget privacy og kontekstafhængig information om brugere – i Scenarie 3 – vil kunne bygge på forskellige *ikke-PKI*-baserede teknologier. SAML 2.0 og OpenID Connect er her de mest modne kandidater.

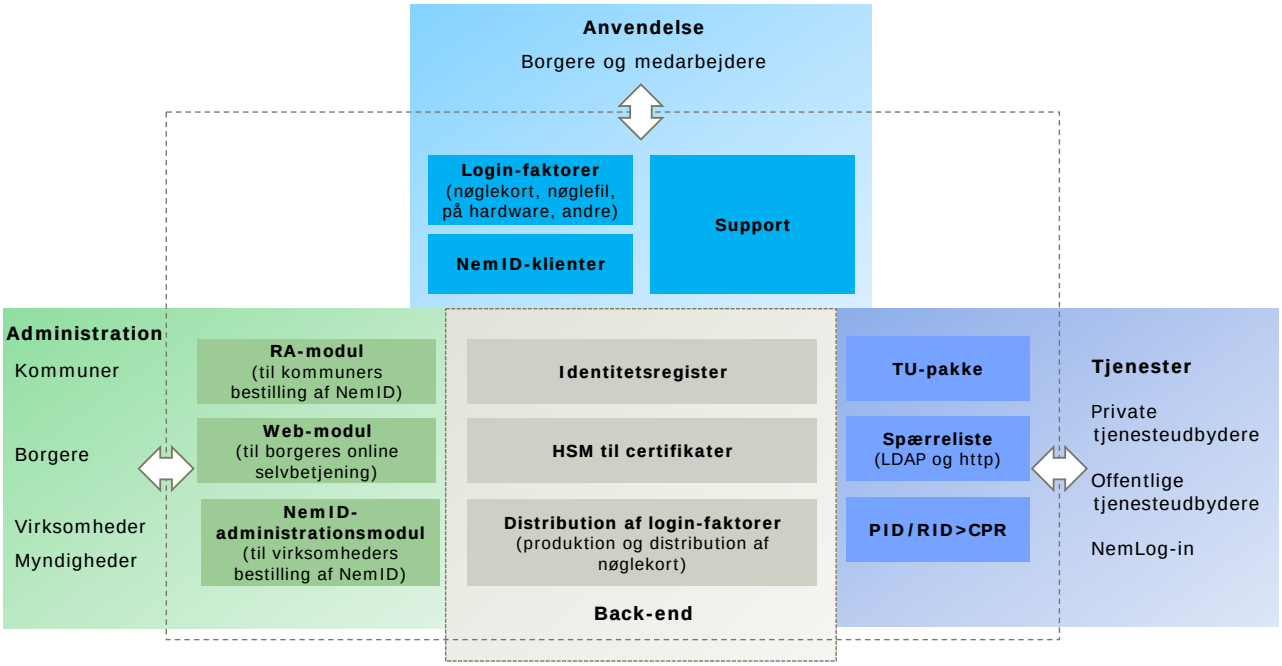
Begge scenarieelementer vil således kunne bygge på samme teknologiske platform. Ligeledes er det gældende for dem begge, at de på en teknologisk 'elegant' måde anvender den grundlæggende arkitekturmodel og rollefordeling, som præsenteret i afsnit 9.

Andre elementer præsenteret i Scenarie 2 og Scenarie 3 er ikke bestemmende for de fremtidige teknologivalg i løsningen, selvom de ikke er fuldstændig teknologisk uafhængige. Således påvirker fx scenarieelementerne "support" og "flere login-faktorer" hverken den kommende teknologi eller den overordnede arkitekturmodel for løsningen.

11.4 Basisfunktionalitet

I dette afsnit præsenteres de fælles funktioner, som den nuværende NemID-løsning indeholder, og som også skal indgå i fremtidige løsninger.

Figur 14: Funktioner i NemID



Figuren og gennemgangen herunder beskriver funktionerne i NemID. De svarer til de nuværende funktioner med enkelte undtagelser.

Administration omfatter bestilling af NemID og efterfølgende administration (for virksomheder og myndigheder). Til administration er der følgende funktioner:

- **RA-modul:** Et system til registrering af nye NemID-brugere for registreringsenheder, fx i kommuner.
- **Web-modul:** Et system, hvor borgere kan bestille NemID og udføre administrative opgaver (https://service.nemid.nu/dk-da/bestil_nemid/index.html?execution=e1s1)
- **NemID-administratormodul:** Et system, hvor virksomheder og myndigheder kan tilslutte sig og bestille NemID samt udføre administrative opgaver (medarbejdersignatur.dk). Mange opgaver kan desuden udføres i en systemsnitflade (API).

Anvendelse omfatter brugen af NemID i forhold til borgere og medarbejdere, og dækker følgende funktioner:

- **Login-faktorer** omfatter faktorer som kodeord og engangskoder (fx nøglekort). Login-faktorer skal enten kunne bruges af personer med særlige behov, eller der skal være løsninger, der dækker deres behov (svarende til de nuværende løsninger med nøglekort med stor skrift og telefonservice til blinde).
- **NemID-klienter:** Løsningen skal indeholde en eller flere klienter, der understøtter login-faktorer. Den nuværende løsning (december 2014) har en Java-klient (under udfasning), en JavaScript-klient (til login) og en Opensign-JavaScript-klient (til signeringsformål).
- **Support** omfatter support til borgere, virksomheder og myndigheder både som arbejdsgivere og tjenesteudbydere og til medarbejdere. Den nuværende løsning er gratis i brug for borgere, og delvist for virksomheder, myndigheder og medarbejdere.

Back-end omfatter opgaver omkring håndtering af identiteter og data samt produktion og distribution af login-faktorer, fordelt på følgende funktioner:

- **Identitetsregister** omfatter det system, der håndterer data om identiteter, personer og medarbejdere samt deres login-faktorer.
- **HSM** sikrer, at en person (og kun personen selv) kan få adgang til egne private nøgler til autentifikation og signering.

- **Distribution af login-faktorer** omfatter systemer til produktion og distribution af login-faktorer. Nøglekort skal trykkes og kobles meget sikkert til den rigtige bruger og sendes sikkert. Nøglevisere skal produceres (eventuelt anskaffes fra underleverandør) og kobles meget sikkert til den rigtige bruger og sendes sikkert. Brev med midlertidig adgangskode skal distribueres via tilstrækkelig sikker kanal.

Tjenester er de udbudte funktioner relateret til private tjenesteudbydere, offentlige tjenesteudbydere og NemLog-in:

- **Tjenesteudbyderpakker (TU-pakke)** er en kodesamling, der letter tjenesteudbyderes arbejde med at etablere tjenester, der anvender NemID.
- **Spærrelister** giver tjenester adgang til en liste over spærrede certifikater (OCSP) med adgang via LDAP eller http, eller mere direkte via OCSP.
- **PID/RID->CPR** er en tjeneste ejet af Digitaliseringsstyrelsen, hvor tjenesteudbydere kan få oplyst eller verificeret CPR-nummeret på en person med et givet PID- eller RID-nummer[7].

Ovennævnte funktioner er mere detaljeret beskrevet i bilag 1: "Afdækning af relevant funktionalitet i den eksisterende NemID for næste generation NemID" og omfatter alle de funktioner, der er markeret obligatorisk.

Yderligere funktioner, som ikke er afbilledet i Figur 14, er:

Virksomheds- og funktionscertifikater til sikker kommunikation mellem it-systemer.

Testfaciliteter er de funktioner, der skal imødekomme krav om øget testbarhed. Det skal omfatte væsentligt forbedrede muligheder for test af tilslutninger af tjenesteudbyderes løsninger samt overførsel af brugerdata i forbindelse med administration af NemID. I processen med udarbejdelse af foranalysen er der nævnt behov for, at testløsningen giver mulighed for at teste NemID i sammenhæng med CPR og NemLog-in og muligvis andre tjenester.

Støttesystemer er de systemer, der understøtter driften af løsningen i form af sikkerhedsløsninger, overvågning, dokumentation, deployment, rapportering om anvendelse, snitflader til supporttjenester m.m.

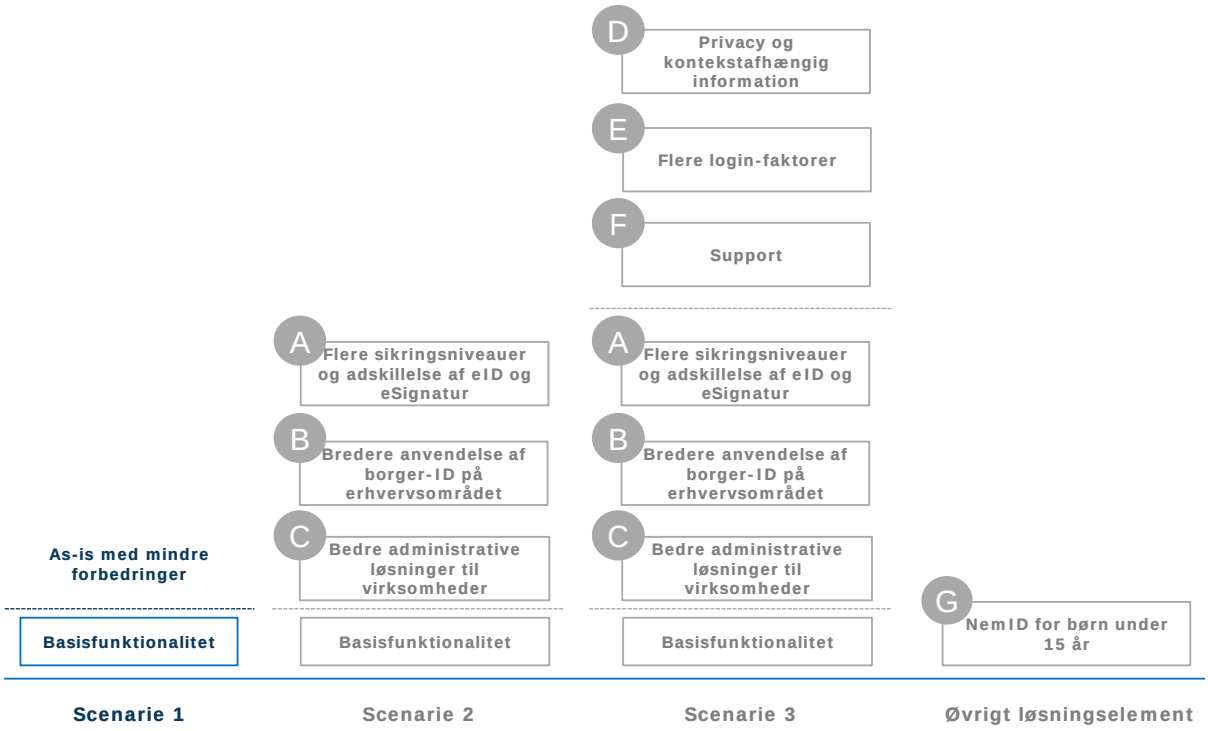
[7] PID = CPR-tjeneste til validering af NemID privat.
RID = CPR-tjeneste til validering af NemID medarbejdersignaturer.

12. Scenarie 1

12.1 Præsentation af scenariet

Scenarie 1 skal dække de samme behov som nu, men med mindre forbedringer inden for den nuværende ramme.

Figur 15: Scenarie 1



Løsningen indeholder basisfunktionaliteten, herunder:

- En central lagring af privatnøgler hos leverandøren og 2-faktor-login med kodeord og engangskode (fx nøglekort) til NemID privat og NemID medarbejdersignatur.
- Nøglefil til NemID til erhverv (herunder mulighed for decentralt at anvende signaturserverløsninger).

I forbindelse med udbuddet vil det være muligt at kræve visse forbedringer i brugergrænsefladen både for borgere og virksomheder for at opnå øget brugervenlighed (fx kan ønskerne i Fase 1 om mere forståeligt sprog imødekommes).

Løsningen bygger på samme PKI-baserede arkitektur som den nuværende NemID.

12.2 Funktioner i Scenarie 1

Scenarie 1 indeholder basisfunktionalitet, jf. afsnit 11 næste generation NemID.

12.2.1 Brugervenlighed i Scenarie 1

Såfremt løsningen fortsat skal leveres af den nuværende leverandør, kan der forventes stor overensstemmelse med de nuværende brugergrænseflader.

Såfremt løsningen leveres af en anden leverandør, er det vanskeligt at forudsige præcist, hvilke brugergrænseflader der vil blive leveret.

I begge tilfælde vil dette blandt andet afhænge af kravene i udbudsmaterialet.

12.3 Gevinster

Dette afsnit har til formål at præsentere de gevinster, løsningselementet kan give. Gevinsterne differentieres i forhold til de forskellige relevante brugergrupper.

12.3.1 Borgere

Borgerne forventes at få samme løsning som nu, dvs. en nøglekortsløsning eller lignende og mulighed for nøglefil på hardware, eventuelt med ændringer i brugergrænsefladerne til bestilling og anvendelse (NemID-klienten).

For de borgere, der er tilfredse med den nuværende løsning, og for de borgere, der lægger vægt på kontinuitet, vil scenariet opfylde deres forventninger.

For de grupper af borgere, der har efterlyst forbedringer, vil løsningen ikke imødekomme ønsker og behov for fx 1-faktor-login, valg mellem et større udvalg af login-faktorer og valg mellem flere udbydere af autentifikation og signering.

12.3.2 Virksomheder – herunder private virksomheders medarbejdere

I den nuværende løsning er der cirka 1 million NemID medarbejdersignaturer.

Tabel 7: Antallet af NemID medarbejdersignaturer

NemID medarbejdersignaturer	Antal identiteter (afrundet til hele 1.000)
MOCES nøglekort	377.000
MOCES nøglefil	663.000
MOCES andre	11.000
VOCES	25.000
FOCES	11.000

Alle i tabellen nævnte løsninger vil fortsat blive stillet til rådighed for virksomhederne.

Der vil være samme (begrænsede) gevinster for virksomheder og deres medarbejdere som for borgere.

Der har været en omfattende kritik af løsninger til virksomheder, og i dette scenarie indgår der kun mindre forbedringer i brugergrænsefladerne for virksomhedernes administration af medarbejdere, inden for rammerne af den nuværende løsning, fx i form af mere forståelige skærmbilleder.

Disse løsninger vil derfor kun imødekomme en del af ønskerne til forbedringer fra virksomhederne.

12.3.3 Myndigheder – herunder myndighedernes medarbejdere

Der er indsamlet tal for antal NemID medarbejdersignaturer udstedt til myndigheder, hvilket fremgår af nedenstående tabel.

Tabel 8: Antal NemID medarbejdersignaturer udstedt til myndigheder

NemID medarbejdersignaturer i myndigheder	Antal identiteter (afrundet til hele 10.000)
Regionerne	80.000
Kommunerne	80.000
Regioner og kommuner i alt	**160.000**

*Note til tabel: Tal for kommuner er beregnet på grundlag af tal fra Favrskov og Odense Kommuner og omregnet til alle kommuner på grundlag af befolkningstal.

Alle løsninger for virksomheder stilles også til rådighed for myndigheder.

Der vil være samme (begrænsede) gevinster for myndigheder og deres medarbejde som for borgere.

12.3.4 Private tjenesteudbydere

For private tjenesteudbydere vil scenariet betyde høj grad af bagudkompatibilitet, mens behov for ændringer, fx i form af kontekstafhængig information og 1-faktor autentifikation ikke imødekommes.

12.3.5 Offentlige tjenesteudbydere

Offentlige tjenesteudbydere vil fortsat anvende NemLog-in og skal ikke implementere ændringer i scenariet.

I scenariet skal der ikke implementeres ændringer NemLog-in.

12.4 Vurdering

Dette afsnit har til formål at analysere og vurdere løsningselementet i forhold til relevante parametre, der er udvalgt i dialog med Digitaliseringsstyrelsen.

12.4.1 Arkitektur

Der anvendes samme PKI-baserede arkitektur som i den eksisterende løsning.

12.4.2 Sikkerhed og privacy

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

I takt med udbredelse og størrelse af de værdier, der er beskyttet af løsningen, må der forventes forsøg på angreb. Derfor er det væsentligt, at der fortsat sikres en proces, hvor sikkerheden løbende håndteres og opgraderes, når det vurderes nødvendigt.

Scenarie 1 adskiller sig ikke fra den nuværende løsning i forhold til sikkerhed og privacy, som både nu og fremover kræver en løbende indsats.

12.4.3 Migrering

Migreringen vil afhænge af, hvilken migreringsmodel der vælges, jf. afsnit 10.

Der vil være begrænsede ændringer ved leverandørskifte, men det kan alligevel betyde væsentlige risici for, at NemID bliver utilgængelig i migreringsperioden.

12.4.4 Relation i forhold til private partnere

Scenariet vil ikke ændre på forudsætningerne for at indgå samarbejde med private partnere i forhold til den nuværende situation.

12.4.5 OCES-certifikatpolitikker

RMC-ICG vurderer, at der kun er behov for mindre, almindelige tilretninger af OCES-certifikatpolitikken i dette scenarie.

RMC-ICG anbefaler dog, at man ved revision af OCES-certifikatpolitikkerne vurderer, om man med fordel kan samle certifikatpolitik for OCES-virksomhedscertifikater og OCES-funktionscertifikater med henblik på at minimere kompleksiteten.

12.4.6 Økonomi

Som forudsætning for de følgende udgiftsskøn indgår, at Scenarie 1 grundlæggende vil koste det samme som den nuværende løsning, både hvad angår udvikling, drift og support. Herved arbejdes der ud fra den forudsætning, at løsningen bygges fra ny. I en situation, hvor den eksisterende leverandør vælger at byde ind med den nuværende løsning, ville omkostninger til udvikling sandsynligvis være mindre.

I det følgende gennemgås økonomien mere detaljeret.

12.4.6.1 Fællesoffentlige udgifter

De fællesoffentlige udgifter vil afhænge meget af, hvilken løsning de kommende leverandører byder ind med. Her er forudsætningen, at der bydes ind med en løsning svarende til den nuværende løsning, med de mindre forbedringer, der er beskrevet ovenfor. Det indgår i beregningerne, at der skiftes til en ny løsning.

Udvikling

De samlede udgifter til anskaffelse (udvikling, etablering og videreudvikling) af den nuværende løsning har været cirka 90 millioner kroner. Heri indgår både de oprindelige udviklingsudgifter og videreudvikling.

Krav til øget sikkerhed og forventninger til mindst samme brugervenlighed som nu påvirker udgifterne i opadgående retning.

Muligheden for at anvende standardkomponenter, eventuelt open source, og mere effektive udviklingsmetoder påvirker udgifterne i nedadgående retning.

Samlet set vurderes udgifterne til udvikling af en ny løsning at være på niveau med de nuværende udgifter, dvs. 70-110 millioner kroner

Videreudvikling

Der regnes med 10 % til årlig videreudvikling, svarende til niveauet for det nuværende NemID.

Drift og support

De samlede årlige udgifter til drift (drift og forvaltning af løsningen) og support skønnes at være på 40-60 millioner kroner. Det skal ses i forhold til udgiftsniveauet i 2014 på 40 millioner kroner.

Support

Det skønnes, at overgang til en ny løsning vil betyde forøgede supportudgifter i det, eller de, første år.

12.4.6.2 Virksomheder og myndigheder som arbejdsgivere

Der forventes ikke øgede udgifter for virksomheder og myndigheder i forhold til den nuværende løsning, idet løsningen svarer til den nuværende.

12.4.6.3 Private tjenesteudbydere

Private tjenesteudbydere vil få mindre udgifter til skift til en kommende løsning, svarende til de løbende udgifter til udskiftning af certifikater og tilpasning af snitflader.

12.4.6.4 Offentlige tjenesteudbydere

Offentlige tjenesteudbydere forventes ikke at få udgifter til denne løsning, idet NemLog-in vil sørge for eventuelt ændrede snitflader.

12.4.7 Finansieringsmodeller

Finansieringsmodeller vedrører både den fællesoffentlige del og de dele, der finansieres i samarbejde med private partnere.

12.4.7.1 Borgere

Da NemID de facto er obligatorisk, vil det opfattes som naturligt, at det fortsat er gratis for brugerne. Mange af gevinsterne ved NemID ligger hos det offentlige og bankerne, hvilket taler for, at det er gratis for borgerne. Erfaringerne fra udlandet, hvor det fx koster penge at anskaffe SmartCard-læsere, viser, at selv små beløb hæmmer anvendelsen kraftigt.

Af samme årsag skal også support af NemID være gratis for borgerne. Ulempen er de udgifter, der i så fald skal finansieres fællesoffentligt.

12.4.7.2 Virksomheder

I dag er de første tre NemID medarbejdersignaturer gratis for brugerne. Virksomheder, der har brug for flere medarbejdersignaturer, skal betale herfor.

Der kan vælges mellem en model som den nuværende eller en model, hvor det offentlige frikøber NemID medarbejdersignatur for virksomheder og myndigheder.

For en fortsættelse af den nuværende betalingsmodel taler, at virksomheder har meget forskelligartede behov, og det er derfor rimeligt, at virksomhederne betaler for de valg, de træffer.

For en model, hvor det offentlige frikøber NemID medarbejdersignatur taler, at NemID de facto er obligatorisk, og mange af gevinsterne ved NemID ligger hos det offentlige og bankerne. Ulempen er de udgifter, det pålægger det offentlige.

Samme overvejelser gælder for betaling eller helt eller delvist frikøb af support.

12.4.7.3 Myndigheder

Der er samme betalingsregler for myndigheder i forhold til anskaffelse af NemID medarbejdersignaturer og support som for private virksomheder.

12.4.7.4 Private tjenesteudbydere

Den nuværende leverandør opkræver betaling hos private tjenesteudbydere, som kan vælge betaling pr. session (1,01 kroner) eller betaling pr. unik bruger pr. år (3,14 kroner).

NemID blev i 2014 anvendt til 88 millioner transaktioner hos private tjenesteudbydere. Med en pris pr. session på 1,01 kroner betyder det en indtjening på 89 millioner kroner til Nets. Sandsynligvis betyder pris pr. unik bruger, som vælges af tjenesteudbydere med mange transaktioner, at tallet er noget lavere.

Et frikøb af private tjenesteudbyderes anvendelse af NemID vil skønsmæssigt koste 20-60 millioner kroner årligt. Det vil derfor kraftigt påvirke det offentliges udgifter, samtidig med at private tjenesteudbyderes transaktioner vil være udgiftsdrivende (nøglekort estimeres at koste 40 øre pr. transaktion[8]).

12.4.7.5 Offentlige tjenesteudbydere

Løsningen er frikøbt for offentlige myndigheder. De skal derfor ikke betale for, at brugerne anvender NemID på deres tjenester.

12.4.8 Leverandørstrategi

Der kan vælges samme leverandørstrategi som nu, dvs. at der er én leverandør til den samlede løsning.

Der kan også vælges opdeling af løsningen, så den centrale lagring af privatnøgler hos leverandøren og 2-faktor-login med kodeord og engangskode (fx nøglekort) til NemID privat og NemID med-

[8] Den nuværende leverandørs pris for et nøglekort er 76 kroner (http://www.nets.eu/dk-da/Produkter/Sikkerhed/medarbejdersignatur/Pages/Priser-uden-Pro-pakken.aspx). Der er 148 nøgler på nøglekortet, hvilket giver en pris på 51 øre pr. nøgle. Anslås leverandørens avance til 20 %, svarer det til 40 øre pr. nøglekort.

arbejdersignatur leveres af én leverandør og nøglefiler af en anden. Der er tale om to forskellige sæt af teknologier, så en opdeling er teknisk mulig. Den vil dog have ulemper i forhold til anvendervirksomheder, som ændrer teknologivalg eller ønsker begge løsninger, idet de så skal interagere med flere leverandører, der ikke nødvendigvis kan håndteres af brokeren.

En opdeling på separate leverandører for borgere og erhverv kan betyde forskellige løsninger i brugergrænsefladen – medmindre der stilles krav om samme brugergrænseflade og samme udseende af nøglekort. Forskelle i brugergrænsefladen vil være til ulempe for de brugere, der nu har fordel ved at anvende samme nøglekortsløsning til både privat- og erhvervsformål.

12.4.9 Risici

En væsentlig risiko ved en løsning som nu er, at der ikke opnås tilbud fra det ønskede antal leverandører, idet mulige leverandører vil se et udbud af en løsning svarende til den nuværende som en favorisering af den nuværende leverandør.

Desuden betyder den nuværende forholdsvist 'lukkede' arkitektur, at de langsigtede udviklingsmuligheder svækkes.

12.4.10 Juridiske problemstillinger

Der vurderes ikke at være særlige juridiske problemstillinger i dette scenarie.

12.4.11 Styringsmæssige problemstillinger

Der vurderes ikke at være særlige styringsmæssige problemstillinger i dette scenarie.

12.5 Samlet konklusion for Scenarie 1

Herunder opsummeres først vurderingen ovenfor, hvor den kommende løsning vurderes i forhold til den nuværende løsning.

Da den nuværende løsning og løsningen i Scenarie 1 er meget overensstemmende, er der på mange punkter ingen ændring i forhold til den nuværende løsning.

Tabel 9: Oversigt over vurdering af Scenarie 1

Vurderingsparametre	RMC-ICG's vurdering
Arkitektur	Ingen ændring i forhold til den nuværende løsning.
Sikkerhed og privacy	Ingen ændring i forhold til den nuværende løsning.
Migrering	Vurdering af migrering afhænger af, om den nuværende leverandør eller en anden får kontrakten. Hvis den nuværende leverandør får kontrakten, vil migrering give begrænsede udfordringer. Ved skift til ny leverandør vil det kræve en målrettet indsats.
Relation i forhold til private partnere	Ingen ændring i forhold til den nuværende løsning.
OCES-certifikatpolitikker	Ingen ændring i forhold til den nuværende løsning.
Økonomi	Udgifter vil afhænge af leverandørernes bud, herunder hvordan den nuværende leverandør vil byde ind.
Finansieringsmodeller	Ingen ændring i forhold til den nuværende løsning.
Leverandørstrategi	Udbud af en løsning svarende til den nuværende vil give risiko for, at kun få andre vil byde.
Risici	Få tilbudsgivere. Risiko for, at de langsigtede udviklingsmuligheder er begrænsede, og at brugerne derved bliver mindre tilfredse med løsningen over tid.
Juridiske problemstillinger	Ingen ændring i forhold til den nuværende løsning.
Styringsmæssige problemstillinger	Ingen ændring i forhold til den nuværende løsning.

12.5.1 Gevinster

RMC-ICG har desuden vurderet gevinsterne ved scenariet ud fra de overordnede gevinster, beskrevet i afsnit 4, der ønskes opnået i den nye NemID-løsning.

Tabel 10: Oversigt over RMC-ICG's gevinstvurdering for Scenarie 1

Gevinst	RMC-ICG's vurdering
Høj tillid til løsningen.	Ingen ændring.
Lettere anvendelse for borgere.	Ingen ændring.
Lettere anvendelse for virksomheder.	Ingen ændring.
Lettere administration for virksomheder og myndigheder.	Minimale forbedringer inden for rammerne af den nuværende løsning og dens økonomi.
Flere offentlige tjenester anvender det nye NemID.	Ingen påvirkning.
Flere private tjenester anvender det nye NemID	Ingen påvirkning.
Mere fleksible udviklingsmuligheder.	Ingen ændring.

Et scenarie med fortsættelse af den nuværende løsning med kun få ændringer vil betyde en høj grad af kontinuitet og bagudkompatibilitet. Til gengæld er der stor risiko for, at scenariet ikke vil imødekomme ønsker om fremtidssikring af teknologien.

Scenariet vil ikke imødekomme de mange krav og behov for forbedringer, der er indkommet i høringsfasen og i Digitaliseringsstyrelsens arbejde med NemID.

12.5.2 Leverandørforhold

Der er en risiko for, at leverandørerne i markedet vil opfatte et udbud af 'samme løsning' som et signal om, at den nuværende leverandør foretrækkes, hvilket kan medføre, at færre vil byde. Det er ikke muligt at vurdere, hvordan det vil påvirke prisen i et eventuelt tilbud fra den nuværende leverandør.

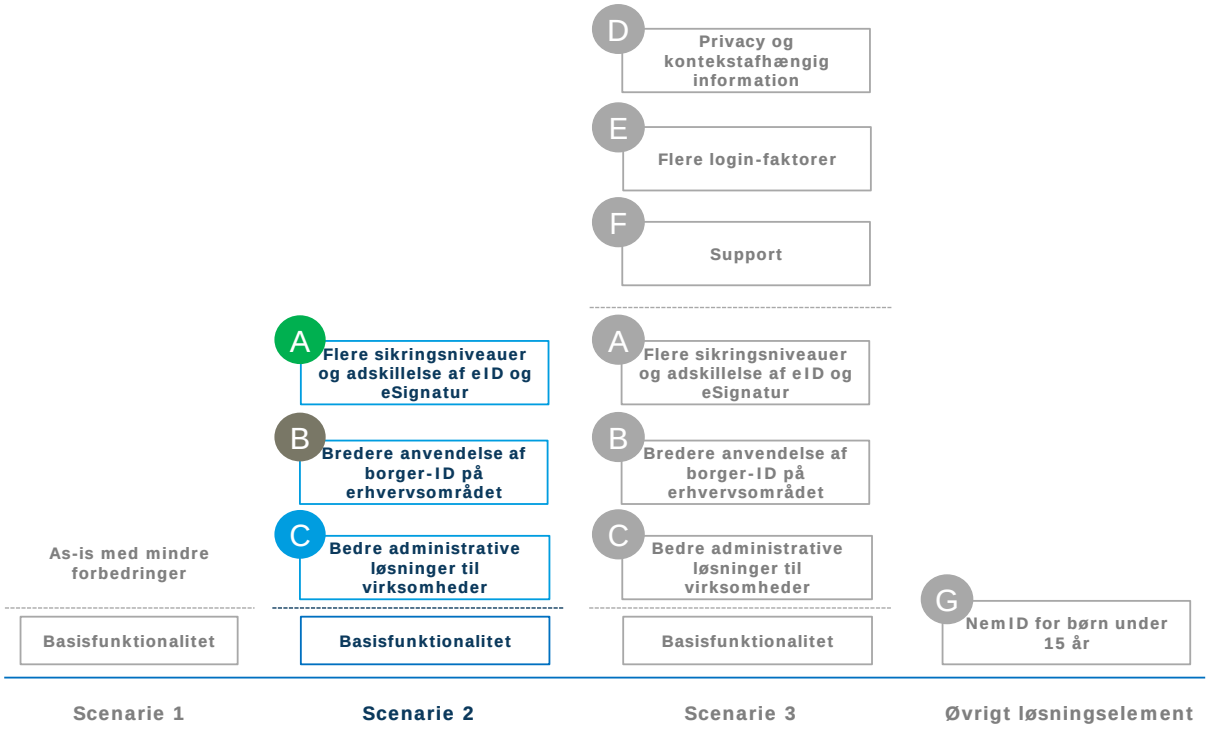
13. Scenarie 2

I dette kapitel præsenteres og vurderes Scenarie 2. Kapitlet angiver først en kort overordnet introduktion til scenariet, hvorefter de enkelte løsningselementer vil blive analyseret og vurderet mere dybdegående. Kapitlet afsluttes med en opsamlende konklusion.

13.1 Præsentation af scenariet

Scenarie 2 skal dække de samme funktionelle behov som Scenarie 1 suppleret med mulighed for 1-faktor-login. I sammenhæng hermed adskilles autentifikation og signering. Dermed er der ikke krav om, at løsningen baseres på PKI for eID-delen. Scenarie 2 indeholder tre løsningselementer, der alle bidrager med nye funktionaliteter.

Figur 16: Løsningselementer i Scenarie 2



Scenariet indeholder følgende:

- Både 1-f
- aktor-login og 2-faktor-login, sidstnævnte med kodeord og engangskode (fx nøglekort) til NemID privat og NemID medarbejdersignatur.
- En central lagring af privatnøgler hos leverandøren til signeringsdelen. Det er et krav, at brugeren oplever sammenhæng mellem login-løsning og signeringsløsning.
- Nøglefil til NemID til erhverv (herunder mulighed for decentralt at anvende signaturserverløsninger).

Løsningens arkitektur adskiller sig fra den nuværende løsning og Scenarie 1. Det er beskrevet i Løsningselement A: *Flere sikringsniveauer og adskillelse af autentifikation og signering*. Arkitekturen bygger på anvendelse af eID-teknologier til autentifikation og på en PKI-baseret arkitektur til signering. Såkaldte eID-teknologier (*identity management*-systemer) giver større fleksibilitet i for-

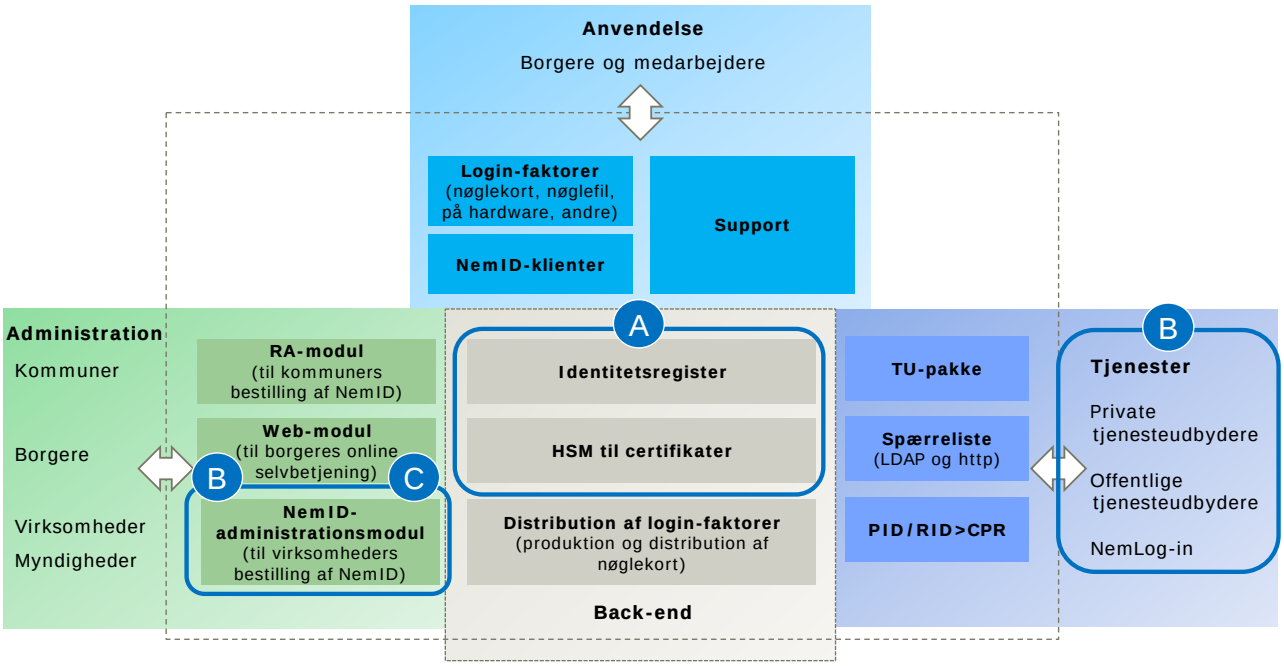
hold til brugergrænseflader og tilpasning til forskelligt brugerudstyr. Desuden forventes de i kraft af større markedsudbredelse at være billigere i anskaffelse og drift.

Desuden indeholder Scenarie 2 elementer på virksomhedsområdet i form af udbredelse af NemID privat til erhvervsformål og bedre administrative løsninger til virksomheder.

I det følgende præsenteres og vurderes de tre løsningselementer, og kapitlet afsluttes med en samlet konklusion og vurdering af Scenarie 2.

13.2 Funktioner i Scenarie 2

Figur 17: Funktioner i Scenarie 2



Scenarie 2 indeholder basisfunktionalitet, jf. afsnit 11.4, samt følgende funktionaliteter:

Løsningselement A: Flere sikringsniveauer og adskillelse af autentifikation samt signering vedrører NemID back-end.

Løsningselement B: Bredere mulighed for anvendelse af borger-ID på erhvervsområdet vedrører primært brokere/login-tjenester og tjenesteudbydere.

Løsningselement C: Bedre administrative løsninger til virksomheder vedrører primært NemID-administratormodulet.

Løsningselementerne B og C har ikke teknisk og funktionel sammenhæng med løsningselement A, og de kan implementeres i forbindelse med Scenarie 1.

De to løsningselementer B og C retter sig begge mod virksomheder og myndigheder, men er funktionelt og teknisk så forskellige, at de kan implementeres hver for sig.

13.3 Løsningselement A: Flere sikringsniveauer og adskillelse af autentifikation og signering

I dette afsnit præsenteres løsningselementet *flere sikringsniveauer og adskillelse af autentifikation og signering*. Herefter analyseres de overordnede potentielle forretningsmæssige gevinster som RMC-ICG vurderer, at løsningselementet kan give. Dernæst foretages en vurdering af løsningselementet, og afsnittet afsluttes med en konklusion, der opsummerer gevinsterne og RMC-ICG's vurderinger af løsningselementet.

13.3.1 Præsentation af løsningselementet

I dette løsningselement indgår forskellige dele, som dækker behovet for differentierede sikkerhedskrav i forhold til adgang til tjenester.

Det grundlæggende i elementet er at dække yderligere forretningsmæssige behov for borgere, virksomheder, offentlige myndigheder og tjenesteudbydere for lettere adgang til tjenester med lavere sikkerhedskrav.

For at give lettere adgang til tjenester med lavere sikkerhedskrav skal NemID udvides med 1-faktor-login med den tekniske benævnelse "flere sikringsniveauer".

RMC-ICG har som forudsætning for dette scenarie valgt at beskrive en løsning, hvor login- og signeringsfunktionalitet adskilles på teknisk niveau, så autentifikation ikke benytter den private nøgle, som anvendes til signering. Dette kan implementeres, uden at brugeren oplever ændringer i brugergrænsefladen i forhold til 2-faktor-login og signering.

I den nuværende løsning anvender brugeren ét certifikat og tilhørende privat nøgle til både autentifikation og signering og er dermed bundet til konsekvent at anvende to login-faktorer (eller tilsvarende sikkerhed).

Implementering af 1-faktor-login vil derfor kræve en adskillelse af autentifikation og signering i den næste generation NemID.

I løsningselementet beskrives flere sikringsniveauer med fokus på 1-faktor-login, men løsningsarkitekturen skal fastlægges, så det også er muligt at udvide med en tredje login-faktor, hvis ændring i trusselbilledet kræver dette.

Nøglekortsdelen (borgere og mindre virksomheder)

Nøglekortdelen vil omfatte både login- og signeringsfunktionalitet uden synlig forskel for brugeren. De to vil blive adskilt rent teknisk, så der fortsat er et OCES-certifikat med tilhørende privat nøgle til signering, mens autentifikation kan løses med andre mekanismer.

Nøglefilsdelen (større virksomheder og myndigheder)

Baseres på signeringscertifikatet, der er identisk med det nuværende.

13.3.1.1 Sammenhæng mellem 1-faktor-autentifikation og opdeling af autentifikation og signering

Den nuværende løsning anvender en samlet PKI-baseret back-end-infrastruktur både til signering og login, hvor der ikke sondres mellem de to funktioner. Samme private nøgle og tilhørende certifikat anvendes således ved både signering og login. Derfor kræves altid to faktorer ved anvendelse af den private nøgle for at opretholde den samlede sikkerhed, som er krævet i OCES-certifikatpolitikken.

Bankernes kontokig er baseret på autentifikation med 1-faktor (adgangskode) og bygger ikke på OCES back-end.

En 1-faktor-login-løsning vil kræve ændring af OCES-certifikatpolitikker, så der også er adgang til certifikatet med 1-faktor. Dette vil være problematisk, da tjenesteudbyderne så skal skelne mellem forskelligt indhold i XMLDSig.

Alternativt kan der dannes en afledt identitet hos identitetsgaranten.

Konsekvenserne vil være forskellige for tjenesteudbyderne i forhold til:

- Anvendere af TU-pakken kan forvente at få en ny TU-pakke, der løser en del af opgaven.
- Anvendere af private login-tjenester får nyt indhold i de billetter, som login-tjenesten sender.
- Anvendere af NemLog-in får nyt indhold i SAML-billetten.

Alle tjenesteudbydere skal selv håndtere at skille sine data, så der kan gives differentieret adgang, samt tilrette sin adgangskontrol, så dette kan styres.

13.3.1.2 Signering

Såfremt dette scenarie vælges, kan signeringen (af fx dokumenter) implementeres med langtids-certifikater som nu eller korttids-certifikater, som bankerne anvender.

Korttidscertifikater bliver typisk genereret og anvendt i software og vil dermed (uanset det reelle sikkerhedsniveau) ikke kunne bliver ratet som kvalificeret elektronisk signatur i forhold til eksisterende elektronisk signaturdirektiv eller eIDAS-forordning (se bilag II til forordningen: "Krav til kvalificerede elektroniske signaturgenereringssystemer").

Brug af korttidscertifikater kan eventuelt give udfordringer i forhold til standardiserede løsninger, hvori der forventes længere tids gyldighed, eller i asynkrone processer. Tjenesteudbyderes løsninger bør dog kunne håndtere korttidscertifikater, da udløb og risiko for spærring under alle omstændigheder også bør håndteres for traditionelle certifikater med lang gyldighed. Inden der vælges en løsning med korttidscertifikater, bør der gennemføres en mere gennemgribende analyse af de faktiske konsekvenser hos tjenesteudbydere i forhold til gængse standarder, anvendelse i international sammenhæng og generelt.

En løsningsmodel, hvor leverandøren signerer på vegne af slutbruger, undersøges ikke nærmere, da eksisterende systemer og lovgivning baserer sig på, at slutbrugeren tilføjer egen elektronisk signatur. Det gælder blandt andet tinglysningsloven og det tilhørende tinglysningssystem samt retsplejelov (tvangsfuldbyrdelse) og de tilknyttede kommercielle løsninger for elektroniske lånedokumenter.

13.3.1.3 Brugervenlighed

For mange brugere vil adskillelse af autentifikation og signering ikke betyde ændringer i brugervenligheden, da brugerne i *mange* tilfælde anvender NemID som adgang til systemer med højt sikkerhedsniveau og dermed altid vil benytte to faktorer.

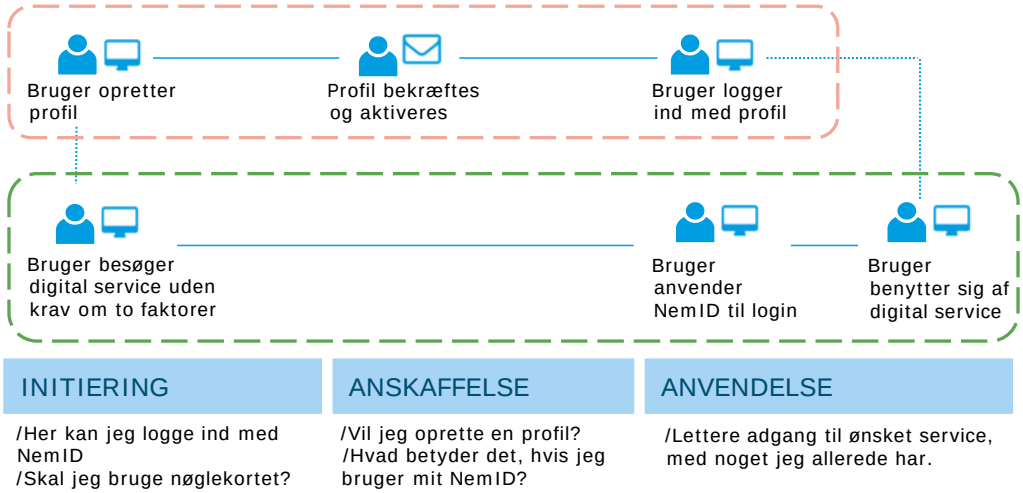
Kravet om samme brugeroplevelse ved autentifikation og signering i en fremtidig løsning skal samtidigt tydeligt fremgå af den kommende kravspecifikation.

For brugere med NemID privat vil 1-faktor-login betyde flere muligheder for at anvende NemID som adgang til digitale tjenester. I Fase 1 udtrykte denne brugergruppe et ønske om at kunne anvende NemID uden samtidig at skulle bruge eksempelvis nøglekort. Begrundelsen for dette ligger i, at anvendelsen i denne målgruppe har nået en højudbredelse, og NemID er dermed noget, de allerede har og ønsker at kunne anvende i flere sammenhænge end i dag.

NemID med 1-faktor-login vil samtidig betyde, at brugen af NemID udbredes til flere digitale tjenester. Indsigter fra Fase 1 peger på, at slutbrugerne gerne ser, at NemID fungerer som en generel adgangsgivende løsning, der gør det nemmere at agere på internettet.

Nedenstående brugerrejse i Figur 18 illustrerer brugerens forskellige berøringspunkter og overvejelser ved anvendelse af NemID med 1-faktor-login. Den repræsenterer dermed blot én ud af adskillige brugerrejser i løsningselementet. Den grønne ramme indikerer den fremtidige løsning, og den røde ramme er trin i brugerrejsen, der vil udgå.

Figur 18: Brugerrejse for oprettelse af login med NemID til flere tjenester



Fordele

Brugerne vil få mulighed for at nøjes med én faktor i nye sammenhænge.

Udfordringer

Et tilbagevendende emne igennem brugeranalysen var brugernes opfattelse af sikkerhed. Det er meget vigtigt for brugere i alle tre målgrupper (borgere, virksomheder og myndigheder), at de oplever de digitale tjenester, hvortil de anvender NemID, som sikre. I den sammenhæng blev faren ved phishing-angreb ligeledes udtrykt. Frygten for identitetstyveri er til stede, især hos borgere.

En anden udfordring er, at dette løsningselement vil påvirke brugernes forståelse af NemID-anvendelsen. Nogle brugere udtrykte i Fase 1 en konservativ holdning til NemID som en løsning, der har sin plads som adgang til offentlige løsninger.

På den måde rummer adskillelsen af autentifikation og signering et paradoks, da slutbrugene på samme tid både ønsker at anvende NemID som adgang til flere digitale tjenester og omvendt også har en naturlig skepsis over for udbredelse og de sikkerhedsrisici, som 1-faktor-login indebærer. Hvis en fremtidig løsning indeholder mange sikkerhedsniveauer, kan dette også skabe uoverskuelighed for brugeren. Desuden er der en risiko for, at tjenesteudbyderne ikke ønsker at anvende de forskellige sikkerhedsniveauer. I så fald vil de potentielle gevinster på dette område ikke blive indfriet.

13.3.2 Gevinster

Dette afsnit har til formål at præsentere de gevinster, løsningselementet kan give. Gevinsterne differentieres i forhold til de forskellige relevante brugergrupper, som NemID opererer inden for.

13.3.2.1 Borgere

Borgerne vil få mulighed for 1-faktor-login.

For de borgere, der er tilfredse med den nuværende løsning, og for borgere, der lægger vægt på kontinuitet, vil scenariet være tilfredsstillende. For alle de borgere, der har efterlyst lettere adgang til tjenester, vil 1-faktor-login blive opfattet som en stor gevinst.

Det er en forudsætning, at brugerne ikke oplever, at eID-delen og signeringsdelen er forskellige. Borgerne vil således ikke opleve, at der eventuelt er tekniske forskelle i løsningerne.

13.3.2.2 Virksomheder, herunder private virksomheders medarbejdere

For virksomheder, hvis medarbejdere anvender nøglekort, vil løsningen opfylde samme behov som for borgere.

For virksomheder, der anvender nøglefil, vil løsningen opfylde samme behov som nu.

13.3.2.3 Myndigheder, herunder myndighedernes medarbejdere

For myndigheder, hvis medarbejdere anvender nøglekort, vil løsningen opfylde samme behov som for borgere.

For myndigheder, der anvender nøglefil, vil løsningen opfylde samme behov som nu.

13.3.2.4 Private tjenesteudbydere

For private tjenesteudbydere vil scenariet betyde flere gevinstmuligheder.

Det forudsættes, at løsningen implementeres med høj grad af bagudkompatibilitet for de tjenesteudbydere, som ikke ønsker nye funktioner. Såfremt det er muligt, vil denne gruppe af tjenesteudbydere ikke opleve forskelle.

For de tjenesteudbydere, der ønsker mulighed for 1-faktor-login, skal der ske ændringer i snitfladerne til NemID, og tjenesterne skal indrettes, så de kan tage højde for adgang til data med forskellige sikkerhedskrav.

Det er forventningen, at TU-pakken vil kunne løse de fleste ændringer i snitfladerne, men ikke alle.

13.3.2.5 Offentlige tjenesteudbydere

Offentlige tjenesteudbydere vil fortsat anvende NemLog-in.

Med 1-faktor-login vil muligheden i den nuværende SAML 2.0-standard for flere sikringsniveauer blive udnyttet. De offentlige tjenesteudbydere skal således ikke lave tekniske ændringer i snitfladerne, men ændre de tjenester, hvor der er behov for at implementere 1-faktor-login. I denne forbindelse skal tjenesteudbydere vurdere data i forhold til, hvilket sikkerhedsniveau de kan udstilles på.

13.3.3 Vurdering

Dette afsnit har til formål at analysere og vurdere løsningselementet i forhold til relevante parametre.

13.3.3.1 Arkitektur

Ved teknisk adskillelse af autentifikation og signering skal identitetsudbyderen implementere og tilbyde et eller flere specifikke login-interfaces til tjenesteudbyderne. SAML 2.0 og/eller OpenID Connect vil være gode kandidater til disse interfaces for autentifikation på grund af åbenhed og markedsaccept.

Tjenesteudbyders pakke (TU-pakken) skal tilpasses til at understøtte de nye interfaces. Af hensyn til bagudkompatibilitet kan det besluttes, at der fortsat skal være en TU-pakke med den eksisterende tekniske grænseflade, der dog så ikke vil tilbyde den nye funktionalitet.

13.3.3.2 Sikkerhed og privacy

I takt med at flere tjenesteudbydere vil give adgang til tjenester ved brug af NemID med lavere sikkerhedsniveau, må det antages, at man i øget omfang vil forsøge at skaffe sig adgang til brugerens akkreditiver til det lavere niveau.

Den eksisterende løsning bliver i vid udstrækning anvendt af tjenesteudbydere, der behandler almindelige og følsomme personoplysninger. Det kan antages, at en fremtidig løsning med understøttelse af differentierede sikringsniveauer vil betyde udbredelse til tjenesteudbydere med mindre fokus på sikkerhed i web-applikationen. Dermed øges risikoen for, at en ondsindet angriber kan tiltvinge sig adgang til en hjemmeside hos en tjenesteudbyder og erstatte NemID-klienten med en alternativ klient under angriberens kontrol.

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

13.3.3.3 Migrering

Den tekniske adskillelse af autentifikation og signering bør ikke umiddelbar få indflydelse på brugerens oplevelse eller krav til brugerens udstyr. Brugeren vil blot opleve mulighed for 1-faktor-funktionalitet i takt med, at tjenester implementerer dette.

Offentlige tjenesteudbydere anvender NemLog-in som login-tjeneste i forbindelse med autentifikation af brugere i den eksisterende løsning. Ved signering kan den offentlige tjenesteudbyder vælge at implementere signeringsfunktionalitet direkte i egen løsning eller anvende NemLog-in Signering. Løsningen bør implementeres, så offentlige tjenesteudbydere ikke vil opleve ændret funktionalitet eller kompleksitet, medmindre de ønsker at gøre brug af ny funktionalitet i form af understøttelse af lavere sikringsniveau. NemLog-in skal implementere understøttelse for et nyt interface og åbne for understøttelse af flere sikringsniveauer mod de offentlige tjenesteudbydere.

I den nuværende løsning kan private tjenesteudbydere vælge at integrere NemID-klienten direkte i egen applikation eller benytte en af flere kommercielle login-tjenester på markedet. Private tjenesteudbydere, der anvender login-tjenester, vil have samme få tilpasningskrav som offentlige tjenesteudbydere, hvor login-tjenesten skjuler kompleksiteten. Private tjenesteudbydere med egen implementering vil skulle lave tilpasninger, hvis der ikke tilbydes et interface svarende til det eksisterende. TU-pakken bør udvides med henblik på at gøre tilpasningen så simpel som mulig.

13.3.3.4 Relation i forhold til private partnere

Løsningen vil give bedre muligheder for at indgå samarbejde med private partnere i forhold til den nuværende situation, idet det forventes, at de fremtidige partnere vil foretrække samme løsning som i dag, dog med både 1-faktor-login og 2-faktor-login samt adskillelse af autentifikation og signering.

13.3.3.5 OCES-certifikatpolitikker

En væsentlig del af den eksisterende løsning er funderet på en X.509 PKI med tilhørende certifikatpolitik. Ved en teknisk adskillelse af autentifikation og signering bør der være en række krav til håndtering af eID, der ikke umiddelbart er relatereret til en Public Key-infrastruktur og derfor ikke naturligt bør beskrives i en certifikat-politik. RMC-ICG anbefaler, at der fortsat skal være sammenhængende nationale standarder, der fastlægger certifikatpolitikker og sikringsniveauer for eID i Danmark, og som er koordineret med de kommende definitioner for sikringsniveauer fra eIDAS-forordningen.

13.3.3.6 Økonomi

Fællesoffentlige udgifter

De fællesoffentlige udgifter vil afhænge meget af, hvilke løsninger de kommende leverandører byder ind med, og i hvilken udstrækning de kan tilbyde standardløsninger.

Da løsninger alene med eID til login er mere udbredte i markedet end PKI-baserede løsninger, vil det som udgangspunkt betyde en lavere udgift at udbyde en løsning uden den nuværende stærke binding til signaturen, idet signering kun bruges i 1 % af NemID-OCES-transaktionerne.

På den anden side vil der være udgifter dels til signeringsløsningen og sammenhængen mellem autentifikation og signering, dels til bagudkompatibilitet. Det er i estimatet af den fremtidige løsning indregnet, at de nuværende snitflader til tjenester kan fortsætte uden ændringer. Den tekniske baggrund herfor er, at signering kræver fortsættelse af den nuværende snitflade (XMLDSig).

Samlet set vurderes det derfor, at en adskillelse af autentifikation og signering og i sammenhæng hermed mulighed for både 1-faktor-login og 2-faktor-login vil kunne anskaffes til samme pris som kerneløsningen.

Der regnes derfor ikke med højere fællesoffentlige udgifter i dette element.

Virksomheder og myndigheder

Der forventes ikke øgede udgifter for virksomhederne og myndighederne.

Private tjenesteudbydere

Private tjenesteudbydere, der ikke ønsker at implementere 1-faktor-login, vil ikke få øgede udgifter.

Private tjenesteudbydere, der ønsker at implementere 1-faktor-login, vil få øgede udgifter til at sikkerhedskategorisere data og funktioner. Da den enkelte tjenesteudbyder kun forventes at implementere, hvis det er muligt at få en god business case, fx i form af flere brugere eller større brugertilfredshed, indgår disse udgifter ikke i skønnene over omkostninger.

Offentlige tjenesteudbydere

Der gælder samme forhold som for private tjenesteudbydere.

13.3.3.7 Finansieringsmodeller

Der vil være behov for at afklare, hvilke betalingsbetingelser private tjenester vil få i forhold til 1-faktor-login. Prisen herfor skal være betydeligt lavere end den nuværende listepris på 1,01 kroner pr. transaktion for NemID for at kunne konkurrere med en kodeordsløsning, som tjenesteudbydere selv etablerer.

13.3.3.8 Leverandørstrategi

Dette element skal leveres som del af den samlede løsning.

13.3.3.9 Risici

Da løsningen indebærer et skift i arkitektur i forhold til den nuværende løsning, vil der være øgede risici for manglende tilgængelighed i forbindelse med migreringen.

Hvis den nye løsning er baseret på en standardløsning, vil der være risici i forbindelse med tilpasningen af standardløsningen til behovene i forhold til NemID. Hvis løsningen skal nyudvikles, er der risici for forsinkelser i forbindelse med udviklingsprocessen.

13.3.3.10 Juridiske problemstillinger

Den gældende lovgivning forhindrer ikke en opdeling i løsninger til autentifikation og signering[9]. Det er dog væsentligt at være opmærksom på, at en række love/bekendtgørelser forudsætter tilstedeværelse af en digital signatur med henblik på gennemførelse af en digital transaktion. Eksempler på et sådant krav følger af tinglysningsloven og af bekendtgørelse om online-væddemål.

Der skal desuden tages stilling til, hvordan forskellige lovgivningsmæssige krav om brug af digital signatur/OCES, fx et sikkerhedsniveau svarende til OCES-standarden eller højere, påvirkes.

Konsekvenserne ved en eventuel opdeling bør derfor analyseres nærmere.

Der kan være behov for at inddrage Datatilsynet i forhold til, hvilke personoplysninger der bør kunne tilgås med henholdsvis en og to faktorer.

13.3.3.11 Styringsmæssige problemstillinger

Der vurderes ikke at være styringsmæssige problemstillinger.

13.3.4 Samlet vurdering for løsningselementet

Der er som beskrevet en række gevinster ved at indføre en opdeling af autentifikation og signering og i sammenhæng med dette muliggøre 1-faktor-login, primært i forhold til større brugertilfredshed og bedre understøttelse af brugerne set fra tjenesteudbydernes side.

Løsningen skønnes som nævnt ikke at medføre ekstra fællesoffentlige udgifter.

[9] Den i 2014 vedtagne forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner mv. indeholder en vis regulering af såkaldte "Ikke-kvalificerede" tillidstjenester, der vil omfatte NemID. Denne regulering har dog ingen betydning for en eventuel opdeling i løsninger til autentifikation og signering.

Tabel 11: Opsummering af RMC-ICG's vurdering af løsningselement A: *Flere sikringsniveauer og adskillelse af autentifikation og signering*

Vurderingsparametre	RMC-ICG's vurdering
Arkitektur	Mere åben arkitektur åbner for flere snitflader mod tjenester.
Sikkerhed og privacy	Flere sikringsniveauer kræver, at tjenesteudbydere klassificerer data.
Migrering	TU-pakke og NemLog-in kan gøre, at tjenester ikke skal gennemføre større ændringer i migreringen.
Relation i forhold til private partnere	Vil give bedre mulighed for teknisk samarbejde med partnere.
OCES-certifikatpolitikker	RMC-ICG anbefaler, at der laves nationale standarder/politikker for både autentifikation og signering.
Økonomi	Løsningselementet forventes ikke at være fordyrende i forhold til Scenarie 1.
Finansieringsmodeller	Prisen for 1-faktor-login til private skal afklares.
Leverandørstrategi	Elementet skal leveres som del af hovedleverancen.
Risici	Risiko for manglende tilgængelighed i forhold til migrering samt risici i forbindelse med implementering af ny løsning.
Juridiske problemstillinger	Ikke specifik lovgivning, der forhindrer en opdeling i løsninger til autentifikation og signering.
Styringsmæssige problemstillinger	Ingen.

13.4 Løsningselement B: Bredere mulighed for anvendelse af borger-ID på erhvervsområdet

I dette afsnit præsenteres løsningselementet: *Bredere mulighed for anvendelse af borger-ID på erhvervsområdet*. Herefter analyseres de overordnede potentielle forretningsmæssige gevinster, som RMC-ICG vurderer, at løsningselementet kan give. Dernæst foretages en vurdering af løsningselementet, og afsnittet afsluttes med en konklusion, der opsummerer gevinsterne og RMC-ICG's vurderinger af løsningselementet.

Muligheden for, at virksomheder kan anvende NemID privat med en CVR-tilknytning, analyseres nærmere af Digitaliseringsstyrelsen og Erhvervsstyrelsen i andet regi. Konklusioner fra dette analysearbejde kan spille ind i det videre arbejde med genudbud af NemID i en senere fase.

13.4.1 Om muligheden for udelukkende at anvende NemID privat til erhverv

Det er i dag muligt at anvende NemID privat i erhvervssammenhæng i nogle sammenhænge, men det er silopræget og ukoordineret. Det er fx muligt at anvende NemID privat for personligt ejede virksomheder til SKAT, ATP og Fødevareministeriets Tast-selv service, mens det ikke er muligt til Digital Post. Dette afspejler, at myndighederne på forskellig vis forsøger at imødekomme virksomhedernes meget forskellige behov i forbindelse med anvendelse af NemID, bl.a. afhængigt af virksomhedernes størrelse, virksomhedsformen, forretningsområdet m.m.

For disse og andre virksomheder kan det være en fordel, hvis de i større omfang kan anvende NemID privat med en CVR-tilknytning. I andre virksomheder understøtter NemID komplekse organisationer og en specialiseret anvendelse af NemID. Fx har regionerne i deres analyse analyseret anvendelsen af NemID. I regionerne anvendes cirka 80.000 NemID medarbejdersignaturer i form af nøglefiler, og der er investeret i en række løsninger (fx signaturservere), der understøtter dette.

Regionerne ønsker derfor fortsat at kunne bruge NemID med nøglefil. Noget tilsvarende forventes at gælde for kommunerne og evt. store private virksomheder.

Som det fremgår af tabellen herunder, er der i alt udstedt knap 700.000 NemID med nøglefil (både nøglefil, VOCES og FOCES).

Tabel 12: Udstedte identiteter til nøglefil

	Antal identiteter (Afrundet til hele 1.000)
MOCES nøglekort	377.000
MOCES nøglefil	663.000
Heraf regioner og kommuner (skøn)	160.000
MOCES andre	11.000
VOCES	25.000
FOCES	11.000

*Note til tabel: Tal for regionerne er oplyst af disse. Tal for kommunerne er skønnet ud fra tal fra Favrskov og Odense Kommuner.

Der er ligeledes en omfattende anvendelse af nøglefiler.

Tabel 13: Antal transaktioner med forskellige typer NemID

	Antal i millioner
Nøglefilstransaktioner SOSI STS (sundhedsområdet)	12
Nøglefils-transaktioner (inkl. digital signatur) NemLog-in	10
Nøglefils-transaktioner (kommuner)	2
Nøglekorts-transaktioner POCES	132
Heraf NemLog-in (offentlige)	42

*Note til tabel: Der er tal for de seneste 12 måneder pr. oktober 2014. Der er, af tekniske grunde, ikke samlede tal for nøglefils-transaktioner. De faktiske tal er derfor større. Tal for kommuner er skønnet for alle kommuner på grundlag af statistik fra Odense Kommune i 14 dage. Nogle af de kommunale transaktioner kan også indgå i tallet for SOSI STS.

Datatilsynet har behandlet medarbejderes anvendelse af NemID privat i kommunal sammenhæng og har fremført, at persondatasikkerheden ikke er tilfredsstillende, hvis medarbejdere tilgår kommunale data alene med deres personlige NemID.

En løsning, der indebærer afskaffelse af NemID medarbejdersignatur, herunder nøglefilsløsninger, skal derfor tage hensyn til regionernes og andre virksomheders investeringer i den eksisterende løsning samt de bindinger, dette medfører. Dette vurderes som en meget kompleks opgave.

En løsning, hvor borgeren skal anvende sit NemID i erhvervssammenhæng kan desuden betyde, at virksomheder ikke kan vælge de tekniske og sikkerhedsmæssige løsninger, der passer til virksomhedens/myndighedens behov, men derimod må følge brugerens valg. Desuden vil virksomheden kunne blive påvirket af medarbejderens personlige forhold, fx undladelse af fornyelse.

13.4.2 Præsentation af løsningselementet

I dette afsnit analyseres en udvidelse og optimering af de nuværende muligheder for at anvende NemID privat i erhvervsmæssig sammenhæng *sideløbende* med NemID medarbejdersignatur. Det kan indebære en koordineret og bredere anvendelse af NemID privat, fx så enkeltmandsvirksomheder altid kan anvende NemID privat, ligesom det kan udvides til, at andre virksomheder kan

vælge det. Denne mulighed analyseres, da den kan forventes at løse en række vigtige udfordringer uden at skabe for stor kompleksitet eller være omkostningsdrivende.

Løsningen skal dække de forretningsmæssige behov hos en meget stor del af borgere og virksomheder for lettere og mere brugervenlig login samt lette administrationen af erhvervsløsninger, som det er beskrevet ovenfor. Der er dermed et vist overlap mellem dette element og element C.

Grundtanken i denne løsning er at give flere muligheder for at anvende NemID privat i virksomhedssammenhæng.

Denne løsning vedrører alene medarbejdersignaturer og indebærer ikke ændring i muligheden for nøglefilsløsninger til erhverv.

Løsningselementets nye funktionaliteter

I den nuværende løsning kan ejere af personligt ejede virksomheder anvende NemID privat i forbindelse med tjenester fra SKAT, ATP mv. Både SKAT og ATP har etableret egne løsninger til at knytte ejere til deres virksomheder.

I løsningselementet kan indgå flere muligheder for at anvende NemID privat i virksomhedssammenhæng, herunder:

- I personligt ejede virksomheder kan ejer *juridisk* set umiddelbart anvende NemID privat i forbindelse med virksomheden. For øjeblikket kan flere offentlige tjenester dog ikke *teknisk* imødekomme dette.
- I forbindelse med foreninger og lignende, hvor 'almindelige borgere' udfører opgaver for en organisation uden at være medarbejdere. Her skal der findes en løsning på, hvordan en borger knyttes til en forening som alternativ til at udstede NemID medarbejdersignaturer til disse.
- Mulighed for at anvende NemID privat i forhold til flere typer virksomheder.

Der vil være behov for at afklare, hvem der afgør, om en medarbejder kan eller skal anvende sit NemID privat i erhvervssammenhæng. Bestemmer medarbejderen eller virksomheden selv, eller skal parterne være enige?

13.4.2.1 Mulighed for anvendelse eller styret udbredelse af NemID privat til erhverv

Et væsentligt spørgsmål er, om der alene etableres mulighed for bredere anvendelse af NemID privat i erhvervssammenhæng, eller om det er et mål at sikre en sammenhængende og koordineret anvendelse af NemID privat i erhvervssammenhæng. Med andre ord om offentlige tjenesteudbydere selv vælger, eller om det gøres obligatorisk at give virksomhederne denne mulighed.

For virksomhederne betyder det forskellen på, om de som nu skal have to NemID eller i fremtiden kan nøjes med en.

En sammenhængende og koordineret udbredelse indebærer dels en styringsmodel for udbredelse, dels en forpligtelse for myndigheder til at sikre, at NemID privat kan anvendes.

Det er RMC-ICG's anbefaling, at der stiles efter en styret udbredelse af NemID privat til erhverv, idet det er afgørende for brugerne, at de kan vælge at anvende NemID privat i alle sammenhænge. Hvis blot en enkelt udbredt løsning stiller krav om NemID medarbejdersignatur, skal virksomhedsejeren have både NemID privat og NemID medarbejdersignatur.

13.4.2.2 Administrative løsninger, der knytter NemID privat til virksomheder

Anvendelse af NemID privat i forbindelse med virksomheder kræver administrative løsninger til at knytte borgeren til virksomheden og registre, der understøtter dette.

I forhold til tilslutning af personligt ejede virksomheder har Erhvervsstyrelsen registreret ejeren og kan oplyse om sammenhængen mellem borger og virksomhed. Disse oplysninger stilles til rådighed i en tjeneste, der angiver, at en person (et CPR-nummer og/eller et PID-nummer) personligt ejer en virksomhed (et CVR-nummer).

For en række selskaber og foreninger kan det være relevant at lade medarbejdere og fx bestyrelsesmedlemmer udføre opgaver med NemID privat i stedet for at udstede NemID medarbejdersignaturer.

I forhold til selskaber og foreninger er der brug for sikre data af høj kvalitet, for at en borger kan tegne selskabet/foreningen med sit NemID privat. For en række af selskaber og foreninger har Erhvervsstyrelsen registreringer, som kan anvendes (tegningsregel og ejer) i forbindelse med den tegningsberettigedes tilslutning af virksomheden, og som betyder, at NemID privat kan anvendes af den tegningsberettigede.

NemID-administrator har behov for en administrationsløsning, hvor han giver en borger med NemID privat rettighed i forhold til foreningen/virksomheden.

Rettigheden kan udformes som en generel medarbejderrolle (svarende til det funktionelle indhold i NemID medarbejdersignatur).

Det skal nærmere analyseres, hvordan der kan etableres løsninger, der kan understøtte administration af medarbejderes tilknytning til selskabet/foreningen. Som udgangspunkt anbefaler RMC-ICG, at dette sker i forbindelse med NemLog-in, i overensstemmelse med princippet om, at NemID alene løser opgaven med identifikation, mens håndtering af rettigheder ligger i NemLog-in. Hermed skabes der tillige mulighed for inden for ét og samme system at skabe enklere brugerrejser for tilknytning af medarbejdere og tildeling af rettigheder til denne.

Der vil yderligere være behov for analyser af, om data om en borgers tilknytning til en virksomhed skal være til rådighed for private tjenester (der er cirka 100 tjenester, der betjener virksomheder), og i givet fald hvordan.

13.4.2.3 Brugervenlighed

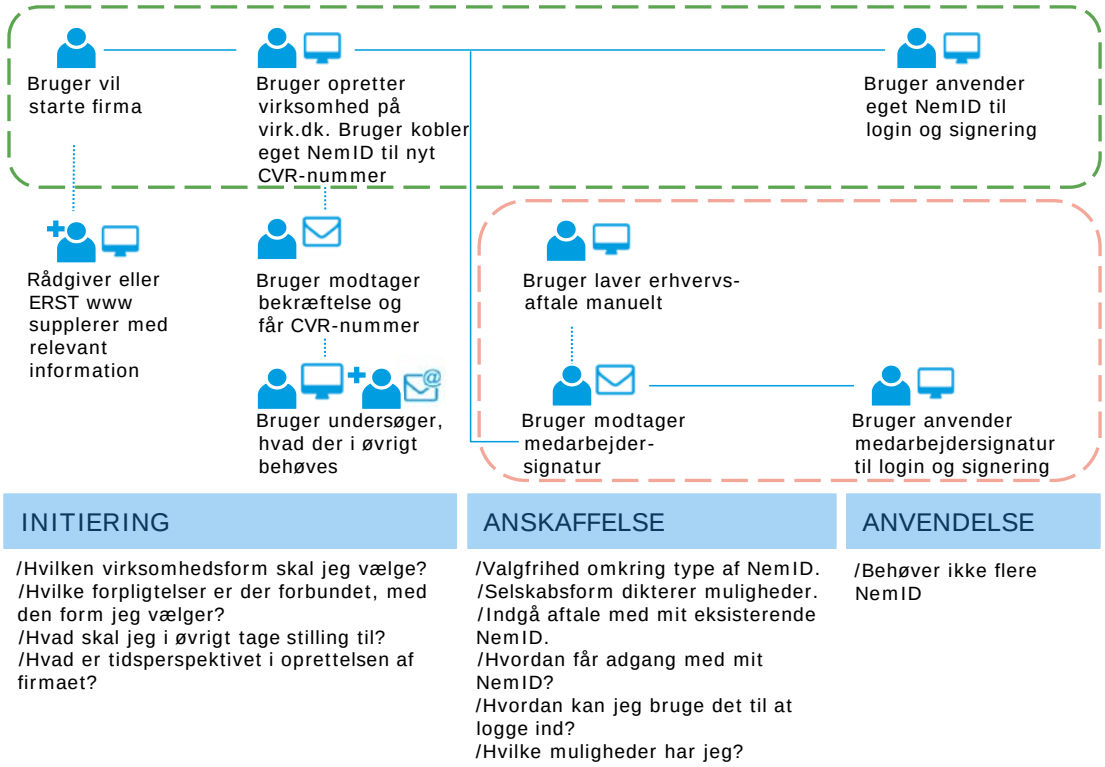
Overordnet set kan man betragte brugervenligheden for løsningselementet som mere forenklet, idet et eller flere led kan fjernes fra brugerrejsen og opgaveudførelsen. I tilfælde af, at NemID til private erstatter en medarbejdersignatur, vil brugerne opleve, at de har mulighed for at logge ind med et NemID, de i forvejen har, i stedet for at skulle anskaffe et nyt NemID.

Indsigter i forbindelse med brugeranalysen peger på, at slutbrugerne foretrækker en enklere anvendelse af NemID som for eksempel at kunne benytte ét NemID til flere forskellige roller. På et konceptuelt niveau blev det vel modtaget i alle tre målgrupper (borgere, virksomheder og myndigheder) at betragte brugeren som én person, der kunne have flere og forskelligartede roller tilknyttet én adgang.

Nedenstående brugerrejse illustrerer brugerens forskellige berøringspunkter og overvejelser ved oprettelse af personligt ejet firma, jf. løsningselement B. Den repræsenterer dermed blot en ud af flere brugerrejser i løsningselementet. Den grønne ramme indikerer den fremtidige løsning, og den røde ramme er trin i brugerrejsen, der vil udgå.

Anskaffelsesproceduren forventes at blive forbedret, idet en godkendelse via brev og underskrift erstattes af en digital godkendelse, hvilket fjerner barrieren ved at modtage, underskrive og returnere et fysisk dokument. Anvendelsen af NemID er ligeledes forbedret ved, at brugeren har udvidet mulighed for at reducere antallet af certifikater og tage udgangspunkt i én adgang.

Figur 19: Brugerrejse for oprettelse af nyt firma



Brugere, der forventes at vælge NemID privat i øvrige sammenhænge, kendetegnes bl.a. ved:

- Sjælden brug af medarbejdersignatur.
- Begrænset behov og kendskab til NemID-økosystemet.
- Begrænset behov for og kendskab til rettighedstildeling og -styring.
- Forskelligarterede opgaver i forbindelse med deres rolle(r).
- Behov for support, når noget går galt.
- Behov for at kunne agere på vegne af flere CVR-numre.

Fordele

I Fase 1 er indhøstet indsigter om, at fokus på formidling, bredere anvendelse af NemID, papirløs tilmeldingsproces og gratis adgang til support vil give høj værdi for brugere i målgruppen.

Konceptet omkring NemID-profilen, hvor ét NemID giver adgang til en række funktioner, blev i Fase 1 prioriteret højest blandt alle tre målgrupper. Samtidig vil løsningselementet give mulighed for at formidle en simplificeret udgave af NemID-anvendelsen.

Udfordringer

Ofte vil brugergrænsefladers kompleksitet stige i takt med, at man introducerer valgmuligheder ved udvalgte funktioner. Den bruger, der ønsker at gå den simpleste vej fra A til B, vil muligvis opleve flere valgmuligheder undervejs som en forhindring.

Omvendt kan valgmuligheder sikre et bedre match mellem tilgængelige funktioner og forskellige slutbrugeres behov, hvilket vil resultere i øget værdi og god brugeroplevelse. Følges principperne i brugercentreret design, sikres samtidig, at formidlingen og placering af valgmuligheder bliver mest hensigtsmæssig for de forskellige typer af brugere. Dette forventes især at være relevant for tjenesteudbyderne og kun i mindre omfang for NemID.

13.4.3 Gevinster

Dette afsnit har til formål at præsentere de gevinster, løsningselementet kan give. Gevinsterne differentieres i forhold til de forskellige relevante brugergrupper.

13.4.3.1 Virksomheder, herunder private virksomheders medarbejdere

De virksomheder, som ønsker fortsat at anvende NemID medarbejdersignatur, vil ikke opleve ændringer med denne løsning.

De virksomheder, der ønsker at anvende NemID privat i erhvervssammenhæng, vil kunne opnå enklere arbejdsgange og mere forståelige begreber i oprettelsessituationen. De medarbejdere, som kan nøjes med at have et NemID, vil desuden have fordele i anvendelsen.

Hvis der satses på en styret og koordineret udbredelse af NemID privat, hvorved virksomheder, som ønsker at anvende NemID privat, ikke bliver mødt med krav om anvendelse af NemID medarbejdersignatur, vil det særligt gavne de mange mindre virksomheder, herunder de 270.000 enkeltmandsvirksomheder, som tænkes at være den primære målgruppe.

Da der kun i meget begrænset omfang anvendes NemID medarbejdersignatur til private tjenester, vil gevinsterne for virksomhederne i forhold til private tjenester være begrænsede. Hvis der sker en større udbredelse af anvendelsen af NemID medarbejdersignatur til private tjenester, bør det også undersøges, om og hvordan NemID privat kan anvendes af disse.

13.4.3.2 Myndigheder, herunder myndighedernes medarbejdere

De myndigheder, som ønsker fortsat at anvende NemID medarbejdersignatur, vil ikke opleve ændringer med denne løsning.

Der kan opnås gevinster for de myndigheder, der med løsningen får udvidet mulighed for, at deres medarbejdere kan anvende NemID privat i arbejdssammenhæng.

13.4.3.3 Private tjenesteudbydere

For private tjenesteudbydere vil løsningen give forskellige gevinster, afhængigt af den valgte løsning:

Der vil ikke være nogen ændring, hvis der ikke åbnes mulighed for private tjenesteudbydere til at få adgang til de data om CVR-tilknytning og tilhørende rettigheder, som ligger i login-tjenesten, jf. at NemLog-in ikke stilles til rådighed for private.

Der vil være bedre muligheder, hvis der stilles en tjeneste til rådighed for private tjenesteudbydere, der har brug for data om CVR-tilknytning og tilhørende rettigheder som en separat rettighedsinformationstjeneste eller som del af en login-tjeneste.

13.4.3.4 Offentlige tjenesteudbydere

Mange offentlige tjenesteudbydere er fokuseret på enten borgere eller virksomheder, mens andre offentlige tjenesteudbydere servicerer begge målgrupper. Disse forskelle i målgrupper har konsekvenser for de tekniske løsninger, der skal etableres.

Offentlige tjenesteudbydere vil fortsat anvende NemLog-in og vil kun opleve mindre ændringer i løsningen. Dette undersøges nærmere nedenfor.

13.4.4 Vurdering

Dette afsnit har til formål at analysere og vurdere løsningselementet i forhold til relevante parametre.

13.4.4.1 Arkitektur

For den del af løsningen, der indebærer, at NemID privat kan anvendes i erhvervssammenhæng, foreslås der etableret følgende funktionalitet i en eller flere rettighedsinformationstjenester:

- En funktion, der knytter en person med et NemID privat som tegningsberettiget med en eller flere CVR-registrerede virksomheder, blandt andet med brug af Erhvervsstyrelsens registreringer.
- En funktion, der alene beskriver personens generelle tilknytning til et CVR-nummer svarende til tilknytningen med en NemID medarbejdersignatur (dvs. er tilknyttet virksomheden). Det

kræver, at virksomheder har knyttet brugeren (identificeret ved det personlige NemID) til virksomheden.

Der er store krav til kvaliteten af sådanne tjenester, fx i forbindelse med konkurser. Her skal tjenesten kunne sikre, at ejer (eller anden funktion) ikke længere har de ovennævnte rettigheder. I dag sker det ved, at NemID medarbejdersignaturer spærres ved virksomhedens ophør eller konkurs.

Informationstjenesterne kan etableres som en del af NemLog-in eller som særskilte tjenester i Erhvervsstyrelsen eller Digitaliseringsstyrelsen.

Der vil være behov for at tilpasse NemLog-in Brugeradministration, så det også er muligt at administrere rettigheder for medarbejdere med NemID privat.

For offentlige tjenesteudbydere vil informationer vedrørende CVR-tilknytning og rettigheder kunne leveres af NemLog-in, som får data fra de ovennævnte informationstjenester. Informationer kan indgå i SAML-responses, og det er muligt i den nuværende SAML 2.0 standard.

Tjenesterne skal gennemføre ændringer i brugerdialogen, så der tages højde for brugere med NemID privat.

13.4.4.2 Sikkerhed og privacy

For borgeren som medarbejder er der er behov for at vurdere, hvilke hensyn der skal tages til, om borgeren overtales eller tvinges til at anvende NemID privat i forbindelse med sin ansættelse.

De ovennævnte informationstjenester vil indeholde information vedrørende borgeres tilknytningsforhold til virksomheder og organisationer. Disse oplysninger vurderes dog ikke at være imod hensynet til privacy.

Det skal dog afklares, om borgeren kan nægte, at oplysningerne videregives, og i så fald om det påvirker muligheden for, at NemID privat kan anvendes i virksomhedssammenhæng.

For borgeren som virksomhedsejer vurderes det ikke, at der er privacy-hensyn, blandt andet fordi virksomhedsejeren selv kan bestemme, om han vil bruge NemID privat eller medarbejdersignatur.

13.4.4.3 Migrering

Migrering behandles i forhold til forskellige parter i økosystemet:

NemID

Ingen ændringer, idet NemID fortsat skal have samme funktioner som nu.

Regler i forbindelse med NemID (fx certifikatpolitikker) og vejledninger skal ændres.

Brugergrænsefladerne i NemID skal tilpasses, så brugerne oplever en sammenhængende proces fra tilslutning til NemID og tilknytning af personlig NemID.

Rettighedsinformationstjenester

Der skal etableres rettighedsinformationstjenester enten som selvstændige tjenester eller som del af NemLog-in.

I det omfang der skal etableres tjenester i forbindelse med NemLog-in, skal det undersøges, om det kan ske i indeværende kontraktperiode, eller om det først kan etableres efter ny kontrakt. I så fald må der forventes længere tid til implementering.

NemLog-in

NemLog-in skal implementere snitflade til rettighedsinformationstjenesterne med rettigheder ”ejer af virksomhed” og ”generel medarbejder”.

Hvis opgaverne placeres i NemLog-in, skal der desuden gennemføres ændringer i brugerrettighedsadministrationen, således at følgende funktioner implementeres:

- For personligt ejede virksomheder skal der automatisk tildeles fulde rettigheder til ejer.
    - Omfanget af ”fulde rettigheder” skal afklares.
    - Det skal være muligt for ejeren at se dette ud fra et princip om gennemsigtighed (privacy).
- Der skal oprettes rettigheden ”generel medarbejder”.
- For øvrige virksomheder skal de nuværende administrative løsninger fortsætte. De nødvendige forbedringer her behandles i afsnit 13.5 *Løsningselement C: Bedre administrative løsninger til virksomheder*.

Hvis også private tjenesteudbydere skal understøtte anvendelse af NemID privat til erhvervsformål, skal de også have adgang til de nævnte informationstjenester. Og hvis rettighedstjenesten er en del af NemLog-in, skal NemLog-in stille denne tjeneste til rådighed.

Det skal overvejes i forhold til NemLog-in’s tidsplaner, hvilke dele det er muligt og økonomisk forsvarligt at implementere under nuværende kontrakt, og hvilke der først indgår efter nyt udbud.

Tjenester

For tjenesterne er det afgørende, om det vælges alene at stille muligheden for at anvende NemID privat til erhvervsformål til rådighed, eller om det skal ske i en styret og koordineret proces.

I sidstnævnte tilfælde skal tjenesterne implementere de ændringer, der er beskrevet ovenfor.

Da ændringerne gennemføres for at gavne virksomhederne, og da gevinsterne for virksomhederne er afhængig af, at alle tjenester understøtter anvendelse af NemID privat, er der behov for en sammenhængende plan for, hvornår tjenesterne har gennemført implementeringen.

13.4.4.4 Relation i forhold til private partnere

Det nuværende samarbejde med bankerne omfatter kun NemID privat, idet NemID medarbejdersignatur udelukkende er finansieret af det offentlige og af virksomhederne selv og ikke bruges af bankerne.

Bankerne har implementeret egne løsninger, ligesom mindre virksomheder i nogle banker kan anvende NemID privat til deres erhvervsnetbank, mens andre banker har en parallel NemID til medarbejdere, der udelukkende kan anvendes til autentifikation og signering af transaktioner i den konkrete bank. Den hedder NemID til erhverv til bank:

https://www.nemid.nu/dk-da/erhverv/nemid_til_erhverv/nemid_erhverv_til_bank/

Således kan en medarbejder i en virksomhed have et personligt nøglekort, et nøglekort til anvendelse over for offentlige sites som medarbejder og et nøglekort til anvendelse over for bank som medarbejder. En frivillig for en forening vil ofte ligeledes have to nøglekort eller et nøglekort og en NemID medarbejdersignatur for at kunne agere på vegne af foreningen over for det offentlige og banken.

Det betyder, at erhvervsbrugere i øvrigt skal anvende forskellige akkreditiver, herunder forskellige brugernavne og kodeord. Det er ikke undersøgt, om det påvirker brugeroplevelsen. En mulighed kan være, at det er forskellige personer i virksomhederne, der anvender forskellige tjenester og dermed forskellige login-løsninger. Der er behov for yderligere undersøgelser af dette.

Der kan være sikkerhedsmæssige og administrative fordele ved, at den tunge anvendelse hos en privat partner og anvendelse i offentlig sammenhæng hænger bedre sammen. Det kan sikre, at virksomhederne kan administrere alle medarbejdere på samme måde og eventuelt med samme snitflade. Det kan desuden sikre effektiv lukning af brugeres adgang ved stillingsændringer og stillingsophør.

13.4.4.5 OCES-certifikatpolitikker

Anvendelse af personlig NemID i erhvervssammenhæng kræver hverken ændringer i certifikatpolitikken for OCES-personcertifikater eller OCES-medarbejdersignaturer.

13.4.4.6 Økonomi

Løsningselementet: *Økonomiske konsekvenser i hele NemID-økosystemet*.

I NemID er der ingen ændringer i teknik, alene ændringer i vejledninger og retningslinjer. De skønnede udgifter er få hundrede tusinde kroner.

Den fællesoffentlige indsats vil kræve ressourcer til følgende:

- En informationstjeneste, der knytter en person (PID) med en eller flere virksomheder (CVR), har skønnede udgifter til etablering af tjenesten på et par millioner kroner, og tilsvarende til drift af tjenesten i fem år. Udgifterne bygger på, at data kan hentes fra Det Centrale Virksomhedsregister (CVR), således at der skal opbygges integrationer hertil samt bygges komponenter til at udstille disse data. Samlet set en forholdsvis begrænset løsning.
- En informationstjeneste, der beskriver personens generelle tilknytning til et CVR-nummer svarende til den tilknytning, en NemID medarbejdersignatur indebærer. Det kræver, at virksomheden har knyttet brugeren (identificeret ved det personlige NemID) til virksomheden. Udgifter til udvikling skønnes til et par millioner kroner, og tilsvarende til drift af tjenesten i fem år. Udgifterne bygger på, at data kan hentes fra CVR-registret og fra et brugerinterface, hvor virksomhedens administrator knytter personen til virksomheden. Der skal opbygges integrationer til CVR-registret og et brugerinterface samt database. Der skal bygges komponenter til at udstille disse data. Samlet set en forholdsvis begrænset løsning.
- En informationstjeneste, der beskriver, hvilke mere specifikke rettigheder personen har i forhold til et CVR-nummer (fx tegningsberettiget, NemID-administrator, sekretær mv.). Det kræver, at virksomheden har administreret brugerens rettigheder. Skønnede udgifter til udvikling og drift af tjenesten i fem år på 5-10 millioner kroner. Udgifterne bygger på, at der skal opbygges et brugerinterface, hvor virksomhedens administrator knytter personen til virksomheden og administrerer forskellige typer rettigheder. Der skal opbygges en database. Der skal bygges komponenter til at udstille disse data. Samlet set en lidt større løsning. Løsningen kan også bygges som en del af NemLog-in. Her forventes der mere funktionalitet for samme udgift.

Samlet set skønnes de fællesoffentlige merudgifter til dette løsningselement at være omkring 10-20 millioner kroner til udvikling og drift i kontraktperioden.

De enkelte tjenester vil have udgifter til tilpasninger af brugergrænseflader. Det skønnes, at der skal bruges mellem 200.000 og 1 million kroner pr. tjeneste. Beløbet skal dække tilpasning af tekniske snitflader til at hente data i ovennævnte informationstjenester og eventuelt til at opbygge brugergrænseflader til, at personer med flere tilknyttede CVR-enheder kan vælge mellem disse. Ved at lægge flere af disse opgaver i en fælles løsning som NemLog-in kan udgifterne for de enkelte tjenesteudbydere nedbringes. Det skønnes at berøre 10 tjenester.

13.4.4.7 Finansieringsmodeller

Løsningselementet vurderes kun at kunne finansieres af de offentlige tjenesteudbydere, der får omkostninger ved ændringer samt af de myndigheder, der får ansvaret for de nødvendige informationstjenester. Hverken Digitaliseringsstyrelsen eller Erhvervsstyrelsen forventes at kunne hente betaling fra brugerne for disse tjenester, bl.a. fordi der arbejdes på at gøre denne type grunddata gratis for brugerne.

13.4.4.8 Leverandørstrategi

En tjeneste med oplysning om personligt ejerskab kan etableres af Erhvervsstyrelsen med deres leverandører.

En tjeneste med oplysning om generel medarbejderrolle kan løses af Digitaliseringsstyrelsen eller af Erhvervsstyrelsen.

Rettighedstjeneste kan leveres af Digitaliseringsstyrelsen i forbindelse med NemLog-in med de af Digitaliseringsstyrelsen valgte leverandører.

13.4.4.9 Risici

Opgaven kan gennemføres trinvist. Som det første skridt skal der etableres to centrale CVR-tjenester, og herefter kan tjenesterne implementere understøttelse af NemID privat i forbindelse med forskellige virksomhedstyper.

Der er stor risiko for, at ikke alle tjenester vil implementere dette, således at virksomheder alligevel skal have både en personlig NemID og en NemID medarbejdersignatur.

13.4.4.10 Juridiske problemstillinger

Der vurderes at være behov for en nærmere afklaring af eventuelle juridiske forhold blandt andet vedrørende sikkerhed som følge af en mere udbredt anvendelse af privat NemID på erhvervsområdet.

13.4.4.11 Styringsmæssige problemstillinger

En bedre understøttelse af NemID privat til virksomheder stiller krav til indsats i flere dele af NemID-økosystemet, og det vil være nødvendigt at sikre en styring af aktørernes indsats, hvis virksomhederne skal opnå en enklere brug.

- Lovmæssig ramme:
  - Der kan etableres lovgrundlag, der utvetydigt muliggør anvendelse af NemID privat i de ønskede sammenhænge.
  - Der kan etableres lovgrundlag for, at tjenesteudbydere SKAL understøtte NemID privat i forbindelse med angivne virksomhedstyper og tjenester.
  - Alternativt kan dette ske på bekendtgørelses- eller cirkulæreniveau i den udstrækning, der er hjemmel hertil.
- Strategisk ramme:
  - Det kan indgå i den kommende digitaliseringsstrategi med initiativer og de styringsmæssige redskaber, der etableres i forbindelse hermed.
- Dedikeret governance-organisation
  - Der kan etableres en governance-organisation, der får bemyndigelse til at fastlægge tidsplaner for offentlige tjenesters understøttelse af NemID privat for udvalgte virksomhedstyper.

Der skal træffes beslutninger om, i hvilket omfang andre end personligt ejede virksomheder kan anvende NemID privat, ligesom der skal fastlægges regler og procedurer, fx vedrørende medarbejdernes valgmuligheder.

13.4.5 Samlet vurdering for løsningselementet

En bredere anvendelse af NemID privat i erhvervssammenhæng vil kunne gennemføres uden ændringer i NemID. Der vil være behov for juridiske afklaringer, og for en fællesoffentlig indsats for løsninger, der knytter borger og virksomhed sammen. Derudover vil der ikke mindst være behov for, at tjenesteudbyderne implementerer anvendelsen i praksis.

Tabel 14: Opsummering af RMC-ICG's vurdering af løsningselement B

Vurderingsparametre	RMC-ICG's vurdering
Arkitektur	Ingen ændring i NemID med nye elementer i økosystemet.
Sikkerhed og privacy	Ingen problemer.
Migrering	Der skal etableres informationstjenester, og tjenester skal tilpasses.
Relation i forhold til private partnere	Der bør være dialog med private partnere om, at de også understøtter anvendelse af NemID privat til erhverv.

Vurderingsparametre	RMC-ICG's vurdering
OCES-certifikatpolitikker	Ingen ændringer.
Økonomi	Der vil være meget begrænsede fællesoffentlige merudgifter i NemID, men udgifter andre steder i økosystemet.
Finansieringsmodeller	Vurderes kun at kunne finansieres af det offentlige.
Leverandørstrategi	Informationstjenester kan leveres af andre end NemID-leverandøren.
Risici	Opgaven kan gennemføres trinvist og med lav projektrisiko. Der er stor risiko for, at ikke alle tjenester vil implementere dette, således at virksomheder alligevel skal have både en personlig NemID og en NemID medarbejdersignatur.
Juridiske problemstillinger	Ingen i NemID. Der kan være juridiske forhold i tjenesters brug af NemID privat til erhverv.
Styringsmæssige problemstillinger	En bedre understøttelse af NemID privat til virksomheder stiller krav til indsats i flere dele af NemID-økosystemet, og det vil være nødvendigt at sikre en styring af aktørernes indsats, hvis virksomhederne skal opnå en enklere brug. Der skal træffes valg om, hvilke virksomhedstyper der kan anvende løsningen.

13.5 Løsningselement C: Bedre administrative løsninger til virksomheder

I dette afsnit præsenteres løsningselementet *bedre administrative løsninger til virksomheder*. Herefter analyseres de overordnede potentielle forretningsmæssige gevinster. Dernæst foretages en vurdering af løsningselementet, og afsnittet afsluttes med en konklusion.

13.5.1 Præsentation af løsningselementet

Løsningselementet vedrører alene NemID medarbejdersignatur.

Elementer i løsningen

Der indgår en række forskellige elementer i en bedre erhvervsløsning. Disse elementer er udarbejdet på grundlag af dele af Erhvervsstyrelsens Virksomhedsanalyse.

Desuden indgår input fra regionernes analyse, med fokus på regionernes særlige behov som meget store virksomheder i forhold til NemID. De fem regioner har således i alt 80.000 NemID. Det er RMC-ICG's vurdering, at regionernes behov deles af mange andre storbrugere af NemID medarbejdersignaturer, fx kommuner og mellemstore og store virksomheder.

Elementerne omfatter dels mere brugervenlige og virksomhedsrettede tilslutningsforløb, dels mere brugervenlige løsninger til løbende administration af medarbejdersignaturer.

Brugerrettede tilslutningsprocesser for forskellige virksomhedstyper

Der er behov for at tilpasse brugergrænsefladerne til de meget forskellige brugergrupper, der skal tilslutte en virksomhed, forening eller lignende til NemID. Brugerne adskiller sig både i digitale kompetencer og i forhold til de typer juridiske enheder, de skal tilslutte.

Begrebet 'NemID medarbejdersignatur' skaber i sig selv stor forvirring blandt mange virksomhedsbrugere. Er man fx ejer af en enkeltmandsvirksomhed, opfatter man sig selv som selvstændig og lige netop ikke som medarbejder. Tilsvarende ser frivillige foreninger generelt ikke sig selv som

virksomheder eller medarbejdere. En mere brugerrettet sprogbrug kan lette tilslutningen og samtidig mindske supportopkald.

Et andet aspekt er, at hæftelses- og tegningsregler er forskellige afhængig af virksomhedsform, hvorfor tilslutningen til NemID varierer for virksomheder med forskellige virksomhedsformer. Derfor foreslås tilslutningsprocesserne tilpasset forskellige virksomhedsformer og med videst muligt brug af allerede indtastede data i fx Det Centrale Virksomhedsregister CVR.

Et tredje aspekt er at øge mulighederne for digital signering af aftaler om tilslutning til NemID. Det vil effektivisere processen i både virksomheden og hos leverandøren af NemID, hvis flere kan signere digitalt med deres personlige NemID privat.

På den måde vil det være muligt fx at kommunikere målrettet til frivillige foreninger, der almindeligvis ikke ser sig selv som virksomheder. Det vil være muligt at forenkle processen for de mange ejere af personligt ejede virksomheder, der ubegrænset kan repræsentere deres virksomhed.

Dette vil kræve:

- Udvikling af mere brugerorienteret sprog – eventuelt i sammenhæng med andre offentlige tjenester – og implementering heraf.
- Tilpasning af tilslutningssystemet med brugergrænseflader til 5-10 forskellige virksomhedsformer. Det skal ske på grundlag af en analyse af forskellige virksomhedsformer og brugernes behov.
- Understøttelse af digital signering ved, at Erhvervsstyrelsen stiller data med tilstrækkelig kvalitet til rådighed om koblingen mellem tegningsberettigedes identitet og virksomhedens CVR-nummer.
- Snitflade til opslag i CVR-registret.

Dette vil bidrage til mere brugervenlige og effektive administrative processer for de 60-65.000 virksomheder mv., der oprettes hvert år.

Forenklet administration af NemID medarbejdersignatur til virksomheder med 1-3 NemID medarbejdersignaturer

Der er i dag udstedt cirka 405.000 medarbejdersignaturer i virksomheder, der blot har 1-3 medarbejdersignaturer. Der er dermed et forholdsvist stort antal virksomheder, der kun har behov for at anvende få medarbejdersignaturer.

Der bør udvikles mere brugervenlige administrationsløsninger målrettet virksomheder med få medarbejdersignaturer, fx ved at denne gruppe undgår at møde NemID-administratorrollerne. Dette kan implementeres ved, at de enten bliver tildelt NemID-administratorrollerne, uden at de skal forholde sig aktivt hertil, eller ved at de kan oprette og administrere deres simple behov uden at blive administratorer. I den forbindelse er det væsentligt at holde sig for øje, at også disse virksomheder kan have behov for at kunne tildele fuldmagt til tredjepart.

Dette vil kræve en tilpasning af brugergrænseflader i forbindelse med oprettelse af medarbejdersignaturer, så de sprogligt og funktionsmæssigt er målrettet juridiske enheder med behov for et begrænset antal medarbejdersignaturer.

Funktioner for myndigheder og virksomheder med mange NemID medarbejdersignaturer

Regionerne ønsker, at de regionale brugeradministrationssystemer skal være det primære værktøj til håndtering af brugere, således at der, når en bruger oprettes i det regionale brugeradministrationssystem, samtidig bestilles en medarbejdersignatur hos NemID-operatøren. For hovedparten af regionerne sker dette allerede i dag gennem anvendelse af tekniske snitflader hos NemID-operatøren. Regionerne ønsker, at der også i næste generation NemID er sådanne snitflader til at oprette og foretage ændringer vedrørende brugere af NemID.

Regionerne ønsker desuden en udvikling af den nuværende NemID-administratorrolle, så forskellige administratorgrupper i regionen kan få forskellige privilegier i forhold til administrationen. Ønsket er at kunne tilbyde decentralisering af dele af arbejdet med indrulning og mere selvbetjening

til medarbejderne i forhold til administration af digital identitet. Den nuværende løsning kræver mellemkomst af en NemID-administrator, hvilket ikke opleves som værdiskabende eller som en øget sikkerhedsfaktor, men alene opleves som en administrativ byrde uden formål.

Regionerne ønsker en fælles, personuafhængig administration, så der ikke fortsat er en tæt binding mellem en given NemID-administrator og grupper af NemID medarbejdersignaturer.

Det er som nævnt RMC-ICG's vurdering, at mange andre brugere med et stort antal NemID medarbejdersignaturer vil have tilsvarende behov for effektiv sammenhæng mellem interne brugerstyringsprocesser og administration af NemID.

Dette vil kræve:

- En udvikling af de nuværende tekniske snitflader i NemID med øget funktionalitet (som nærmere skal afdækkes).
- En udvikling af den nuværende NemID-administratorrolle med mere finmaskede rettigheder og større fleksibilitet i forhold til tilknyttede medarbejdersignaturer.

Det forventes, at disse ændringer kan medføre besparelser i regioners, kommuners og større virksomheders oprettelse og administration af medarbejdersignaturer. De cirka 12.000 virksomheder med mere end 10 medarbejdersignaturer administrerer skønsmæssigt 300-400.000 medarbejderes signaturer.

Samlet set betyder forslagene om bedre administrative løsninger til virksomheder følgende aktiviteter:

- Mere detaljeret analyse af, hvordan de forretningsmæssige behov kan dækkes blandt andet i dialog med interessenter. Heri indgår også analyser af juridiske forhold.
- Udvikling af mere målrettede brugergrænseflader til tilslutningsforløbet.
- Udvikling af mere målrettede brugergrænseflader til bestilling af medarbejdersignaturer.

13.5.1.1 Brugervenlighed

For brugere, der anvender NemID i erhvervsmæssige sammenhæng, vil brugergrænsefladerne blive lettere at anvende på flere vigtige områder. Med udgangspunkt i brugeranalysen og de koncepter, der blev udformet og valideret i målgruppen i Fase 1, beskriver løsningselementet en række forbedringer i forhold til:

- Smidigere brugerrejser i oprettelses- og aktiveringsflows på grund af optimerede processer i det bagvedliggende system.
- Brugen af begreber og sprog, som målgruppen kan forstå og relatere til deres virksomhedsdrift.
- Tydelig præsentation af værdifulde funktioner.

Fordele

I Fase 1 udtrykte brugere fra især målgrupperne for virksomheder og myndigheder, at de oplever mange uhensigtsmæssigheder i forbindelse med deres digitale administrative arbejdegange. Disse uhensigtmæssigheder spændte fra store forhindringer i brugergrænsefladen til små irritationsmomenter.

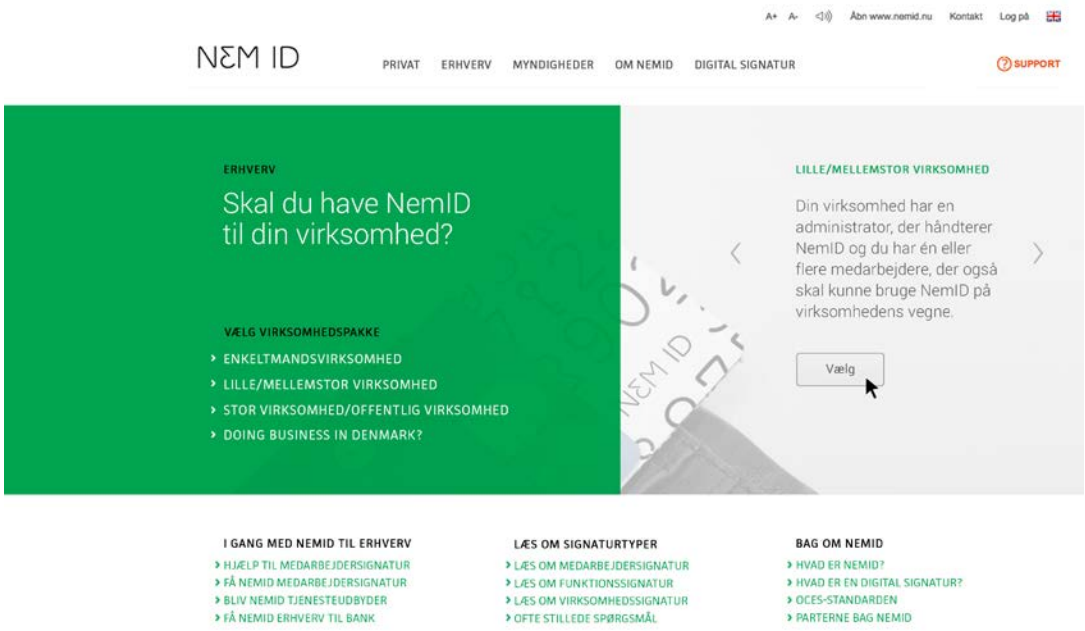
Implementering af løsningselement C og en kontinuerlig afdækning af brugernes behov, fx efter implementering, ved anvendelse af disse administrative brugergrænseflader har stort potentiale for den samlede brugeroplevelse i målgruppen.

Udfordringer

For brugere med gentagne opgaver i de samme brugergrænseflader er ændringer sjældent velkomne, alene ud fra den betragtning, at det er svært at ændre vaner. Fx kan der ske ændringer i anvendelsen af NemID i de forskellige brugerrejser, som Erhvervsstyrelsens selvbetjeningsunivers indeholder. Genvinsterne ved løsningselementet må dog forventes at kunne fungere som motivation for at gøre tingene på en anden og lettere måde.

Derudover kan det være en udfordring at tilpasse NemID til de mange forskellige brugerrejser.

Figur 20: Muligt grafisk design for optimeret oprettelses-flow



13.5.2 Gevinster

Dette afsnit har til formål at præsentere de gevinster, løsningselementet kan give. Gevinsterne i dette løsningselement tilfalder virksomheder, myndigheder og foreninger (juridiske enheder i CVR-registret).

Fokus er på at opnå gevinster i relation til de administrative processer, der er i forbindelse med tilslutning til NemID og oprettelse samt løbende administration af medarbejdersignaturer.

Efter implementeringen af obligatorisk Digital Post er der sket en omfattende oprettelse af NemID til nu 570.000 virksomheder og andre juridiske enheder. Fremover vil tilslutningsopgaven berøre de cirka 60.000-65.000 virksomheder og andre juridiske enheder, der oprettes hvert år, samt de virksomheder, hvor der skal administreres ændringer.

I forhold til den løbende administration af cirka 1 million medarbejdersignaturer forventes der dels en årlig stigning i det samlede antal på 500.000 som følge af øget digitalisering, dels håndtering af ændringer for forventet 20 % af de udstedte medarbejdersignaturer, dvs. 200.000 ændringer årligt. Det betyder oprettelser, ændringer og nedlæggelser af skønnet 250.000 medarbejdersignaturer årligt (det skønnede antal bygger på erfaringstal for personaleomsætning på cirka 20 % pr. år).

Mere brugervenlige tilslutningsprocesser for forskellige virksomhedstyper vil gavne størstedelen af de cirka 65.000 juridiske enheder, der hvert år oprettes i CVR-registret og efterfølgende tilsluttes NemID.

Forenklet administration af NemID medarbejdersignatur i virksomheder med 1-3 NemID medarbejdersignaturer vil være til gavn for skønnet mere end 300.000 virksomheder, som hvert år administrerer ændringer i forhold til cirka 400.000 medarbejdersignaturer i virksomheder, der blot har 1-3 medarbejdersignaturer.

Funktioner for myndigheder og virksomheder med mange NemID medarbejdersignaturer vil gavne forholdsvis få virksomheder og myndigheder (skønnet nogle få tusinde) med administration af skønnet 400.000 medarbejdersignaturer årligt.

Det forventes at øget fokus på brugervenlighed kan reducere virksomhedernes behov for support.

Mere end 10 % af alle supportkald er relateret til administration, og bedre brugergrænseflader forventes at kunne reducere disse supportkald.

13.5.3 Vurdering

Dette afsnit har til formål at analysere og vurdere løsningselementet i forhold til relevante parametre.

13.5.3.1 Arkitektur

Som nævnt vedrører forslagene administrative værktøjer i NemID, og forslagene vurderes ikke at have konsekvenser for andre dele af det samlede NemID-økosystem.

Inden for rammerne af NemID betyder forslagene en række ændringer i brugergrænsefladerne, hvor nuværende brugergrænseflader skal opdeles i mere differentierede brugergrænseflader på en måde, så brugerne mere eller mindre automatisk får præsenteret relevante udsnit.

De tekniske snitflader udvikles tilsvarende til at håndtere de mellemstore og store organisationers behov.

13.5.3.2 Sikkerhed og privacy

Løsningerne indebærer, at leverandøren af NemID skal have adgang til langt flere data om den enkelte virksomhed. Dog vurderes disse data at have lav fortrolighed, idet de i forvejen er offentligt tilgængelige.

Sikre processer i forbindelse med oprettelse af virksomheder har fx betydning for, at fx finansielle institutioner kan yde kredit, og for at risici for svindel og unddragelse af skat og moms kan minimeres.

Det bør derfor sikres, at overgangen til rent digitale løsninger kan ske på en måde og med redskaber, der ikke giver større risici for kriminalitet på erhvervsområdet.

En løsning, hvor flere funktioner løses med digital overførsel af data til NemID, stiller større krav til sikre processer i myndigheder og virksomheder. Kontroller heraf er en betingelse for, at sikkerheden svarer til den nuværende, hvor en NemID-administrator skal godkende manuelt.

13.5.3.3 Migrering

Løsningerne kan etableres trinvist. De kan etableres helt eller delvist i den nuværende kontraktperiode.

Flere af løsningerne kræver, at Erhvervsstyrelsen kan stille tjenester til rådighed med data i tilstrækkelig høj kvalitet.

13.5.3.4 Relation i forhold til private partnere

Det nuværende samarbejde med bankerne omfatter kun NemID privat, idet NemID medarbejdersignatur udelukkende er finansieret af det offentlige og af virksomhederne selv og ikke bruges af bankerne.

Forslagenes relation til private partnere afhænger derfor af, om medarbejdersignaturer bliver omfattet af en aftale.

13.5.3.5 OCES-certifikatpolitikker

Der indgår ændringer i tilslutningsforholdene og krav om tilpasning af sprog. Det kan have konsekvenser for OCES-certifikatpolitikkerne.

Ligeledes kan regionernes ønske om at begrænse behovet for NemID-administrators mellemkomst i administrationsprocessen betyde ændringer i OCES-certifikatpolitikker.

13.5.3.6 Økonomi

I dette løsningselement er der primært tale om fællesoffentlige udgifter til NemID. Mellemstore og store myndigheders og virksomheders etablering af snitflader til digital overførsel af brugerdata til NemID forudsættes kun at ske, hvor der er en positiv business case lokalt, og disse udgifter indgår derfor ikke.

Samlet set betyder forslagene følgende aktiviteter:

Der skal gennemføres en detaljeret analyse af, hvordan de forretningsmæssige behov kan dækkes blandt andet i dialog med interessenter samt analyser af juridiske forhold. Det skønnes, at der skal afsættes 300-500 timer til yderligere analyser svarende til 500.000 kroner.

Der skal udvikles mere målrettede brugergrænseflader til tilslutningsforløbet i NemID med udvikling af eksempelvis brugergrænseflader til forskellige virksomhedstyper samt udvikling af snitflader til CVR.

Der skal udvikles mere målrettede brugergrænseflader til bestilling og administration af medarbejdersignaturer til forskellige virksomhedstyper.

Det anslås, at bedre administrative løsninger med bedre brugergrænseflader kan reducere supportkald med 5 %, svarende til 500.000 kroner pr. år.

Der skal udvikles funktioner for myndigheder og virksomheder med mange NemID medarbejdersignaturer. Det indebærer udvikling af de nuværende tekniske snitflader i NemID med øget funktionalitet (som nærmere skal afdækkes) samt udvikling af den nuværende NemID-administratorrolle med mere finmaskede rettigheder og større fleksibilitet i forhold til tilknyttede medarbejdersignaturer.

De samlede udgifter til udvikling og drift i kontraktperioden skønnes at være 10-20 millioner kroner.

13.5.3.7 Finansieringsmodeller

Løsningerne i dette element er alle forbedringer og udbygninger af NemID-administratormodulet, som er en del af NemID-løsningen. Løsningen skal derfor anskaffes som en del af den samlede løsning, som finansieres fællesoffentligt. Det vil være muligt at øge prisen for NemID til erhverv for helt eller delvist at finansiere udgifterne. Finansieringsmulighederne skal derfor ses i sammenhæng med beslutninger om betalingsmodeller.

Samlet vurderer RMC-ICG, at løsningselementet skal finansieres af det offentlige.

13.5.3.8 Leverandørstrategi

Erhvervsstyrelsens tjenester skal leveres af Erhvervsstyrelsens leverandør.

De øvrige tekniske løsninger skal leveres af leverandøren af NemID til erhverv eller af andre leverandører med specialviden om forskellige virksomhedsgrupper.

13.5.3.9 Risici

Der vil være risici i forbindelse med anskaffelse, udvikling, implementering og migrering.

13.5.3.10 Juridiske problemstillinger

Der vurderes ikke at være juridiske problemstillinger i dette element.

13.5.3.11 Styringsmæssige problemstillinger

Der vurderes ikke at være styringsmæssige problemstillinger i dette element.

Dog vil ønsker fra brugerne om bedre sammenhæng i brugergrænsefladerne i forskellige offentlige tjenester stille krav til styring af brugergrænseflader på tværs af myndigheder.

13.5.4 Samlet vurdering for løsningselementet

Udvikling af de administrative løsninger i NemID for virksomheder og myndigheder kræver alene ændringer i NemID-administrationsmodulet. Der vil være fællesoffentlige udgifter hertil, men indsatsen vil betyde store gevinster i form af administrative lettelser i virksomheder og for myndigheder.

Tabel 15: Opsummering af RMC-ICG's vurdering af løsningselement C

Vurderingsparametre	RMC-ICG's vurdering

Vurderingsparametre	RMC-ICG's vurdering
Arkitektur	Ingen arkitekturmæssige konsekvenser, da der alene skal ske forbedringer i NemID-administrationsmodul mv.
Sikkerhed og privacy	Der skal være mekanismer til at sikre mod misbrug af identitet.
Migrering	Ændringer alene i NemID.
Relation i forhold til private partnere	Afhænger af, om medarbejdersignaturer omfattes af aftale med partner.
OCES-certifikatpolitikker	Ændringer i administrative løsninger kan have konsekvenser for OCES-certifikatpolitikker.
Økonomi	Begrænsede fællesoffentlige udgifter (cirka 20-30 millioner kroner).
Finansieringsmodeller	Vurderes at skulle finansieres af det offentlige.
Leverandørstrategi	Leveres som del af grundløsningen.
Risici	Ingen særlige risici.
Juridiske problemstillinger	Der vurderes ikke at være juridiske problemstillinger i dette element.
Styringsmæssige problemstillinger	Der vurderes ikke at være styringsmæssige problemstillinger i dette element. Dog vil ønsker fra brugerne om bedre sammenhæng i brugergrænsefladerne i forskellige offentlige tjenester stille krav til styring af brugergrænseflader på tværs af myndigheder.

13.6 Samlet konklusion for Scenarie 2

13.6.1 Samlede gevinster

RMC-ICG har vurderet gevinsterne ved scenariet ud fra de overordnede gevinster, der er beskrevet i afsnit 4.

Tabel 16: Oversigt over RMC-ICG's gevinstvurdering for Scenarie 2

Gevinst	RMC-ICG's vurdering
Høj tillid til løsningen	Ingen ændring.
Lettere anvendelse for borgere	Forbedring i kraft af mulighed for 1-faktor-login (Element A).
Lettere anvendelse for virksomheder	Forbedring i kraft af de mange enkeltmandsvirksomheders mulighed for at benytte NemID privat (Element B).
Lettere administration for virksomheder og myndigheder	Store forbedringer som følge af indsatsen i Element B og C.
Flere offentlige tjenester anvender det nye NemID	Stigning som følge af muligheden for at anvende 1-faktor-login (Element A).
Flere private tjenester anvender det nye NemID	Stor stigning som følge af muligheden for at anvende 1-faktor-login (Element A).
Mere fleksible udviklingsmuligheder	Store forbedringer som følge af muligheden for at adskille autentifikation og signering (Element A).

Scenariet betyder en fortsat høj tillid til løsningen og lettere anvendelse for borgere i kraft af 1-faktor-login.

Virksomheder, der ønsker at anvende NemID privat i erhvervssammenhæng, vil få lettere anvendelse og dermed tidsbesparelser som følge af muligheden for at anvende NemID privat i erhvervssammenhæng.

Virksomheder og myndigheder vil få betydeligt bedre administrationsmuligheder end i den nuværende løsning.

Tjenesteudbydere (både private og offentlige) vil kunne drage fordel af muligheden for 1-faktor-login, hvilket kan betyde, at der vil blive flere, der anvender NemID, hvilket vil gavne brugeroplevelsen.

Scenariet forudsætter, at der skal stilles krav om, at leverandøren understøtter de nuværende tekniske snitflader, så der også i dette scenarie opnås en høj grad af kontinuitet og bagudkompatibilitet.

Scenariet vil imødekomme flere af de mange krav og behov for forbedringer, der er indkommet i høringsfasen og i de fællesoffentlige parters arbejde med NemID, særligt fra virksomhedsområdet.

Samlet set betyder Scenarie 2 mere brugervenlige løsninger for borgere og erhvervsliv, både i form af mulighed for 1-faktor-login, bredere muligheder for at anvende NemID privat i erhvervssammenhæng og bedre og mere differentierede løsninger til administration af NemID i forbindelse med virksomheder og myndigheder og deres medarbejdere.

13.6.2 Samlet økonomi

Teknisk set kan et scenarie, der giver mulighed for 1-faktor-login og adskillelse af autentifikation og signering, bygge på en bredere vifte af tilgængelige løsninger i markedet. Det vil også være attraktivt for flere leverandører at byde. Samlet set kan det efter RMC-ICG's vurdering betyde, at der kan opnås større kvalitet, uden at det betyder øgede udgifter.

Hvor Scenarie 1 kun indebar fællesoffentlige udgifter til NemID, betyder Scenarie 2 i forskelligt omfang udgifter flere steder i det samlede NemID-økosystem.

Der vil være fællesoffentlige udgifter til løsningselement A til NemID-infrastruktur og drift *med flere sikringsniveauer samt adskillelse af autentifikation og signering* på niveau med Scenarie 1.

Hertil kommer udgifterne i løsningselement C til *bedre administrative løsninger* til virksomheder på samlet 10-20 millioner kroner, som desuden forventes at betyde en besparelse i udgifterne til support.

Udgifterne i løsningselement B *til bredere muligheder for at anvende NemID privat* ligger ikke i NemID, men i de tjenester, der skal etableres i Digitaliseringsstyrelsen, eventuelt i forbindelse med NemLog-in og/eller i Erhvervsstyrelsen. Udgifterne skønnes samlet at være 10-20 millioner kroner i kontraktperioden til udvikling og drift.

Desuden indebærer løsningselement B udgifter for en række tjenester, der skal gennemføre ændringer, for at NemID privat kan anvendes.

Den største usikkerhed knytter sig til de priser, som leverandørerne vil byde ind med, og aftaler om udgiftsfordeling med eventuelle partnere.

En anden usikkerhed knytter sig til antallet af tjenesteudbydere, der skal gennemføre ændringer for at give mulighed for bredere anvendelse af NemID privat til erhvervsformål.

Udgifterne til informationstjenester er en betingelse for at understøtte videre brug af NemID privat.

Derimod afhænger de samlede udgifter hos tjenesteudbydere af, om der fastlægges fælles krav til at understøtte NemID privat (det kan betyde større udgifter end nævnt), hvor mange udgifter tjenesterne reelt får, og hvor mange tjenester der vælger at understøtte dette.

13.6.3 Leverandørforhold

Et udbud af en løsning, der afviger fra den nuværende, vil gøre det mere attraktivt for andre leverandører end den nuværende leverandør, og et sådant udbud kan medføre, at flere leverandører vil finde det attraktivt at byde. Det har dermed betydning for konkurrencesituationen og i sidste ende for den samlede pris på løsningen. I skønnene ovenfor indgår det, at øget konkurrence og bedre mulighed for standardløsninger betyder, at der kan anskaffes mere funktionalitet i dette

scenarie til samme pris som Scenarie 1.

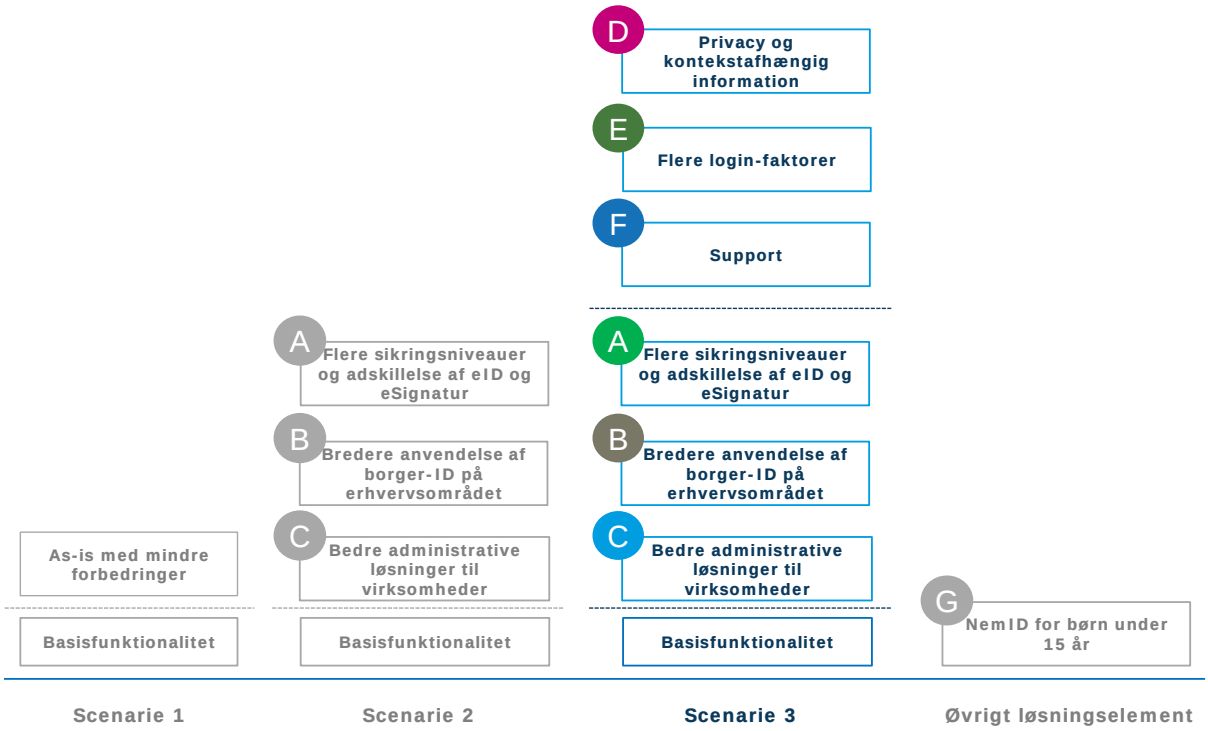
14. Scenarie 3

14.1 Præsentation af scenariet

Scenarie 3 er en udvidelse af Scenarie 2 med tre løsningselementer, jf. Figur 21.

- Privacy og kontekstafhængig information.
- Mulighed for flere login-faktorer.
- Bedre og billigere support.

Figur 21: Løsningselementer i Scenarie 3



De øvrige elementer i Scenarie 3 indeholder fortsat følgende:

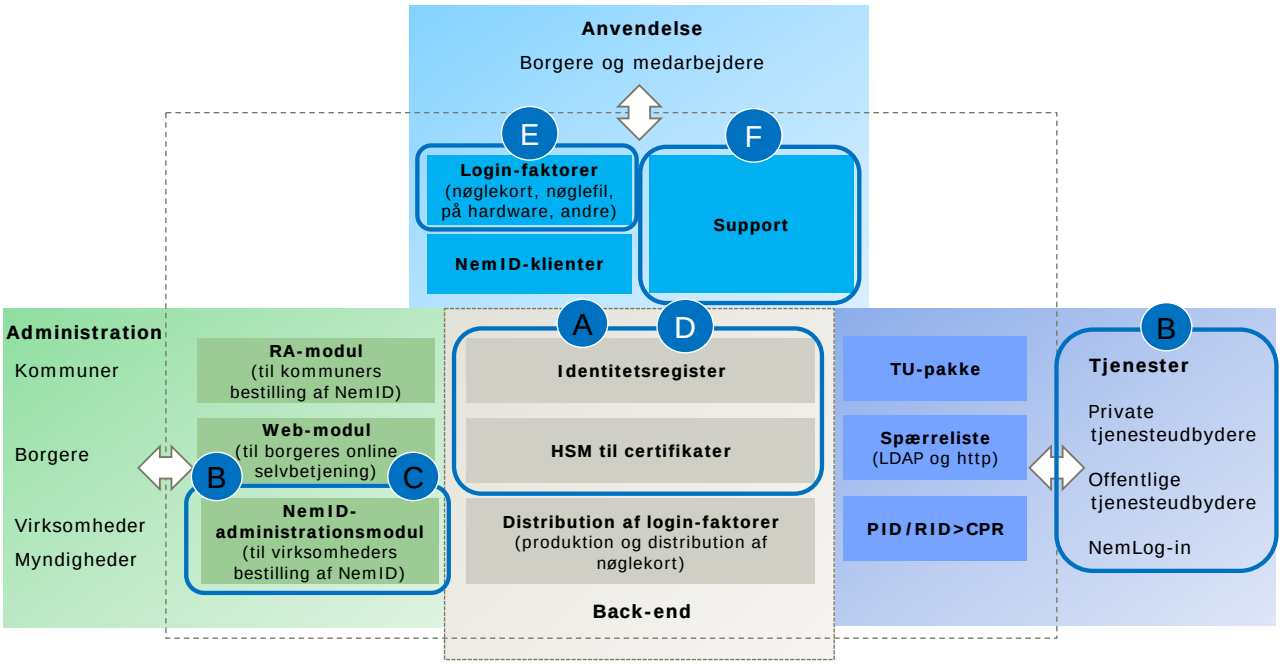
- Både 1-faktor-login og 2-faktor-login, sidstnævnte med kodeord og engangskode (fx nøglekort) til NemID privat og NemID medarbejdersignatur.
- I sammenhæng hermed adskilles eID og eSignering, og dermed er der ikke krav om, at løsningen baseres på PKI for eID-delen.
- En central lagring af privatnøgler hos leverandøren til signeringsdelen. Det er et krav, at brugeren oplever sammenhæng mellem login-løsning og signeringsløsning.
- Nøglefil til NemID til erhverv – herunder mulighed for decentralt at anvende signaturserverløsninger.
- Bedre erhvervsløsninger i form af udbredelse af NemID privat til erhvervsformål og bedre administrative løsninger til virksomheder.

Løsningens arkitektur bygger som Scenarie 2 på anvendelse af eID-teknologier til autentifikation og på en PKI-baseret arkitektur til signering.

I de følgende afsnit præsenteres, analyseres og vurderes de tre løsningselementer.

14.2 Funktioner i Scenarie 3

Figur 22: Funktioner i Scenarie 3



Scenarie 3 indeholder basisfunktionalitet, jf. afsnit 11 næste generation NemID. Derudover, som det fremstår af Figur 22, indeholder Scenarie 3 løsningselement A, B og C fra Scenarie 2. Desuden indeholder Scenarie 3 yderligere tre løsningselementer: D, E og F.

De tre løsningselementer i Scenarie 3 vedrører følgende af ovenstående funktioner:

Løsningselement D: Privacy og kontekstafhængig information vedrører NemID back-end.

Løsningselement E: Flere login-faktorer.

Løsningselement F: Bedre og billigere support.

Løsningselementerne D, E og F har ikke tekniske og funktionelle sammenhænge og kan implementeres uafhængigt af hinanden.

Løsningselementerne D og F kan implementeres i forbindelse med Scenarie 1.

Løsningselementer D og E vil være langt lettere og billigere at implementere med den arkitektur, der indgår i scenarierne 2 og 3, mens det med den nuværende arkitektur vil betyde meget store omkostninger.

14.3 Løsningselement D: Privacy og kontekstafhængig information

I dette afsnit præsenteres løsningselementet *privacy og kontekstafhængig information*. Herefter analyseres de overordnede potentielle forretningsmæssige gevinster. Dernæst foretages en vurdering af løsningselementet, og afsnittet afsluttes med en konklusion.

14.3.1 Præsentation

I den eksisterende løsning er borgere identificeret ved et såkaldt PID-nummer efter autentifikation. Dette PID-nummer er indkodet i brugerens certifikat. Offentlige myndigheder kan foretage et opslag via den såkaldte PID-tjeneste og herved finde borgerens CPR-nummer. Private tjenesteudbydere kan ikke foretage dette *direkte* opslag, men kan anmode brugeren om at angive CPR-nummer og via PID-tjenesten *verificere sammenhængen mellem* PID- og CPR-nummer.

Der findes en tilsvarende RID-tjeneste for medarbejdere, der har CPR tilknyttet deres medarbejdersignatur. Denne tjeneste er udelukkende tilgængelig for offentlige tjenesteudbydere.

Ud over PID/RID kan certifikatet indeholde brugerens navn og e-mail-adresse. For medarbejdersignaturer vil der desuden altid være angivet CVR-nummeret og virksomhedens navn.

I alle praktiske sammenhænge er den entydige identifikation af brugeren således reelt begrænset til PID/RID eller CPR. Både PID/RID og CPR er globale identifikatorer, der kan sammenkædes på tværs af tjenesteudbydere.

I sig selv kan NemID derfor siges at have et højt niveau af privacy.

Til gengæld medfører arkitekturen i det samlede NemID-økosystem bindinger på, hvor høj grad af privacy der kan understøttes, idet langt hovedparten af de offentlige digitale løsninger og en række private tjenester (forsikring, a-kasse, pension og kreditlångivere) benytter CPR som entydig identifikator af borgerne og trækker på data fra CPR.

En række øvrige private tjenesteudbyder har samtidig behov for helt andre data om brugerne. Således kan brugere i netbutikker være identificeret ved navn og adresse, mens man hos en udbyder af online-spil kan nøjes med at identificere brugeren som en person over 18 år, der ikke er registreret i "Register Over Frivilligt Udelukkede Spillere" (ROFUS). Tilsvarende findes der også digitale løsninger i offentligt regi, hvor man udelukkende har behov for at vide, om en given bruger er borger i en given kommune.

Der findes en række private tjenester, hvor der kun er behov for at genkende en tilbagevendende bruger og eventuelt sikre sig, at brugeren ikke i forhold til tjenesten kan skifte identifikator (ved behov for udelukkelse). Endelig vil visse tjenester have behov for, at efterforskningsmyndigheder kan finde den fysiske bruger i tilfælde af svig. Den Blå Avis med NemID-validering er et eksempel på en sådan tjeneste.

Ved adskillelse af autentifikation og signering er det muligt at udvide infrastrukturen med denne type funktionalitet samtidig med, at man overholder brugernes krav til privacy.

Løsningen kan implementeres således, at brugeren som udgangspunkt skal give informeret samtykke inden videregivelse af identificerende data og med mulighed for øget grad af pseudonymisering af brugeren. Løsningen kan også understøtte muligheden for, at en bruger kan forblive anonym over for tjenesteudbyderen, medmindre der opstår mistanke om kriminelle handlinger. Derudover kan infrastrukturen have indbygget mulighed for tjenesteudbyderspecifikke pseudonymer, så to tjenesteudbydere ikke kan sammenkæde identiteter på tværs af tjenester.

Identifikation med kontekstafhængig information kan være et væsentligt element i understøttelse af øgede krav (herunder EU-krav) om indtænkning af privatlivsbeskyttelse i digitale løsninger (privacy-by-design). Løsningselementet adresserer desuden ønsker til privatlivsbeskyttelse fra Forbrugerrådet og Rådet for Digital Sikkerhed.

Identifikation med kontekstafhængig information sammen med anvendelse af differentierede sikkerhedsniveauer kan øge værdien af infrastrukturen væsentligt for en række private tjenesteudbydere, der ikke anvender den eksisterende NemID-infrastruktur. I Fase 1 har blandt andet Dansk Industri, DANSK IT og FDIH givet udtryk for ønsker, der kan opfyldes med kontekstafhængig information. Således kan den øgede funktionalitet være med til at udvide anvendelsen af infrastrukturen til nye parter, der kan bidrage til finansieringen.

Det skal bemærkes, at løsningen ikke adresserer et eventuelt privacy-behov i forhold til, at broker kan afgøre, hvilken tjenesteudbyder en given bruger forsøger at tilgå.

Der er ikke fundet samme behov for identifikation med kontekstafhængig information i erhvervssegmentet.

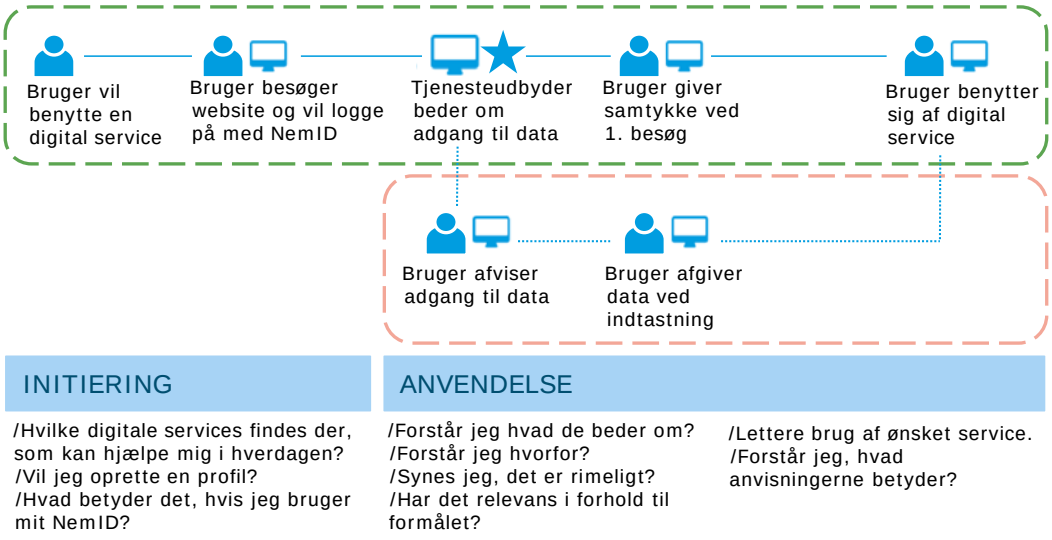
14.3.1.1 Brugervenlighed

Brugervenligheden vil ændres på den måde, at brugerne i visse tilfælde skal tage aktivt stilling til, om relevante personlige data må deles med den tjenesteudbyder, de er ved at logge ind hos.

Brugernes behov og forventninger ved disse data-transaktioner skal afdækkes, da kontekst og relevans har stor betydning for, om brugeren oplever en øget værdi eller det modsatte.

Nedenstående brugerrejse illustrerer brugerens forskellige berøringspunkter og overvejelser ved videregivelse af personlige oplysninger til tjenesteudbyder. Den grønne ramme indikerer den fremtidige løsning, når brugeren accepterer at videregive data, og den røde ramme er trin i brugerrejsen, der vil udgå, eller som brugeren vil møde, hvis de ikke accepterer at give tjenesteudbyder adgang til data.

Figur 23: Brugerrejse for videregivelse af relevante personlige data



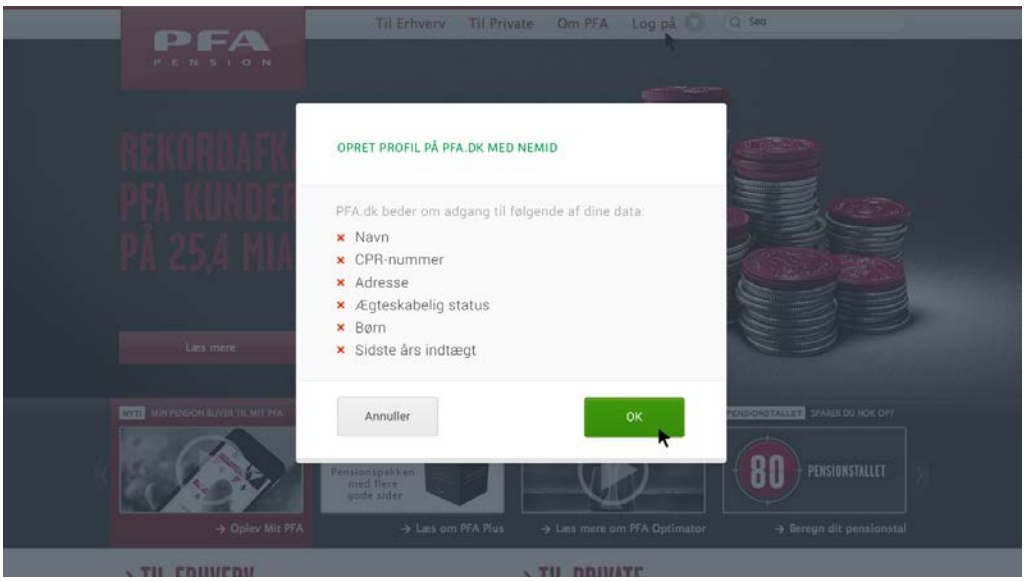
Fordele

I takt med udbredelsen af NemID vil brugerne have øget mulighed for at vælge tjenesteudbydere, der imødekommer den enkelte brugers behov. Løsningselementet giver mulighed for, at disse tjenesteudbydere i højere grad kan tilpasse løsningerne til deres målgruppes specifikke behov og dermed opnå større brugertilfredshed i den samlede brugeroplevelse.

Udfordringer

Brugergrænsefladen skal designes, så brugeren forstår og reelt kan tage stilling til datatransaktionen, herunder hvilke konsekvenser det har for brugeren, hvis de ikke videregiver data. Fase 1 viste, at borgere bekymrer sig om sikkerheden, når det vedrører egne personlige data og mulig spredning af disse. Denne bekymring skal imødekommes ved at lave løsninger, hvor brugeren let kan afkode, hvilke data der bliver anmodet om, og hvilken relevans data har i forhold til formålet.

Figur 24: Muligt grafisk design for videregivelse af personlige data



14.3.2 Gevinster

Dette afsnit har til formål at præsentere de gevinster, løsningselementet kan give. Gevinsterne differentieres i forhold til de forskellige relevante brugergrupper, som NemID opererer inden for.

14.3.2.1 Borgere

En løsning med identifikation ved brug af kontekstafhængig information vil understøtte en højere grad af fx rollebaseret adgangskontrol, hvor brugeren udelukkende er identificeret med rettighedsrelevant information, der er nødvendig i en given kontekst. Løsningen vil derfor understøtte behov hos brugergrupper, der efterspørger mere privacy. Desuden kan løsninger implementeres med fokus på at sætte brugeren i centrum ved at lade brugeren acceptere eller afslå, at den relevante information videregives til en tjenesteudbyder.

Desuden understøtter teknologien anvendelse af tjenesteudbyderspecifikke pseudonymer, der ikke kan linkes mellem forskellige tjenesteudbydere.

14.3.2.2 Tjenesteudbydere – offentlige og private

Tjenesteudbydere får mulighed for at identificere brugere med information, der er mere relevant. I modsætning til den eksisterende løsning vil det eksempelvis betyde, at tjenesteudbyderen kan få adgang til en verificeret adresse uden at skulle kende brugerens CPR-nummer.

Det er primært private tjenesteudbydere, der har efterspurgt denne type funktionalitet, men der er desuden en række offentlige tjenester, der med fordel kan anvende kontekstafhængig identifikation. Der vil givetvis være en række kommunale løsninger, hvor det kun er nødvendigt at vide, at en bruger er bosiddende i kommunen. Leverandører af digitale løsninger inden for renovationsområdet har givet udtryk for, at verificerede adresseoplysninger er tilstrækkelig information for at kunne servicere borgerne.

14.3.3 Vurdering

Dette afsnit har til formål at analysere og vurdere løsningselementet i forhold til relevante parametre.

14.3.3.1 Arkitektur

Identifikation ved anvendelse af kontekstafhængig information understøttes af en arkitektur med en identitetsgarant og en broker.

Der findes en række åbne standarder til autentifikation, hvor brugeren identificeres med kontekstafhængig information. Af disse tegner SAML 2.0 og OpenID Connect sig til at blive markedsledende i de kommende år. Sidstnævnte er designet til ”at gøre simple ting simple og komplekse ting mulige”. Der findes allerede Open Source moduler til en række platforme (herunder Apache og Drupal), der kan hjælpe tjenesteudbydere med at reducere etablerings- og vedligeholdelsesudgifterne.

Identitetsudbyderen (identitetsgaranten eller brokeren) skal udstille en eller flere grænseflader over for tjenesteudbyderne. Dette sker allerede i NemLog-in, der udstiller et SAML 2.0 interface.

Tjenesteudbyderen skal ligeledes implementere håndtering af identifikation med kontekstafhængig information. Det må forventes, at private tjenesteudbydere fremadrettet vil foretrække OpenID Connect som interface i takt med, at dette interface får større understøttelse.

14.3.3.2 Sikkerhed og privacy

Anvendelse af kontekstafhængig information kan øge den samlede sikkerhed for NemID-økosystemet i forhold til at sammenkæde en digital identitet til et CPR-nummer. En forøgelse af sikkerheden forudsætter, at tjenesteudbyderne gennemfører tiltag for at øge sikkerhed og privacy.

Hvis tjenesteudbydere ikke har data, der kan koble brugere på tværs af systemer, vil den samlede sikkerhed for brugeren være større. Dette gør sig naturligvis kun gældende i systemer, hvor man ikke har behov for at databehandle på baggrund af CPR-nummer.

I forhold til privatlivsbeskyttelse har kontekstafhængig information primært relevans i borgersegmentet. Dog er der i forhold til erhvervssegmentet særlige privacy-problemstillinger i forbindelse med CPR-tilknytning til medarbejdersignatur og ved en øget anvendelse af private identiteter til erhvervsløsninger.

14.3.3.3 Migrering

Hovedparten af de eksisterende tjenesteudbydere, der har taget NemID i brug (både offentlige og private), har behov for at behandle data med brug af CPR. Disse vil kunne fortsætte med de eksisterende interfaces. Men visse private tjenesteudbydere kan med fordel vælge at skifte til anvendelse af kontekstafhængig information, da brugeren således ikke skal indtaste CPR-nummer med henblik på PID/CPR-verifikation, men udelukkende acceptere videregivelse af CPR-nummer eller anden relevant information fra identitetsudbyderen til tjenesteudbyderen.

14.3.3.4 Relation i forhold til private partnere

Der er ingen særlige problemstillinger i forhold til private partnere. Disse kan dog som tjenesteudbydere også drage nytte af den øgede funktionalitet.

14.3.3.5 OCES-certifikatpolitikker

Kontekstafhængig information bør ikke implementeres i form af certifikatteknologi. Dermed vil OCES-certifikatpolitikkerne ikke være påvirket af den øgede funktionalitet. Det kan blive relevant at lave politikker for anvendelse af kontekstafhængig information.

14.3.3.6 Økonomi

Understøttelse af kontekstafhængig information og øget privacy vil ikke føre til øgede fællesoffentlige udgifter i NemID, men derimod i andre dele af økosystemet.

I det følgende antages det, at løsningen er opdelt med en identitetsgarant og en broker (logintjeneste). Desuden antages det, at brokeren udstiller et standardiseret interface mod tjenesteudbydere. En oplagt kandidat for et interface vil være OpenID Connect.

Derudover bør NemLog-in videreføre understøttelse af SAML 2.0, der i store træk anvendes til at give samme funktionalitet og allerede anvendes bredt blandt offentlige tjenesteudbydere.

Da det antages, at det inden for en kort tidshorisont vil blive væsentligt billigere at implementere OpenID Connect, eksempelvis gennem standardmoduler, vil de samlede udgifter for de private tjenesteudbydere kunne minimeres. Udgifterne ved implementering vil variere for tjenesteudbyderne, afhængig af deres størrelse og karakter, men det skønnes, at etableringsudgifterne vil ligge mellem 50.000 kroner og 500.000 kroner med et tilsvarende beløb for vedligehold og drift over en 5-årig periode.

Udgifterne skal ses i forhold til de besparelser, tjenesterne opnår ved at anvende NemID i stedet for egen brugerstyringsløsning. Da hver enkelt tjeneste vil implementere løsningen efter en vurdering af gevinsterne i forhold til udgifterne, indregnes tjenesteudbydernes udgifter til etablering og deres gevinster ved ikke at skulle etablere egen brugerstyringsløsning ikke.

Da det er broker, der udstiller interface for kontekstafhængig identifikation, vil der ikke være fællesoffentlige udgifter for NemID ved etablering og drift.

Det forventes, at udgifter til etablering af et interface for kontekstafhængig identifikation for en broker vil omfatte etablering af interfaces til tjenester med relevant information (CPR, ROFUS) samt et interface til tjenesteudbyderne. De samlede udgifter vil afhænge af antallet af interfaces og prisen på de enkelte interfaces. Hertil kan komme udgifter til informationsleverandøren, som dog ikke indgår i nedenstående udgifter, da offentlige grunddata generelt stilles gratis til rådighed. Med en gennemsnitlig pris på 200.000 kroner pr. interface og gennemsnitligt fem interfaces vil den samlede etableringspris være 1 millioner kroner pr. broker.

Der vil være yderligere udgifter til brokerens system og til tilpasning af interfaces mod tjenester. Disse skønnes at være på 1-3 millioner kroner pr. broker.

De samlede etableringsudgifter vil således være 2-4 millioner kroner pr. broker og et tilsvarende beløb for drift og vedligehold over fem år.

Hvis en 1-faktorbaseret autentifikation med kontekstafhængig identifikation har en værdi på 5 øre pr. transaktion, vil en ekstra pulje på 200-400 millioner transaktioner over en femårig periode finansiere udgiften til broker-delen. Dette er i gennemsnit 40-80 millioner årlige transaktioner, hvilket ikke vurderes urealistisk. JUST EAT oplyser på deres hjemmeside, at de har over 10 millioner årlige bestillinger, og ifølge FDIM har BilletNet og Billetlugen samlet i størrelsesordenen 5 millioner unikke pc-brugere om året.

14.3.3.7 Finansieringsmodeller

RMC-ICG vurderer, at denne funktionalitet vil have så meget værdi for private tjenesteudbydere, at der vil være villighed til, at tjenesten kan finansieres på markedsvilkår.

Som det fremgår af økonomiafsnittet, kan denne funktionalitet sammen med understøttelse af flere sikkerhedsniveauer betyde et samlet større finansieringsgrundlag og dermed nedbringe det offentliges andel af udgifterne.

14.3.3.8 Leverandørstrategi

Et udbud af en løsning, der afviger fra den nuværende, vil gøre det mere attraktivt for andre leverandører end den nuværende leverandør, og et sådant udbud kan medføre, at flere leverandører vil finde det attraktivt at byde. Det har dermed betydning for konkurrencesituationen og i sidste ende for den samlede pris på løsningen.

14.3.3.9 Risici

Der er en økonomisk risiko for, at værdien af funktionaliteten ikke overstiger de udgifter, der pålægges tjenesteudbyderne.

I forhold til anvendelsen er der risiko for, at visse tjenesteudbydere misbruger løsningen og anmoder om langt flere personlige informationer om brugeren, end der er behov for i den givne kontekst.

Samtidig er der risiko for, at brugerne ikke forstår brugergrænsefladen og blot laver 'click-through' uden at vurdere, hvilke data der videregives.

14.3.3.10 Juridiske problemstillinger

Ingen særlige juridiske problemstillinger.

14.3.3.11 Styringsmæssige problemstillinger

Ingen særlige styringsmæssige problemstillinger.

14.3.4 Samlet vurdering for løsningselementet

Udvidelse af løsningen til at understøtte identifikation med kontekstafhængig information vil:

- Øge mulighed for at udvikle privacy-venlige løsninger.
- Stille efterspurgt funktionalitet til rådighed.
- Potentielt bidrage til større finansiereringsgrundlag for NemID-økosystemet og dermed mindske det offentliges andel af udgifterne.

Tabel 17: Opsummering af RMC-ICG's vurdering af løsningselement D

Vurderingsparametre	RMC-ICG's vurdering
Arkitektur	Understøtter en arkitektur med identitetsgarant og broker. Der findes åbne, standardiserede markedsstandarder for interfaces mellem broker og tjenesteudbyder.
Sikkerhed og privacy	Teknologi åbner mulighed for god privacy-håndtering hos tjenesteudbyder. Dette gælder særligt for tjenesteudbydere, der ikke identificerer brugere ved CPR, og dermed særligt private tjenesteudbydere.
Migrering	Eksisterende tjenesteudbydere kan fortsætte med anvendelse af eksisterende interfaces eller vælge at skifte til nye interfaces til autentifikation. Nye tjenesteudbydere kan med fordel anvende nye interfaces.
Relation i forhold til private partnere	Ingen særlige problemstillinger.
OCES-certifikatpolitikker	Ingen særlig påvirkning.
Økonomi	Kontekstafhængig information kan bidrage positivt til finansieringen af broker-delen af infrastrukturen.
Finansieringsmodeller	Kan finansiereres af tjenesteudbydere.
Leverandørstrategi	Understøtter flere leverandører.
Risici	Udgifter for tjenesteudbyder overstiger værdien for tjenesteudbyder. Manglende fokus på privacy fra tjenesteudbyder og brugere. Kan give dårligere brugeroplevelse og udfordringer for nogle brugergrupper.
Juridiske problemstillinger	Ingen juridiske problemstillinger.
Styringsmæssige problemstillinger	Ingen styringsmæssige problemstillinger.

14.4 Løsningselement E: Flere login-faktorer

I dette afsnit præsenteres løsningselementet *flere login-faktorer*. Herefter analyseres de overordnede potentielle forretningsmæssige gevinster, som RMC-ICG vurderer, at løsningselementet kan give. Dernæst foretages en vurdering af løsningselementet, og afsnittet afsluttes med en konklusion.

14.4.1 Præsentation

Den grundlæggende løsning skal som i den eksisterende løsning have en række generelle egenskaber:

- Løsningen skal have størst mulig uafhængighed af teknologi. Eksempelvis bør der ikke stilles krav om USB/Bluetooth/fingeraftrykslæser/kamera eller lignende.
- Løsningen skal i størst mulig omfang kunne anvendes på flere klienter, uden at brugeren skal eksportere og importere data.
- Løsningen skal have varianter, der understøtter svagtseende, blinde og øvrige med nedsat funktionsevne.

Understøttelse af disse egenskaber vil naturligt begrænse mulighederne for at udvikle løsninger, der er tilpasset og udnytter særlige teknologier, der i særlige brugssituationer vil give merværdi for brugeren. Som et eksempel blandt mange kunne dette være en PC-baseret autentifikationsløsning, hvor nøglekortet er erstattet af et USB-baseret hardware-token, hvor indtastning af tal fra

nøglekort er erstattet af et tryk på en knap på token'et. Ligeledes kan man forestille sig løsninger, der er direkte tilrettet anvendelse på mobile platforme og måske endda eksklusivt for bestemte operativsystemer.

RMC-ICG anbefaler, at løsningen designes, så der tilbydes en grundlæggende funktionalitet med varianter, så alle borgere og medarbejdere i virksomheder og myndigheder har mulighed for at anvende NemID. Dette svarer til NemID-nøglekortsløsningen og NemID-nøglefilsløsningen suppleret med nøglekort til blinde (*voice response*) og nøglekort med stor skrift.

RMC-ICG anbefaler desuden, at løsningen designes, så leverandøren eller andre på markedet kan suppleres med alternative login-faktorer, tilpasset særlige brugerbehov. Dette kan enten ske ved integration i leverandørens back-end eller ved etablering af en alternativ NemID-identitetsgarant. Det skal tilstræbes, at der ikke skabes unødvendige forretningsmæssige eller tekniske barrierer for introduktion af alternative login-faktorer, der kan give værdi for selv mindre brugergrupper. Løsningen bør eksempelvis åbne mulighed for, at en bruger kan anvende eksisterende NemID i forbindelse med elektronisk registrering til en alternativ løsning.

RMC-ICG vurderer, at kun meget få borgere vil være villige til at betale for supplerende login-faktorer, men det kan ændres over tid – særligt hvis der udvikles en sikker løsning, baseret på smartphone-teknologi. Det må forventes, at der på erhvervsområdet fortsat vil være stort behov for kustomiserede løsninger, der er tilpasset den enkelte organisations behov. Dette gælder særligt for større organisationer.

14.4.1.1 Brugervenlighed

Brugervenligheden vil ændres i den forstand, at valgfriheden omkring valg af login-faktor udvides med flere løsninger. Ved anskaffelsen af NemID eller udskiftning af en eksisterende login-faktor (eksempelvis nøglekort) vil brugeren skulle tage stilling til forskellige løsninger, forstå hvad de indebærer og vurdere, hvilken løsning der passer til personens individuelle behov.

I Fase 1 blev borgere præsenteret for konceptet omkring en mobil kodegenerator. Af sikkerhedsmæssige årsager vil en smartphone og app-software som login-faktor ikke være det foretrukne bud på en løsning, men afprøvningen af konceptet viste, at brugerne tog positivt imod at kunne vælge alternative måder at skaffe engangskoder på.

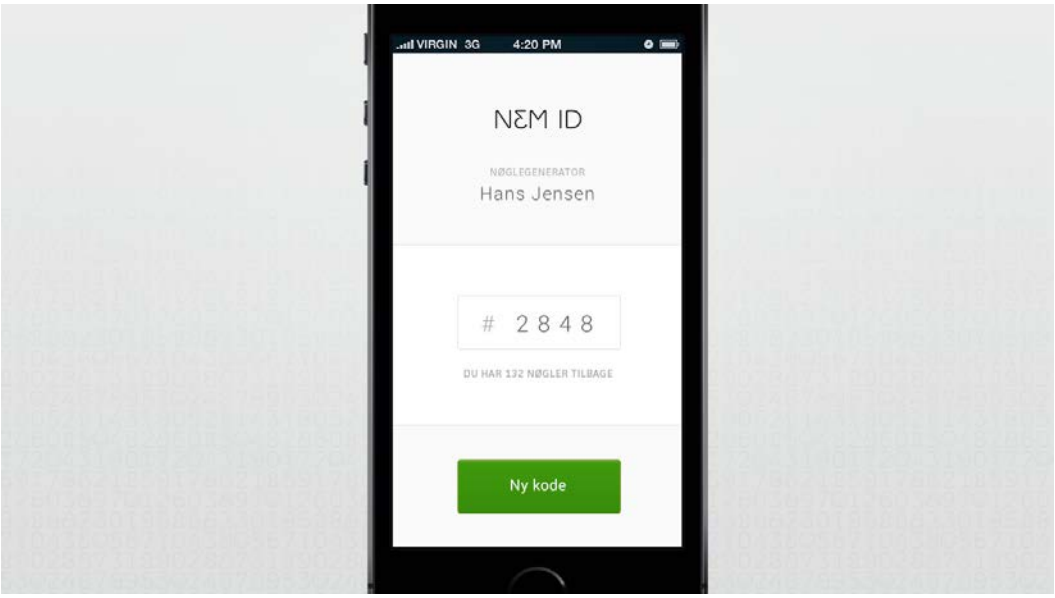
Fordele

Flere login-faktorer vil kunne dække flere brugeres behov og ønsker og på den måde give oplevelsen af, at NemID er let at anvende. Den enkelte bruger bliver i højere grad medbestemmende i en løsning, der for mange opfattes som obligatorisk. Nøglekortet har af nogle interessenter været udskældt, hvor Fase 1 fx viste, at der er borgere, som betragter kortet som et nødvendigt onde. Andre interessenter har rost nøglekortet som forholdsvist enkelt og let at forstå. Alternative login-faktorer vil derfor give den enkelte bruger mulighed for at forme deres brug af NemID på den måde, der giver mest værdi.

Udfordringer

Man må forvente, at brugergrænsefladen i forbindelse med valg af login-faktor vil have øget kompleksitet, idet der præsenteres flere valgmuligheder end i eksisterende løsning. Valgmulighederne har hver især styrker og svagheder, som brugeren skal vurdere i forhold til deres egne individuelle behov. Anvendes principperne i brugercentreret design, vil brugervenligheden sikres i forhold til formidlingen og placeringen af valgmulighederne.

Figur 25: Muligt grafisk design til en kodegenerator-app til smartphones



14.4.2 Gevinster

Både borgere og virksomheder vil have mulighed for at tilvælge en eller flere løsninger, der passer ind i konkrete anvendelsesscenarier. Det betyder mulighed for udvikling af en mere dynamisk infrastruktur og øget brugertilfredshed.

14.4.3 Vurdering

Dette afsnit har til formål at analysere og vurdere løsningselementet i forhold til relevante parametre.

14.4.3.1 Arkitektur

Med et øget antal tjenesteudbydere vil omkostningerne ved introduktionen af nye login-faktorer øges tilsvarende, hvis der skal foretages integration hos hver enkelt tjenesteudbyder. Tjenesteudbydere må formodes at foretage en forretningsmæssig vurdering, der betyder, at login-faktorer, der udelukkende bliver benyttet af en lille brugergruppe, ikke vil blive understøttet. Som eksempel er det stort set kun NemLog-in, som understøtter den såkaldte NemID på hardware-delen i den eksisterende løsning.

Ved anvendelse af brokere vil introduktion af nye login-faktorer have en langt højere grad af transparens i forhold til de enkelte tjenesteudbydere, der derfor ikke har direkte omkostninger til integration.

14.4.3.2 Sikkerhed og privacy

Det er væsentligt for den samlede sikkerhed og dermed tilliden til infrastrukturen, at alle tilbudte løsninger på markedet har et ensartet og højt sikkerhedsniveau. RMC-ICG anbefaler, at der formuleres en række objektive krav til login-faktorer gennem et samlet trust framework, og at der eventuelt etableres en akkrediteringsordning, hvor eID-løsninger bliver ”NemID-godkendt”. Det er oplagt, at løsninger, der i andre EU-medlemsstater godkendes som *kvalificerede elektroniske signaturgenereringssystemer*, automatisk godkendes i et dansk trust framework.

14.4.3.3 Migrering

Hvis der introduceres krav om anvendelse af brokere, vil en række private tjenesteudbydere skulle tilpasse deres løsninger. Udgifterne vil kunne begrænses ved at tilpasse TU-pakken.

Offentlige tjenester, der anvender NemLog-in, vil ikke være påvirket.

14.4.3.4 Relation i forhold til private partnere

Private partnere skal acceptere et fælles trust framework og de tilhørende objektive kriterier for godkendelse i stedet for en vurdering af hver enkelt teknologisk implementering af login-faktorer.

14.4.3.5 OCES-certifikatpolitikker

Beskrivelse af sikkerhedsniveau, inklusive krav til login-faktorer, bør fastlægges i et trust framework. Det må antages, at en lang række krav til registrering og anvendelse allerede findes i de eksisterende OCES-certifikationspolitikker. RMC-ICG vurderer, at disse informationer med fordel kan flyttes fra OCES-certifikationspolitikker til politikker for eID i et trust framework, hvorefter OCES-certifikationspolitikkerne fremadrettet henviser til trust frameworket i forhold til anvendelse af login-faktorer i forbindelse med signering.

14.4.3.6 Økonomi

Udgifter i back-end til flere login-faktorer vil være fællesoffentlige, såfremt det vælges at lade NemID-leverandøren stå for opgaven. Alternativt kan opgaven løses af andre i økosystemet, fx ved at de tilbyder login-faktorer mod betaling.

Udgifter til supplerende løsninger til login-faktorer afhænger meget af den valgte løsning. Introduktion af en særlig hardware-token vil eksempelvis typisk være dyrere i anskaffelse og distribution end en løsning, der anvender elementer, som brugeren allerede er i besiddelse af (fx mobiltelefon).

Udgifter til back-end-implementering hos identitetsgaranten skønnes til at være 10-20 millioner kroner og inkluderer udgifter til at opnå akkreditering. Udgifter til vedligehold og drift skønnes tilsvarende at være 10-20 millioner kroner over fem år.

Der kan opstå behov for support i forbindelse med flere login-faktorer, afhængigt af den konkrete løsning.

Hvis en supplerende leverandør som identitetsgarant ønsker at tilbyde markedet en alternativ løsning, hvor brugeren registreres elektronisk ved brug af NemID fra den grundlæggende infrastruktur, vil registrering af brugere højst beløbe sig til 1,01 kroner (med de nuværende priser) pr. bruger, svarende til en login- eller signeringstransaktion. Hvis brugeren allerede er digitalt registeret hos identitetsgaranten med eksisterende login-faktor, bortfalder denne udgift.

De enkelte brokere/login-tjenester skønnes hver at have udgifter til implementering på 500.000 kroner og et tilsvarende beløb for drift og vedligehold over fem år.

Der vil ikke være udgifter hos tjenesteudbydere, da funktionaliteten er afskærmet gennem brokere/login-tjenesterne.

Det vil først være muligt at lave en beregning af udgifterne, når der er valgt login-faktor.

14.4.3.7 Finansieringsmodeller

Flere login-faktorer kan finansieres af det offentlige og eventuelt via sponsorer, der ønsker at stille en løsning til rådighed for egne kunder eller ved brugerbetaling.

Udgifter til eventuel hardware og forsendelse kan pålægges brugerne.

14.4.3.8 Leverandørstrategi

Kan leveres af NemID-leverandøren eller af andre, jf. mulighed for afledte identiteter.

14.4.3.9 Risici

Der vil være risiko for, at der ikke opstår et marked.

14.4.3.10 Juridiske problemstillinger

Der er ingen særlige juridiske problemstillinger ved understøttelse af flere login-faktorer.

14.4.3.11 Styringsmæssige problemstillinger

Hvis der er flere leverandører, skal der være styring af standarder og eventuelt godkendelser via et fastlagt trust framework.

14.4.4 Samlet vurdering for løsningselementet

Login-faktorer i form af fx nøglekort er meget væsentlig for brugernes oplevelse af NemID, og en bredere vifte af tilbud vil tilfredsstille mange brugere og kunne dække deres meget forskellige behov.

På den anden siden kan valgmuligheder betyde ulemper for nogle brugergrupper.

Indførelse af flere login-faktorer betyder udgifter til udvikling og anskaffelse af faktoren og eventuel tilpasning af brugergrænseflader både i NemID og i tjenester. Disse udgifter skal finansieres, og erfaringerne med brugerbetaling viser, at efterspørgslen efter login-faktorer, der kræver betaling, er begrænset.

Tabel 18: Opsummering af RMC-ICG's vurdering af løsningselement E

Vurderingsparametre	RMC-ICG's vurdering
Arkitektur	Implementeres nemmest og billigst med en adskillelse af identitetsgarant og broker (login-tjeneste).
Sikkerhed og privacy	Akkrediteringsordning og automatisk accept af sikre signaturgenereringssystemer godkendt i andre EU-medlemsstater som en del af et trust framework.
Migrering	Understøttelse af nye login-faktorer kræver integration, der nemmest implementeres ved anvendelse af en broker-funktion.
Relation i forhold til private partnere	Generel accept af et trust framework og akkrediteringskriterier.
OCES-certifikatpolitikker	Krav til login-faktorer bør flyttes til et trust framework.
Økonomi	Afhænger af de konkrete implementeringer. Anvendelse af broker afskærmer for direkte udgifter for tjenesteudbydere.
Finansieringsmodeller	Kan være offentligt finansieret, finansieret af private sponsorer eller brugerfinansieret.
Leverandørstrategi	Kan leveres af forskellige leverandører på markedsvilkår.
Risici	Det danske marked er for lille.
Juridiske problemstillinger	Ingen juridiske problemstillinger.
Styringsmæssige problemstillinger	Opbygning af en akkrediteringsordning.

14.5 Løsningselement F: Bedre og billigere support

God support er væsentligt for at opretholde eller etablere en positiv opfattelse af en løsning. Behovet for support opstår, når brugeren er forhindret i at gennemføre en opgave i en brugergrænseflade. Den gode support kan fjerne forhindringen samt øge brugerens tilfredshed. Er det omvendte tilfældet, kan dårlig support gøre situationen værre.

I Fase 1 var det tydeligt, at brugerne, især gruppen af erhvervsbrugere og offentligt ansatte, var meget utilfredse med den tilgængelige support på erhvervsområdet.

I dette afsnit præsenteres løsningselementet. Herefter analyseres de overordnede potentielle forretningsmæssige gevinster, som RMC-ICG vurderer, at løsningselementet kan tilvejebringe. Dernæst foretages en vurdering af løsningselementet, og afsnittet afsluttes med en konklusion.

14.5.1 Præsentation

Når NemID bliver mere kompleks med adskillelse af autentifikation og signering, flere sikkerhedsniveauer, flere login-faktorer og flere leverandører vil brugerne stille større krav til support. Det vil betyde en stigning i supporthenvendelser.

Brugernes krav til den kommende NemID-løsning er, at supporten bliver bedre. For de fællesoffentlige parter er det vigtigt, at behovet for support kan mindskes og dermed bliver billigere. Det skal ske samtidig med, at der skal opnås større brugertilfredshed.

Dette gælder både support for borgere og i endnu højere grad support for NemID til erhverv.

Løsningselementet "Bedre og billigere support" indeholder således forslag til optimering af supportydelsen. Det omfatter både dens kvalitet og udgiftsniveau, og det skal opnås gennem en række tiltag, der blandt andet omfatter bedre betalingsvilkår og reducerede priser for erhvervssupport. Der skal være mere sammenhængende support fra serviceudbydere, bedre online-supportmuligheder og udnyttelse af elektroniske kanaler. Der skal stilles krav om øget brugervenlighed særligt i forhold til NemID til erhverv, og der skal være større kontraktmæssige incitamenter.

14.5.1.1 Bedre kvalitet af erhvervssupport

Erhvervskunder har ikke kun store forventninger til løsningens funktionalitet, store brugervenlighed og fejlfrie drift, men også til kvaliteten af den ydede support samt håndteringen af fejl og supporthenvendelser.

Der efterspørges i den forbindelse en højere kvalitet af erhvervssupporten, også i forhold til henvendelser til andet og tredje *support-level*. Specifikt ønsker regionerne en direkte adgang til tredje level support i forhold til NemID til erhverv.

Kvalitetsløft skal omfatte både supportmedarbejdernes kompetencer og de implementerede supportprocesser som fx indberetning og registrering. Der skal være muligheder for prioritering og eskalering, opfølgningsmuligheder og tilbagerapportering, som forventes at bygge på best practice i branchen.

14.5.1.2 Bedre betalingsvilkår for erhvervssupport

Bedre support for NemID skal omfatte bedre betalingsvilkår for virksomheder. NemID til erhverv kritiseres specifikt for prisen pr. henvendelse på 250 kroner. Denne pris forlanges, uanset om det drejer sig om en henvendelse via telefon, mail eller chat. Alternativt kan virksomhederne tegne en supportaftale.

Denne flat rate-model er baseret på gennemsnitligt tidsforbrug, dvs. uden differentiering i forhold til ressourceanvendelse. Modellen er derfor meget leverandørvenlig og bidrager ikke til større tilfredshed hos brugerne. Samtidig kan det argumenteres, at denne faste pris er sat relativt højt. Det foreslås i denne sammenhæng, at support for medarbejdersignaturer opdeles i veldefinerede pakker, hvor det er klart specificeret, hvad virksomheder betaler for. Samtidig anbefales det, at der etableres en differentiering af priser, fx i relation til, hvilket overordnet problem henvendelsen drejer sig om, typen af henvendelsen, antallet af medarbejdersignaturer, som virksomheden har, osv.

14.5.1.3 Reducerede priser for erhvervssupport

Prisen pr. henvendelse til erhvervssupport i den nuværende version af NemID er på 250 kroner for de virksomheder, der ikke har tegnet en supportaftale med NemID.

Gratis henvendelse til erhvervssupport omfatter alene følgende situationer:

1. Hvis man ikke har modtaget velkomst-e-mail, et brev med adgangskode eller nøglekort inden for den oplyste tid.
2. Hvis man har glemt sit bruger-id.
3. Hvis man som administrator har mistet sin nøglefil, glemt adgangskode eller ikke har fået fornyet sin medarbejdersignatur.

4. Henvendelsen skyldes en fejl i de underliggende systemer hos Nets.

De forholdsvis høje supportudgifter bidrager væsentligt til utilfredshed med løsningen til NemID til erhverv, hvor betaling for support opfattes som en tvungen udgift, der påføres virksomheden af det offentlige. Argumentationen er, at myndighedernes digitale tjenester er obligatoriske, og når man skal betale for at kunne anvende dem (blot fordi tjenesterne eller en del af dem, som det offentlige har et ansvar for, ikke er brugervenlige nok), er der tale om ekstraudgifter, som ikke kan fravælges af virksomheden.

Det er derfor vurderingen, at en kraftig prisreduktion (eller eventuelt et frikøb) af erhvervssupport vil have en positiv indflydelse på brugertilfredsheden, både med selve NemID til erhverv og med de offentlige (og private) tjenester, der benytter erhvervssupport.

14.5.1.4 Mere sammenhængende vejledning og support

Reaktionerne fra brugerne peger på behov for, at man fjerner den meget skarpe adskillelse mellem vejledning og support til NemID (og til NemLog-in) og support til tjenester, som anvender NemID/NemLog-in-infrastruktur. Denne fragmentering af vejlednings- og supportopgaven, bidrager til den negative opfattelse af NemID som et nødvendigt onde hos brugere. Samtidig mindsker den skarpe adskillelse mellem support til NemID og support til tjenester tjenesteudbydernes opmærksomhed og fokus fra den samlede løsning, som den opleves af brugerne. Det foreslåede arkitekturgrundlag med indførelsen af broker-funktionen kan føre til yderligere fragmenteringen af supportopgaven.

Virksomhederne (og borgerne) har behov for en sammenhængende og kontekstnær vejledning og support. NemID skal således i højere grad betragtes som del af de udbudte tjenester, bl.a. med integrerede bestillingsmuligheder og dertilhørende ansvar for vejledning og support af brugere i de offentlige tjenester. Denne tankegang forudsætter naturligvis, at supportleverandøren stiller en relevant 'vejlednings-/supportpakke' til rådighed for tjenesteudbydere.

Tilsvarende anbefales det, at offentlige tjenester som Virk.dk, SKAT samt domænespecifikke tjenester vil være med til at løfte vejlednings- og supportopgaven for medarbejdersignaturer.

Bedre borger- og virksomhedssupport kan omfatte *fælles* vejledning og support for flere offentlige digitale løsninger som fx NemID, NemLog-in, Digital Post og andre tjenester, dvs. udbredelse af en mere effektiv supportmodel, som kommunerne p.t. leverer i borgerservice.

14.5.1.5 Bedre online-supportmuligheder

De eksisterende supportstatistikker viser tydelige forskelle i henvendelsesmønstret for medarbejdere og borgere. Omkring 85 % af alle realiserede henvendelser vedrørende medarbejdersignaturer foregår via telefon. De resterende henvendelser er fordelt mellem 11 % for mail og 4 % for chat. For henvendelser fra borgerne er tilsvarende tal: 65 % af henvendelserne sker telefonisk, 20 % via mail og 15 % via chat.

En større andel af telefoniske henvendelser inden for virksomhedsområdet skyldes muligvis forskellige behov og forskelligt adfærdsmønster i forhold til borgere. Spørgsmål og problemer vedrørende medarbejdersignaturer og deres administration skal helst besvares og løses med det samme. Desværre mister man cirka 60 % af alle telefonopkald (cirka 70 % for borgere). Dette svarer til omkring 1.800 mistede telefonopkald pr. dag[10].

Disse tal understreger behovet for at undersøge potentialer ved at håndtere brugerne på en anden måde end nu. Dette betyder også, at der i højere grad skal skelnes mellem forskellige brugergrupper.

[10] Det er dog her ikke muligt at sondre mellem situationer, hvor brugeren ikke kunne komme igennem eller blot har lagt på, og hvor han/hun faktisk har fået besvaret sin henvendelse gennem *Integrated Voice Response*-funktion (IVR).

RMC-ICG anbefaler, at supportfunktionen for den kommende NemID-løsning i højere grad bygger på online-support som primær kommunikationskanal. Det kan fx ske ved at opprioritere chatfunktionen for på den måde at minimere ubesvarede henvendelser. Det kan ske ved at forbedre online-vejledninger, der i højere grad skal tage udgangspunkt i brugssituationen og ved at stille online-diagnoseværktøjer til rådighed for brugerne. Endelig kan der igangsættes en målrettet kommunikationsindsats for at flytte brugerne til at anvende online-supportmuligheder.

RMC-ICG anbefaler endvidere, at den fremtidige kontrakt og kravspecifikation definerer præcise målsætninger i forbindelse med supportydelsen (såsom svartidsgarantier, antal af besvarede henvendelser, max. antal af 'droppede' telefonhenvendelser m.m.). Udbudsmaterialet bør også stille meget konkrete krav om udformning af supportværktøjer i form af fx e-læringsmateriale, online-vejledninger m.m., der skal kunne anvendes både af brugerne og i supportøjemed. Disse produkter skal være en del af den samlede leverance (i form af en supportpakke) og skal kunne anvendes af andre end hoved- eller supportleverandøren, fx af tjenesteudbyderne. Endelig kan der i kontrakten indbygges incitamenter, der understøtter den ønskede udvikling i supportydelserne.

14.5.1.6 Kontraktmæssige incitamenter

RMC-ICG anbefaler, at der skabes nogle direkte kontraktmæssige incitamenter, der skal bidrage til minimering af supportbehovene og udgifterne. De fællesoffentlige udgifter for perioden 2018-2022 estimeres, med udgangspunkt i de nuværende supportbehov, til at udgøre cirka 125 millioner kroner.

Incitamenterne kan blandt andet omfatte følgende kontraktmæssige krav (ud over de gængse supportservicemål):

- Krav om inddragelse af brugere i udviklingsfaserne.
- Krav om gennemførelse af brugervenlighedstest m.m.
- Krav om uafhængig vurdering af løsningernes brugervenlighed i kontraktperioden.
- Krav om inddragelse af brugerne og om kontinuerlig forbedring af brugervenlighed efter idriftsættelsen.
- Krav om detaljeret afrapportering af henvendelses- og anvendelsesmønstre.
- Krav om reducering af supporthenvendelser i kontraktperioden.

14.5.1.7 Øget brugervenlighed

Supportbehov kan forenklet betragtes som omvendt proportionel til løsningens brugervenlighed. Dette synes at være bekræftet for NemID til erhverv, der får kritik på grund af dens utilstrækkelige brugervenlighed. NemID til erhverv har en høj supportfrekvens, forstået som antallet af henvendelser i forhold til antallet af certifikater. Det er fire gange så stort som for NemID privat.

NemID til erhverv dækker på nuværende tidspunkt en meget bred brugerskare og anvendes inden for forskellige domæner af forskellige brugertyper og -segmenter, både med stærke og svage it-kompetencer samt forskellige brugsmønstre.

Flere af de konceptuelle løsningsmuligheder, der blev præsenteret i Fase 1, omhandlede øget brugervenlighed for erhvervsbrugere, både rent kommunikativt og med hensyn til funktioner. En vigtig indsigt var, at én løsning ikke dækker de forskellige erhvervsaktørers behov. Der er brug for differentiering, og brugernes forskellige behov hænger ofte sammen med virksomhedens størrelse. Øges brugervenligheden i de administrative brugergrænseflader, vil behovet for support falde og den overordnede brugertilfredshed stige.

Det er primært de tunge administrative arbejdsgange, der er forbundet med indgåelse af den juridiske aftale, identificering af, hvem der er underskrifts- og tegningsberettiget for virksomheden, og processerne forbundet med etableringen af NemID-administratormodulet, der skaber frustrationer. Disse forstærkes yderligere af brugen af administrativt tungt sprog og uforståelige tekniske begreber. Det er tydeligt, at supportbehovet vil kunne mindskes betydeligt ved at øge brugervenligheden. Dette kunne fx være i forhold til bestillingsproceduren, ved at anvende et naturligt og forståe-

ligt sprog samt ved bedre at kommunikere og forklare arbejdsgangene, dvs. det samlede forløb og formål med de forskellige trin i procesflowet. Samtidig skal brugervenligheden øges ved aktivt at styre en mindre fragmenteret og mere tværgående tilgang til arbejdsgange på tværs af forskellige systemer, tjenester eller offentlige myndigheder, og ikke kun inden for NemID. Dette kan omfatte synkronisering og harmonisering af reglerne, anvendte begreber, brugergrænseflader, vejledninger, guides m.m. Denne opgave vil kun i mindre omfang direkte relatere sig til NemID.

Denne forbedring af brugeroplevelsen for NemID til erhverv i forhold til de administrative processer har et stort økonomisk potentiale. Hvis supportfrekvensen for medarbejdersignaturer, konservativt sat, kan reduceres med 20 %, hvilket stadig vil være over tre gange så højt som supportfrekvensen for NemID privat, vil udgifterne til erhvervs-support kunne reduceres kraftigt.[11]

14.5.2 Gevinster

Dette afsnit har til formål at præsentere de gevinster, løsningselementet potentielt tilvejebringer i forhold til relevante brugergrupper.

14.5.2.1 Borgere og medarbejdere

Løsningselementet og elementets enkelte tiltag rummer et stort gevinstpotentiale i forhold til større samlet tilfredshed hos brugerne.

Det er i særdeleshed virksomhederne og virksomhedernes medarbejdere, der har udtrykt deres manglende tilfredshed med NemID's brugervenlighed i relation til administrationsopgaven, i kombination med den tilbudte support. Løsningselementet forholder sig således til begge aspekter og indeholder tiltag, der adresserer både øget brugervenlighed og øget kvalitet af den ydede support. Tillige vil der kunne opnås større tilfredshed hos denne målgruppe med en prisreduktion eller et frikøb af brugersupport for medarbejdersignaturer.

14.5.2.2 Tjenesteudbydere

En bedre og billigere support vil bidrage positivt både til den generelle tilfredshed med NemID og til brugerenes oplevelse af de offentlige og private tjenester. Brugerne opfatter NemID som en del af de udbudte tjenester, og utilfredshed med NemID har en afsmittende og negativ indflydelse på, hvordan borgere og virksomheder opfatter selve tjenesterne. Specifikt kan de offentlige tjenesteudbydere forvente større tilfredshed med deres tjenester, både fra borgerne og ikke mindst fra virksomhederne.

Samtidig vil tjenesteudbydere være i stand at tilbyde en mere sammenhængende og dermed mere effektiv support gennem anvendelse af supportpakker.

14.5.3 Vurdering

Dette afsnit har til formål at analysere og vurdere løsningselementet i forhold til relevante parametre.

14.5.3.1 Arkitektur

Udformningen af supportydelsen har begrænset indflydelse på udformningen af den samlede infrastruktur og arkitektur af den kommende NemID-løsning.

Supportens omfang er i høj grad afhængig af løsningens tekniske kompleksitet.

14.5.3.2 Sikkerhed og privacy

Optimering af supporten vurderes ikke at have indflydelse på sikkerhed og privacy i den kommende NemID-løsning. Dog kan en udvidelse af supportfunktionen med nye medarbejdergrupper fra

[11] Beregningerne er foretaget med udgangspunkt i den nuværende leverandørs estimeringer af egne udgifter pr. henvendelse.

andre organisationer og virksomheder, der ikke nødvendigvis ser support, men derimod egen tjenesteydelse, som det centrale, føre til en øget risiko.

Det er derfor afgørende, at tjenesteudbydere, der vil tilbyde vejledning og support, skal overholde samme relevante sikkerhedsforskrifter og -krav som hovedsupportleverandøren.

14.5.3.3 Migrering

En optimeret support skønnes ikke at have betydning for migrering til den kommende NemID-løsning.

14.5.3.4 Relation i forhold til private partnere

Supportopgaven i forhold til NemID til erhverv forventes ikke at indgå som et element i et eventuelt samarbejde med private partnere.

14.5.3.5 OCES-certifikatpolitikker

Der er ikke behov for at ændre OCES-certifikatpolitikker i forbindelse med de beskrevne tiltag vedrørende optimering af supporten.

14.5.3.6 Økonomi

Der vil være fællesoffentlige merudgifter til frikøb af erhvervsløsningerne samt til etablering og drift af løsninger i forbindelse med sammenhængende support og bedre online-supportmuligheder.

Særligt udgifter i forhold til erhvervssupport til bedre betalingsvilkår og reducerede priser og eventuelt frikøb af support vejer tungt og estimeres til at udgøre et mindre trecifret millionbeløb over en periode på 5 år. Etableringsudgifter og driftsudgifter (over en femårig periode) til mere sammenhængende support og bedre online-supportmuligheder vurderes til at beløbe sig til et encifret millionbeløb.

Disse udgifter skal ses i relation til mulige besparelser som følge af tiltag, der vil være med til at reducere den høje supportfrekvens for NemID til erhverv, og som samtidig vil bidrage til yderligere reduktion af supportbehov for borgere. Disse besparelser estimeres til at være på mellem 10 og 30 millioner kroner, svarende til reduktion af fællesoffentlige udgifter til support på mellem cirka 10 % og 25 %.

Det er primært tiltag vedrørende øget brugervenlighed, bedre online-supportmuligheder samt kontraktmæssige incitamenter, der rummer de største besparelsespotentialer. Disse besparelser kan være ret store, hvis man tager udgangspunkt i leverandørens *egne* estimater af de reelt afholdte udgifter, under forudsætning af, at de fremover i højere grad skal dækkes af det offentlige.

Det antages samtidig, at reduktion af supportpriser eller frikøb af erhvervssupport kun i begrænset omfang vil medføre en forøgelse i antallet af supporthenvendelser.

14.5.3.7 Finansieringsmodeller

Supportydelser til erhverv har i dele af den nuværende kontraktperiode været betalt af virksomheder og myndigheder, som nævnt med udbredt ønske om at gøre support gratis, da det er obligatorisk at anvende NemID til fx Digital Post.

I en fremtidig løsning kan der overvejes en mere differentieret support til forskellige brugergrupper, herunder erhvervs- og borgergrupper. Der kan endvidere overvejes en differentieret grad af brugerbetaling for forskellige brugergrupper afhængigt af deres supportbehov.

Supportydelser til borgere vurderes kun i begrænset omfang at kunne finansieres af andre end det offentlige.

14.5.3.8 Leverandørstrategi

Det vurderes, at opgaven med at levere den konkrete supportydelse med fordel kan forsøges adskilt fra de øvrige NemID-leverancer for at sikre større specialisering i opgavevaretagelsen og

præcis ansvarsplacering af leverancen. En særskilt udbudsforretning vil kunne afprøve markedsaktørernes villighed til at løfte denne opgave.

14.5.3.9 Risici

Optimering af supportydelsen tilfører ikke i sig selv nogle væsentlige risikoelementer. Tværtimod bidrager den til risikominimering, både under migrering og drift af den nye løsning.

14.5.3.10 Juridiske problemstillinger

Der er ingen særlige juridiske problemstillinger ved bedre og billigere support.

14.5.4 Samlet vurdering for løsningselementet

RMC-ICG vurderer, at forbedret support ikke kun vil øge brugertilfredsheden, men også bidrage væsentligt til reduktion af de økonomiske rammer for den kommende NemID-løsning.

Tabel 19: Opsummering af RMC-ICG's vurdering af løsningselement F

Vurderingsparametre	RMC-ICG's vurdering
Arkitektur	Lille eller ingen indflydelse på den samlede infrastruktur og arkitektur.
Sikkerhed og privacy	Ingen indflydelse på sikkerhed og privacy.
Migrering	Ingen betydning for migrering.
Relation i forhold til private partnere	Det er p.t. uafklaret, om supporten er et element i et eventuelt samarbejde med private partnere.
OCES-certifikatpolitikker	Ingen ændring.
Økonomi	Positivt bidrag til den samlede økonomi.
Finansieringsmodeller	Meget begrænsede finansieringsmuligheder fra andre end det offentlige.
Leverandørstrategi	Kan bidrage til flerleverandørstrategi via eventuel adskillelse af support fra de øvrige NemID-leverancer.
Risici	Positivt bidrag til det samlede risikobillede.

14.6 Samlet konklusion for Scenarie 3

14.6.1 Samlede gevinster

RMC-ICG har vurderet gevinsterne ved scenariet ud fra de overordnede gevinster, der er beskrevet i afsnit 4.

Tabel 20: Oversigt over RMC-ICG's gevinstvurdering for Scenarie 3

Gevinst	RMC-ICG's vurdering
Høj tillid til løsningen	Højere tillid som følge af mere fokus på privacy (Element D).
Lettere anvendelse for borgere	Forbedring i kraft af mulighed for login med 1-faktor (Element A), flere login-faktorer (Element E) og bedre support (Element F).
Lettere anvendelse for virksomheder	Forbedring i kraft af de mange enkeltmands-virksomheders mulighed for at benytte NemID privat (Element B). Forbedring i kraft af mulighed for flere login-faktorer (Element E) og bedre support (Element F).
Lettere administration for virksomheder og myndigheder	Store forbedringer som følge af indsatsen i Element B og C og mulighed for bedre support (Element F).
Flere offentlige tjenester anvender det nye NemID	Stigning som følge af muligheden for at anvende 1-faktor-login (Element A) og mulighed for at få kontekstafhængig information (Element D).
Flere private tjenester anvender det nye NemID	Stor stigning som følge af muligheden for at anvende 1-faktor-login (Element A).
Mere fleksible udviklingsmuligheder	Store forbedringer som følge af muligheden for at adskille autentifikation og signering (Element A).

Scenarie 3 dækker de samme behov som Scenarie 2 og giver desuden mulighed for gevinster på yderligere tre områder.

Scenariet kan betyde en styrkelse af borgernes høje tillid til løsningen i kraft af styrkelsen af privacy. For tjenesteudbyderne betyder scenariet mulighed for mere målrettet (kontekstafhængig) information om brugerne.

Desuden kan løsningen give lettere anvendelse for borgere i kraft af mulighed for flere login-faktorer. Hvilke login-faktorer, der kan komme på tale og på hvilke betingelser, vil dog først blive afklaret i forbindelse med det videre arbejde i projektet.

Endelig indebærer scenariet mulighed for bedre supportløsninger for borgere i sammenhæng med tiltag for øget brugervenlighed. For erhvervslivet vil der dels være bedre support, dels mulighed for adgang til billigere eller helt gratis support.

Hvor Scenarie 2 gav mulighed for gevinster i form af tidsbesparelser for borgere, virksomheder og myndigheder, betyder de yderligere elementer i Scenarie 3 gevinster i form af øget brugertilfredshed og øget tillid til løsningen.

14.6.2 Samlet økonomi

Udgifterne for Scenarie 3 bygger på den samlede økonomi for Scenarie 2 med tilføjelse af udgifterne til elementerne fra Scenarie 3.

Også i Scenarie 3 er der dels fællesoffentlige udgifter, dels udgifter i det øvrige økosystem.

Som nævnt er det ikke muligt at beregne udgifterne til login-faktorer uden at have valgt en konkret faktor. De samlede fællesoffentlige udgifter til Scenarie 3 er omkring 40-60 millioner kroner højere end for Scenarie 2. Det skyldes øgede nettoudgifter til bedre og billigere support. Især udgifter til delvist frikøb af support for erhvervslivet. Der knytter sig dog en vis usikkerhed til størrelsen af dette på sigt, idet supportudgifterne muligvis vil falde som følge af, at der nu er bedre kendskab til løsningerne blandt brugerne. Da de samlede supportudgifter udgør en stor del af udgifterne til

NemID, anbefaler RMC-ICG, at der sættes fokus på, hvordan supporten kan optimeres og effektiviseres.

Også i dette scenarie knytter den største usikkerhed sig til de priser, som leverandørerne vil byde ind med og aftaler om udgiftsfordeling med eventuelle partnere.

En anden usikkerhed knytter sig til antallet af tjenesteudbydere, der skal gennemføre ændringer i forbindelse med bredere anvendelse af NemID privat til erhverv.

Derimod er de samlede udgifter hos tjenesteudbydere afhængigt af, om der fastlægges fælles krav til at understøtte NemID privat (det kan betyde større udgifter end nævnt), hvor mange udgifter tjenesterne reelt får, og hvor mange tjenester der vælger at understøtte dette.

Udgifter i forbindelse med kontekstafhængig information og øget privacy forventes at balancere for broker-leverandører.

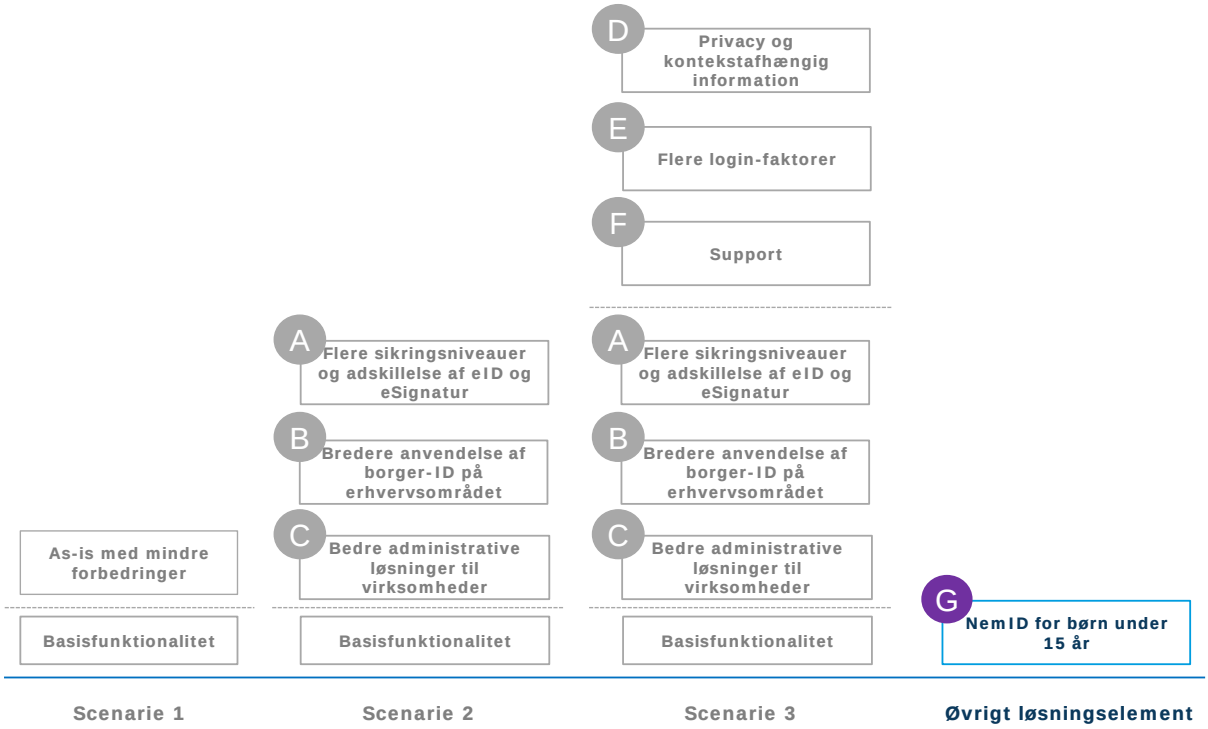
14.6.3 Leverandørforhold

Et udbud af en løsning, der som Scenarie 2 afviger fra den nuværende, vil gøre det mere attraktivt for andre leverandører end den nuværende leverandør, og et sådant udbud kan medføre, at flere leverandører vil finde det attraktivt at byde. Det har dermed betydning for konkurrencesituationen og i sidste ende for den samlede pris på løsningen.

15. Øvrigt løsningselement

Dette kapitel præsenterer løsningselementet *NemID for børn under 15 år*, der skal opfattes som en separat byggeklods til de tre scenarier, jf. Figur 26.

Figur 26: Øvrigt løsningselement



15.1 Løsningselement G: NemID til børn under 15 år

I dette afsnit præsenteres løsningselementet. Herefter analyseres de overordnede potentielle forretningsmæssige gevinster, som RMC-ICG vurderer, at løsningselementet kan tilvejebringe. Dernæst foretages en vurdering af løsningselementet, og afsnittet afsluttes med en konklusion.

15.1.1 Præsentation

NemID til børn under 15 år omfatter udvidelse af login-funktionaliteten til at dække behovene hos flere tjenesteudbydere i forhold til at understøtte denne målgruppe. Det gælder fx i forhold til skole- og institutionsformål og børns behov for let og sikker login i relation til følgende områder:

- Skoler.
- SKAT, e-Boks, Feriekonto.
- Biblioteker.
- Fritidsinstitutioner.
- Pengeinstitutter (kontokig i egne konti).

Udvidelsen af NemID-login funktionaliteten til børn under 15 år kan omfatte forskellige aldersgrupper og -segmenter. Det vurderes, at kravene i forbindelse med registrering og administration af NemID til børn i alderen 6-12 år vil medføre behov for specielle tilpasninger i forhold til basisløsningen og dermed også et større udgiftsniveau. Disse specielle tilpasninger vil blandt andet omfatte specielle registreringsprocedurer, hvor fx skolerne eller forældre skal kunne stå for registrering

samt specialtilpasset og målrettet support. Ligeledes vil der være et krav om, at læreren eller en anden ressourceperson på skolen skal kunne nulstille en glemt adgangskode inden for få minutter.

Dette kan tale for, at løsningen for børn skal indskrænkes til alene at omfatte børn i alderen 13-14 år, der formodes at have tilstrækkelige færdigheder og modenhed til selv at kunne administrere og anvende løsningen. Det skal dog i den sammenhæng pointeres, at en eventuel afgrænsning af NemID til de 13-14-årige i første omgang ikke udelukker, at NemID på sigt også kan blive tilbudt til børn under 13 år.

15.1.1.1 Brugervenlighed

Indførelse af NemID til børn under 15 år vil forudsætte udvikling af særlige, meget brugervenlige løsninger til denne målgruppe. Løsningerne skal både tage hensyn til børns kompetencer og forståelse og meget specifikke krav til administration af løsningen, herunder ikke mindst på skoleområdet.

Disse overordnede krav kan bidrage til fragmentering af NemID-løsningen og begrænse muligheder for udbredelse af løsningen på tværs af de offentlige og private tjenesteudbydere. Begge faktorer kan have en utilsigtet og negativ virkning for den samlede brugeroplevelse.

15.1.2 Gevinster

15.1.2.1 Børn

Børn under 15 år har meget forskellige behov i forhold til NemID afhængig af både de specifikke brugssituationer, børns kompetencer og ikke mindst i relation til forståelsen af løsningen og betingelserne for at anvende den. Dog vurderes det, at de fleste login-behov på et lavere sikkerhedsniveau for denne målgruppe allerede er dækket af UNI•Login på skoleområdet. UNI•Login er den mest anvendte (og oftest den eneste) løsning, som børn i denne aldersgruppe har brug for.

De få situationer, hvor man kræver en login-funktion på et højere sikkerhedsniveau, dækkes ligeledes i høj grad allerede af UNI•Login – suppleret med relevante retningslinjer og processer i forhold til specifikke situationer som fx eksaminer. For anvendelse af SKAT's løsning er det procedurerne for udstedelse af et TastSelv-nummer, der er med til at øge sikkerhedsniveauet (i forhold til registrering).

For andre områder inden for det offentlige (biblioteker, fritid) dækkes login-behovene for børn under 15 år af forskellige løsninger med PIN-kode.

Samlet vurderes gevinsterne for børn under 15 år isoleret set som ret begrænsede.

15.1.2.2 Forældre

Forældre til børn under 15 år er kun en *indirekte* målgruppe for NemID til børn under 15 år. Deres behov knytter sig mere til en nem mulighed (dvs. helst med 1-faktor-login) for at anvende deres eget NemID til at have adgang til tjenester med informationer om deres børn (fx gennem attributter, der knytter barnet til forældrenes NemID).

Forældrenes adgang til tjenester med informationer om deres børn under 15 år er gældende for de fleste situationer, undtagen bestemmelser i sundhedslovgivningen, jf. § 37 i Sundhedsloven: "…forældremyndighedsindehaverens interesse i at blive gjort bekendt med oplysningerne findes at burde vige for afgørende hensyn til den mindreårige".

På skoleområdet anvender forældrene i dag et forældreintra-system med login, som vil blive erstattet af UNI•Login til forældre. Dette vil på sigt kunne give forældrene mulighed for at logge på UNI•Login via NemID gennem den etablerede centrale envejs-kobling mellem NemID og UNI-ID/UNI•Login.

15.1.2.3 Tjenesteudbydere

Gevinsterne for tjenesteudbydere vil være en funktion af, hvorvidt NemID udstedes til børn under 13 år.

Skoleområdet

Målgruppen på skoleområdet er *alle* elever. Der er cirka 400.000 elever i alderen 5-12 år og cirka 135.000 elever i alderen 13-14 år.

Styrelsen for IT og Læring har overvejet en model, hvor NemID skal kunne udstedes til alle børn, da også børn under 13 år skal kunne anvende skolesystemer og -løsninger. At give kun de 13-14-årige mulighed for at benytte NemID, vil fx ikke gøre den store forskel i den daglige anvendelse på skolerne. Så længe det ikke er *alle* elever, der kan få et NemID, vil det kun være et supplement til – og ikke en erstatning for – UNI•Login brugernavn/adgangskode. Med 1-faktor-login vil NemID kunne benyttes til autentifikation i elevernes dagligdag, og med 2-faktor-login vil den kunne benyttes til autentifikation ved særlige lejligheder, der kræver en ekstra sikkerhed.

De samme overvejelser vedrørende afgrænsning af løsningen til 13-14-årige gør sig også gældende på SKAT og andre områder.

SKAT

SKAT har udtrykt ønske om, at NemID skal udstedes til børn under 15 år for at reducere anvendelsen af TastSelv-løsningen for denne målgruppe. SKAT har således – i forbindelse med forskudsregistrering for 2015 – registreret cirka 81.000 brugere i alderen 13-14 år, cirka 22.500 brugere i alderen 6-12 år og cirka 3.000 brugere i alderen 0-5 år.

For SKAT skal alle børn beskattes som selvstændige skattepligtige personer på helt samme måde som voksne, dvs. principielt fra fødsel. Derfor er der ikke en nedre grænse for, hvornår man er skattepligtig, og målgruppen er således principielt de 0-15-årige. Børn i alderen 0-6 år formodes dog at blive håndteret ved at knytte dem til forældrenes/værgernes identiteter.

Andre områder

NemID til børn under 15 år vil kunne anvendes af andre tjenester, hvor der ikke kræves et højt sikkerhedsniveau – fx biblioteker, sportsklubber, fritidsinstitutioner osv. Eksisterende loginmekanismer (PIN-kode, sundhedskortbaserede løsninger m.m.), der dækker behov på disse områder, vil således på længere sigt kunne erstattes eller suppleres med 1-faktor-NemID. Der skal dog sondres mellem behov for adgang for forældre/værge, der fx skal reservere plads til deres barn m.m., og barnets eget behov for adgang til institutionernes systemer.

NemID til børn under 15 år kan ligeledes anvendes i forbindelse med brugerportalsinitiativet som alternativ til eller som en eventuel erstatning for UNI•Login.

Specifikt om UNI•Login

NemID til børn under 15 år skal ikke mindst vurderes i forhold til den eksisterende UNI•Login-infrastruktur og løsning på skoleområdet. UNI•Login består af både UNI-ID funktionalitet[12] og en login-tjeneste. UNI-ID er et unikt identifikationsnummer for hver identitet for både elever og lærere, hvor der tilknyttes brugernavn og adgangskode, som opbevares i en brugerdatabase. UNI•Login er på nuværende tidspunkt den eneste offentlige tjeneste, som udbyder en generel autentifikation af personer under 15 år – næsten alle børn over 5-6 år er registreret i UNI•Login.

UNI•Login agerer således både som identitetsgarant, dvs. det står for elevens identitet og udstedelse af akkreditiver (brugernavn og adgangskode), og som en login-tjeneste og føderation (single sign-on) mellem skoler, forskellige tjenester og løsninger. Der er på nuværende tidspunkt mere end en million elever, lærere og ansatte i UNI•Logins brugerdatabase.

Log-in-tjenesten styrer desuden brugerrettigheder og -roller (dvs. elevtyper, medarbejdertyper m.m.) og deres tilknytning til uddannelsesinstitutionen, så de registrerede brugere kan logge på institutionens tjenester og abonnementer. Brugerne og deres attributter håndteres gennem et bru-

[12] UNI-ID-begrebet anvendes her for at sondre mellem identitetsgarant-funktionalitet og login-tjeneste i UNI•Login.

ger-administrationsmodul af UNI•Logins brugeradministrator, der er udpeget af skolen. Brugeradministratoren kan manuelt oprette og fjerne brugere, editere stamoplysninger, nulstille adgangskode samt give den enkelte lærer en særlig rettighed til at nulstille elevers adgangskoder.

Ud over den manuelle brugeradministration foregår der, via en standard-grænseflade, en automatisk (og delvist tovejs) synkronisering af informationer om brugerne mellem uddannelsesinstitutionernes administrative systemer og den centrale brugerdatabase i UNI•Login blandt andet med mulighed for masseoprettelse af brugerne i UNI•Login.

15.1.3 Vurdering

Dette afsnit har til formål at analysere og vurdere løsningselementet i forhold til relevante parametre.

15.1.3.1 Arkitektur

En løsning til børn og unge under 15 år forudsætter, at der ikke indgår signering – da børn og unge under 15 år ikke er personligt myndige. Samtidig skal løsningen kunne anvendes med 1-faktor-login, fx i relation til de mange tjenester på skoleområdet. Det vil sikre en smidig adgang til digitale læremidler, nationale test, digitale afgangsprøver, elevplaner, skolens intranet osv. En løsning med 2-faktor-login kan fx anvendes i forbindelse med afgangsprøver og andre digitale eksaminer.

Disse funktionsmæssige krav for NemID til børn under 15 år forudsætter, at man skal adskille eID og eSignering primært som følge af, at der skal være mulighed for at understøtte flere sikkerhedsniveauer. Scenarie 2 og Scenarie 3, som begge indeholder den nævnte adskillelse af eID og eSignering samt flere sikkerhedsniveauer, må derfor betragtes som en forudsætning for indførelsen af NemID til børn under 15 år.

15.1.3.2 Sikkerhed og privacy

Implementering af NemID til børn under 15 år kan have både nogle sikkerhedsmæssige implikationer og konsekvenser i forhold til privacy. Børn under 15 år har forskellige forudsætninger og kompetencer for at anvende løsningen, herunder for selv at kunne håndtere og beskytte deres adgangskode (eller andre login-faktorer). Dette kan udgøre sikkerhedsrisici, som dog også eksisterer i dag i forhold til de nuværende login-mekanismer.

Disse sikkerhedsrisici kan blive større som følge af kravet om administration og nulstilling af adgangskode af lærerne i undervisningssituationer.

15.1.3.3 Migrering

Etablering af muligheden for at anvende NemID til børn under 15 år vil kræve, at tjenester, der hidtil har anvendt andre login-mekanismer, gradvist skal åbne op for en NemID-adgang for denne gruppe af brugere.

Konkret vil det fordre, at NemID skal kunne anvendes i stedet for SKAT's TastSelv på samme måde som for andre brugergrupper (dvs. med 2-faktor-login). Denne migrering af andre tjenester, der i forvejen har en NemID-baseret adgang, vurderes ikke at kræve ekstra ressourcer og udgifter i forhold til den generelle migrering til næste generation NemID.

Tjenester, der derimod ikke baseres på NemID (eller NemLog-in) på nuværende tidspunkt, som det fx er tilfældet for mange bibliotekssløsninger og fælles bibliotekstjenester, vil naturligvis kræve en tilpasning af deres login-mekanismer (fx PIN-login) og etableringen af koblingen til den kommende NemID-infrastruktur gennem TU-pakken.

For UNI•Login-infrastrukturen vurderes omfanget af migreringsopgaven ikke som særlig stor, da UNI•Login allerede har oprettet en central envejs-kobling mellem NemID og UNI-ID/UNI•Login, som i værste fald vil kræve en mindre tilpasning til den kommende NemID-løsning. En afskaffelse af UNI•Login (og UNI-ID dvs. identitetsgarantsdelen) vil på sigt naturligvis kun være mulig, hvis NemID udstedes for alle elever. Dette vil dog kræve, at eksisterende integrationer via dataoverførsler mellem UNI•Logins brugerdatabase og decentrale studieadministrative systemer på uddan-

nelsesinstitutionerne vil blive migreret til tilsvarende løsninger med NemID. Det er tvivlsomt, om en sådan migrering vil være teknisk mulig eller økonomisk rentabel.

15.1.3.4 Relation i forhold til private partnere

NemID til børn under 15 år forventes kun at have en begrænset interesse fra eventuelle private partnere, specifikt fra dem, der på nuværende tidspunkt er nødt til at tilbyde skræddersyede løsninger for denne målgruppe. De eventuelle private partnere vil have meget forskellige krav til sikkerhedsniveauer, administrative rettigheder m.m. i forhold til fx i uddannelsessektoren.

Således forventes fx bankerne ikke at ville kunne acceptere et eID, hvor skolepersonale har adgang til at genudstede adgangskoder, da det kan medføre risiko for misbrug af adgang til bankløsninger.

15.1.3.5 OCES-certifikatpolitikker

I den nuværende NemID-løsning er det allerede muligt at få NemID ned til 15 år. NemID til unge under 18 år kan ikke anvendes til at indgå aftaler med samme retslige virkning som NemID til personer over 18 år. Derfor er NemID med offentlig digital signatur mærket, så det fremgår af certifikatet, at der er tale om en signatur til unge mellem 15 og 18 år.

Den enkelte tjenesteudbyder skal således tjekke certifikatets oplysninger om, at en given bruger er under 18 år, og sikre, at de muligheder, som brugeren har, er tilpasset herefter.

OCES-certifikatpolitikker og registreringsprocedurer understøtter teknisk set allerede i dag mulighed for NemID til børn under 15 år. Men den nuværende certifikatpolitik for OCES-personcertifikater stiller krav om, at brugeren af NemID skal kunne indgå forpligtende aftaler, og børn under 15 år kan ikke indgå forpligtende aftaler.

15.1.3.6 Økonomi

De økonomiske estimater for indførelsen af NemID til børn under 15 år omfatter udgifter til udvikling af specielle administrative løsninger, merudgifter som følge af flere NemID samt migreringsudgifter for de vigtigste tjenesteudbyder.

Udgifter i forbindelse med udvikling af specialtilpassede administrative løsninger

En udvidelse af NemID til også at omfatte børn under 15 år vil kræve udvikling af tilpassede løsninger i forhold til basisløsningen. Disse løsninger vil omfatte specielle registreringsprocedurer samt løsninger, der gør det muligt for en lærer at nulstille en adgangskode i en undervisningssituation, hvor en elev måtte have glemt sin adgangskode.

Engangsudgifter i forbindelse med udvikling af disse løsninger estimeres til et mindre encifret millionbeløb.

Merudgifter i forbindelse med udstedelse, fornyelse, drift og support af flere NemID

Hvis alle børn i alderen 6-15 år, dvs. over 500.000 personer, ønsker at anskaffe NemID, vil dette svare til ekstra udgifter til udstedelse og etablering på mellem 20 og 50 millioner kroner – med en listepris for nøglekort på 75 kroner. Dette vil således udgøre merudgifterne, hvis man vælger at understøtte 2-faktor-login for *alle* skolebørn.

Fornyelse eller udskiftning af nøglekort skønnes at medføre mindre årlige udgifter, hvis der i gennemsnit udstedes et nyt nøglekort til cirka 5 % af alle børn hvert år. Stigningen i driftsudgifter estimeres til at udgøre et større millionbeløb over en periode på 5 år.

Dertil skal føjes ekstra supportudgifter, hvor der regnes med mindre supportbehov både på grund af 1-faktor-login og som følge af, at en stor del af supporten vil kunne leveres af skolerne. Det antages derfor, at merudgiften for support ligeledes vil være på et encifret millionbeløb over en periode på 5 år.

NemID til børn under 15 år som erstatning for UNI•Login

Udstedelsen af et NemID til børn under 15 år – og unge under 18 år – til brug inden for skoleområdet skal alene ses som en mulighed for at erstatte en *del* af UNI•Login-infrastrukturen. Dvs. den del, der står for registrering og udstedelse af identiteter (UNI-ID). Udstedelsen vedrører derfor ikke login- og rettighedsstyring i UNI•Login-infrastrukturen.

Afskaffelse af identitetsgarantsdelen af UNI•Login-infrastrukturen vil kun være mulig, hvis eksisterende integrationer via dataoverførsler mellem UNI•Login-brugerdatabasen og decentrale studieadministrative systemer på uddannelsesinstitutionerne erstattes med tilsvarende løsninger med NemID.

Samtidig er de økonomiske konsekvenser af indførelse af NemID til børn under 15 år ligeledes afhængige af, om NemID vil blive indført for *alle* børn eller kun for de 13-14-årige.

Sammenlagt vurderes det, at udbredelsen af NemID til børn under 15 år (enten for børn ned til 6 år eller for de 13-14-årige) alene vil være en udgift i relation til skoleområdet. UNI•Login-infrastrukturen – eller en del af den – vil skulle bibeholdes, hvilket vil betyde opbygning af en parallel infrastruktur på skoleområdet med meget usikre gevinster og besparelsespotentiale.

NemID til børn under 15 som erstatning for TastSelv-kode hos SKAT

En erstatning af TastSelv-koden for børn med NemID (uagtet om det omfatter alle børn eller kun de 13-14-årige) vil bidrage til reduceret brug af SKAT's TastSelv-kode. På nuværende tidspunkt vil det dog ikke være ensbetydende med, at hele TastSelv-løsningen vil kunne udfases, og den bagvedliggende infrastruktur afvikles.

Løsningen vil således ikke føre til væsentlige besparelser. Løsningen må derfor betragtes som økonomisk neutral, da udgifter til migrering vurderes at være af begrænset omfang.

15.1.3.7 Finansieringsmodeller

RMC-ICG vurderer, at finansieringen af NemID til børn under 15 år ikke vil være forskellig fra finansieringen af andre borgercertifikater. Dog vil man kunne forvente en vis medfinansieringsvilje fra nogle private tjenesteudbydere.

Det skønnes, at de årlige transaktionsudgifter, der kan påføres tjenesteudbyderne, vil udgøre et mindre encifret millionbeløb.

15.1.3.8 Leverandørstrategi

NemID til børn under 15 år må betragtes som en specifik løsning, der blandt andet skal omfatte specielle registreringsprocedurer, mulighed for nulstilling/udstedelse af adgangskode samt specialtilpasset og målrettet support. Omfanget af disse behov taler for, at løsningen, hvis besluttet, etableres som en særskilt leverance (og eventuelt udbudsforretning) adskilt fra basisløsningen.

15.1.3.9 Risici

De største risikoelementer i forbindelse med NemID for børn under 15 år knytter sig til migreringsprocessen på skoleområdet. Dette gælder migrering af brugere fra den eksisterende UNI•Login – den del, der står for registrering og udstedelse af identiteter (UNI-ID). Det gælder desuden migrering af uddannelsesinstitutionernes studieadministrative systemers integrationer fra UNI•Login-brugerdatabasen (UNI-ID) til tilsvarende NemID-løsninger.

15.1.3.10 Juridiske problemstillinger

En række særlige juridiske problemstillinger knytter sig til etableringen af NemID for børn under 15 år, herunder undtagelser i forhold til forældrenes adgang til sundhedsinformationer, der kræver en særskilt håndtering fra tjenesteudbydere.

15.1.3.11 Styringsmæssige problemstillinger.

Det er vurderingen, at NemID for børn under 15 alt andet lige bringer øget kompleksitet i den samlede løsning, med øget behov for styring og styringsressourcer som følge.

15.1.4 Samlet konklusion

Sammenfattende anbefaler RMC-ICG på nuværende tidspunkt, at NemID *ikke* udvides til også at omfatte børn under 15 år, da business-casen for det offentlige for denne udvidelse *ikke* er positiv.

Det understreges, at denne anbefaling forholder sig til estimering af *nuværende* behov, gevinster og omkostninger, og at anbefalingen om ikke at implementere NemID til børn under 15 år kan revurderes ved afgørende ændringer af de forudsætninger, der ligger til grund for den gennemførte analyse.

Udgifter i forbindelse med udvikling af specialtilpassede løsninger for NemID til børn under 15 år, udstedelse, drift og support med medregnet medfinansiering estimeres til at være et større million-beløb. Det skal betragtes som *merudgifter*, da de eksisterende UNI•Login- og TastSelv-infrastrukturer ikke vil kunne fjernes. Denne merudgiftsbetragtning gælder i høj grad også andre tjenester, hvor det er en forventning, at eksisterende login-mekanismer i lang tid vil fungere ved siden af NemID til børn under 15 år – herunder gevinster og merudgifter, der følger af at udvide NemLog-in.

Samtidig anbefales det, at det i samarbejde med Styrelsen for IT og Læring undersøges, hvorvidt det er muligt at udvide med en alternativ tilgang til autentifikationsløsninger til børn under 15 år.

En alternativ tilgang kunne fx tage udgangspunkt i et trust framework, hvor UNI-ID/UNI•Login-infrastrukturen indgår som identitetsgarant og broker i den foreslåede arkitekturmodel. UNI-ID/UNI•Login vil kunne udbredes og anvendes på andre domæner, hvor der i lighed med på skole-området kræves et lavere sikkerhedsniveau – fx i biblioteker, sportsklubber, fritidsinstitutioner osv.

Login-mekanismer, der er etableret på disse områder, vil således enten kunne anvende UNI•Login eller 1-faktor-NemID, forudsat at der er tillid til sikkerhedsniveauer både i forhold til registrering og autentifikation. Der bemærkes i denne sammenhæng, at UNI•Login allerede indgår i et tillidsfuldt samarbejde med andre tjenester under WAYF (Where Are You From).

Disse digitaliseringsstrategiske afklaringer i forhold til løsningen til børn under 15 år foretages af Digitaliseringsstyrelsen uden for denne analyses rammer.

Tabel 21: Opsummering af RMC-ICG's vurdering af løsningselement G

Gevinst	RMC-ICG's vurdering
Høj tillid til løsningen	Ingen ændring
Lettere anvendelse for borgere	Lille forbedring
Lettere anvendelse for virksomheder	Lille forbedring
Lettere administration for virksomheder og myndigheder	Ingen ændring
Flere offentlige tjenester anvender det nye NemID	Lille stigning
Flere private tjenester anvender det nye NemID	Lille stigning
Mere fleksible udviklingsmuligheder	Flere udviklingsmuligheder

16. Overordnede konklusioner

Formålet med analysen er at bistå de fællesoffentlige parter med at forberede et beslutningsgrundlag forud for anskaffelsen af næste generation af den nationale infrastruktur for e-identitet og digital signatur (næste generation NemID).

Da NemID er en grundsten for digitale løsninger både i den offentlige og private sektor, har der været meget stor interesse for, hvordan næste generation udformes samt betingelserne for anvendelse af den.

De mange forskellige interessentgrupper har medvirket ved at tilkendegive behov og ønsker, og de indgår som en del af grundlaget for foranalysen. Desuden er der gennemført en teknisk analyse af tekniske udfordringer og løsningsmodeller for næste generation NemID. Det er suppleret med markedsanalyser og teknisk dialog med interesserede leverandører både i Danmark og fra udlandet.

16.1 Behov, lovgivning, økonomi og arkitektur

En række forhold sætter rammen for næste generation NemID, enten i form af udefrakommende krav og begrænsninger, eller beslutninger af overordnet karakter i projektet.

EU's forordning om elektronisk identifikation og tillidstjenester betyder en begrebsmæssig opdeling i eID og digital signering, som kan få indflydelse på næste generation NemID.

Udformning af næste generation NemID vil være bestemt af prioriteringen af mål og gevinster, herunder afvejninger mellem brugervenlighed, økonomi, finansieringsforhold og hensyn til sikker migrering til den ny løsning.

Til den nuværende NemID-løsning blev der i 2008 afsat 850 millioner kroner samlet for det offentlige og bankerne. Den kommende løsning forventes at koste mere, primært som følge af en langt større udbredelse og anvendelse af NemID end forventet ved indgåelsen af den nuværende kontrakt i 2008. Hvor store udgifterne til den fremtidige løsning bliver, er dog meget usikkert.

Brugervenligheden i næste generation NemID kræver et kontinuerligt fokus på brugernes behov både i forbindelse med kravspecifikation, udvikling af den ny løsning og løbende i hele kontraktperioden. RMC-ICG anbefaler, at der arbejdes med iterative designprocesser for at sikre, at brugervenligheden for NemID bliver bedst mulig og udvikler sig i takt med fremtidige behov.

Analysen af fremtidige forretningsmodeller viser, at brugerne forventer, at NemID fortsat er gratis, og at de nuværende betalinger reduceres eller fjernes helt. Det kan dog betyde, at andre markedsaktører vil få svært ved at komme ind på markedet for autentifikation og digital signering med løsninger, der supplerer eller erstatter NemID. Dermed hænger beslutning om forretningsmodel sammen med valg af leverandørstrategi for den kommende løsning. Heri indgår om og hvordan der skal være mulighed for flere supplerende leverandører ud over en eller flere hovedleverandører.

Indhold og økonomi i næste generation NemID vil være afhængig af, om der kan skabes en tilstrækkelig konkurrence i den kommende udbudsforretning. Her kan der være risiko for et begrænset antal tilbudsgivere, givet markedets størrelse samt den eksisterende leverandørs dominerende position. Det er derfor afgørende, at der aktivt arbejdes både med rammerne og eventuelt opdeling af de efterspurgte leverancer, for derved at skabe tilstrækkelig kommerciel interesse, ikke mindst blandt de internationale leverandører.

Den valgte arkitekturmodel har væsentlig indflydelse på fleksibiliteten og den samlede sikkerhed i infrastrukturen. Med en løsere kobling mellem identitetsgarant og tjenesteudbyder vil man kunne

opnå en række fordele. Det betyder efter RMC-ICG's vurdering, at der er behov for grundlæggende arkitekturændringer. Derfor anbefales det, at en kommende NemID-infrastruktur baseres på anvendelse af en arkitektur med broker-funktionalitet.

NemID er kritisk for en lang række offentlige tjenester, for private tjenester og for bankerne, hvilket stiller særdeles høje krav til tilgængeligheden døgnet rundt, året rundt. Det betyder store krav til både de nuværende og kommende leverandører om løsninger og et fokus på tilgængeligheden i den kommende migreringsproces.

16.2 Valg af scenarier

Analyserne peger på to grundlæggende veje for næste generation NemID: en fortsættelse af den nuværende løsningsmodel eller fornyelse.

En fortsættelse af den nuværende løsningsmodel bygger på Scenarie 1.

En fornyelse bygger på Scenarie 2 eller 3 eller en kombination af disse to.

Valget mellem fortsættelse og fornyelse forudsætter en række beslutninger om de tekniske løsningsmodeller, men også om ønsket funktionalitet, leverandørstrategi, migrering osv.

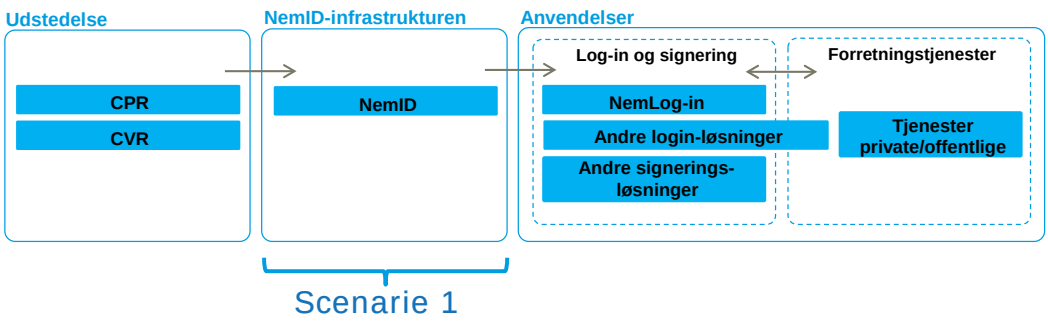
Det har afgørende betydning, hvilke leverandører og hvor mange det lykkes at få til at deltage i det kommende udbud. Der er således risiko for, at der kun vil være én leverandør på banen, som det også var tilfældet ved sidste udbud, og det vil trække i retning af en fortsættelse af den nuværende løsningsmodel. Det har ligeledes stor betydning, om der etableres mulighed, for at andre leverandører får reel mulighed for at bidrage til den samlede løsningsportefølje.

Det spiller ind i valget, at der foregår et standardiseringsarbejde i EU, som kan have betydning for NemID. Ved at vælge en løsning, der er i overensstemmelse med det internationale marked for løsninger til autentificering, kan der opnås bedre og billigere løsninger.

Foranalysen viser endvidere, at beslutningerne om næste generation NemID har konsekvenser – ikke kun for løsningen selv, men også andre steder i NemID-økosystemet og dermed digitaliseringen af Danmark.

Scenarie 1 er karakteriseret ved at være som den nuværende løsning og indebærer derfor kun ændringer – så få som muligt – i selve NemID-infrastrukturen.

Figur 27: Konsekvenser af Scenarie 1 for NemID-økosystemet

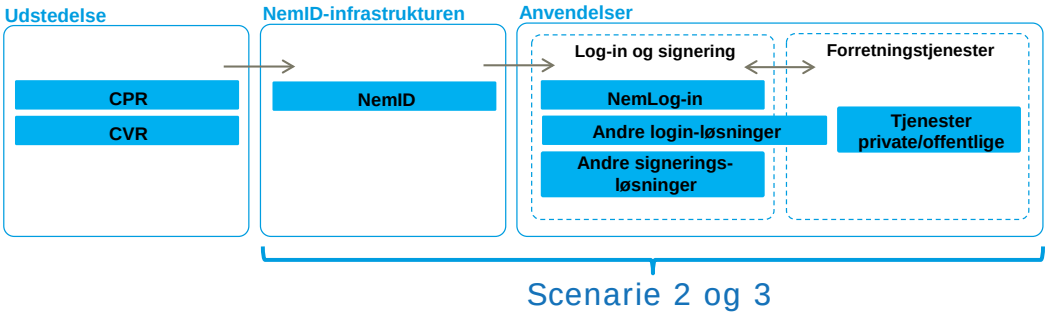


Scenarie 2 indebærer ændringer i NemID-økosystemet, som har konsekvenser for login- og signeringslaget, idet der her skal ske tilføjelse af rettighedsinformationstjenester og eventuelt ændringer i NemLog-in.

Desuden betyder indførelse af 1-faktor-login, at de tjenesteudbydere, der ønsker at implementere dette, skal gennemføre ændringer i egne tjenester.

Det samme gælder i forbindelse med udbredelse af NemID privat til erhvervsformål.

Figur 28: Konsekvenser af Scenarie 2 og 3 for NemID-økosystemet



Også Scenarie 3 har konsekvenser i hele NemID-økosystemet.

Interessenternes behov og ønsker har ikke kun vedrørt selve NemID, men også anvendelsen i tjenester og forbedringer i andre dele af NemID-økosystemet. Nogle af disse behov er behandlet i denne foranalyse, mens andre, fx vedrørende fuldmagter og rettigheder, er videreformidlet til andre parter.

Det forhold, at der indgår mange elementer og parter i det samlede NemID-økosystem, betyder, at gevinster som fx brugervenlighed er afhængig af, at flere parter gennemfører ændringer. Derfor skal det vurderes, om der er behov for styringsmæssige tiltag for at opnå de ønskede gevinster, fx i forbindelse med udarbejdelse af ny digitaliseringsstrategi.

En samlet vurdering af udgifter og gevinster i scenarierne viser, at Scenarie 1 vil have de mindste påvirkninger på både gevinst- og udgiftssiden i det samlede økosystem. De fællesoffentlige udgifter til løsningen forventes at være højere end til den nuværende løsning, da der er flere identiteter og transaktioner end forudsat i den nuværende kontrakt.

Scenarie 2 vil betyde et mindre tocifret millionbeløb i fællesoffentlig merudgift, mens der vil være gevinster i form af sparet tid for erhvervslivet og borgerne.

Scenarie 3 vil betyde fællesoffentlige merudgifter til især frikøb af erhvervssupport. Gevinsterne vil primært være større brugertilfredshed og tillid til løsningen.