Indholdsfortegnelse - Bilag

2.2 Migrationsstrategi i forbindelse med sikker udveksling af information på sundhedsområdet

SUNDHEDSDATA-STYRELSEN

Migrationsstrategi for migration fra DGWS til IDWS XUA

Indhold

Indledning

Dette notat beskriver en overordnet strategi for, hvordan Den Gode WebService (DGWS) kan udfases til fordel for den foreslåede IDWS XUA profil. Begge profiler fastlægger en national sikkerhedsmodel for webservice-kald fra en serviceaftager (fx et EPJ system) til serviceudbydere inden for sundhedsområdet (fx det Fælles Medicin-Kort).

Indledningsvis beskrives motivationen for at udfase DGWS, samt det arbejde der ligger til grund for denne beslutning. Herefter beskrives forskellene mellem DGWS og IDWS XUA sikkerhedsprofilerne. Herefter opstilles fordele og ulemper ved en lang kontra en kort migrationsfase og til sidst beskrives migrationsstrategien.

Sidst i notatet findes 7 appendices, som giver detaljer vedrørende migrationsmodeller på serviceudbyder- og serviceaftager-siden, roapmap for migrationsfasen, budget i den indledende fase samt erfaringstal for omkostninger i den efterfølgende fase. Endelig er der et appendiks vedr. fremtidig governance af profiler og understøttende værktøjer.

Motivation og baggrund

DGWS (Den Gode WebService) blev udviklet i 2005-2006. Profilen er implementeret i mere end 50 løsninger, og der foretages et stort antal kald af webservices baseret på denne profil. I december 2018 blev der alene på den nationale serviceplatform (NSP) foretaget mere end 100 mio. kald (svarende til ca. 2.000 i minuttet).

Da verden har ændret sig siden profilen blev udviklet, gav man den et "servicetjek" i 2013-2014 (det mellem parterne aftalte initiativ 3.4 i den "Nationale Strategi for Digitalisering af Sundhedsvæsenet 2013 – 2017 – Digitalisering med effekt"). Resultatet heraf fremgår af en analyserapport fra projektet "En analyse af sikkerhedsstandarder og løsninger" i 2014. Denne peger på, at DGWS sikkerhedsstandarden har 1) anvendelsesmæssige begrænsninger, 2) har sikkerhedsmæssige udfordringer og 3) manglende kompliance til standarder og markedet.

Anvendelsesbegrænsninger

1) DGWS understøtter kun system- og medarbejderadgang. Borgeradgang skal håndteres via andre sikkerhedsprotokoller, og det er dermed ikke muligt, at anvende samme sikkerhedsløsning på tværs af de gængse brugertyper indenfor sundhedsområdet.
2) DGWS er låst til et fast og begrænset attributindhold i det token (SOSI idkort) som udgør adgangsbilletten. Siden frigivelsen af DGWS standarden er der opstået en række nye adgangsgivende kriterier og denne udvikling forventes at fortsætte. DGWS understøtter fx ikke fuldmagt, bemyndigelse, samtykke, behandlingsrelation samt anonyme og pseudonyme identiteter.
3) DGWS bør ikke anvendes i usikre miljøer. Fx via det åbne internet eller på mobile platforme (se mere under sikkerhedsmæssige udfordringer)

Sikkerhedsmæssige udfordringer:

1) DGWS understøtter udelukkende SHA-1 (Secure Hash Algorithm 1), som kryptografisk hash algoritme. SHA-1 bliver af flere kryptografer ikke længere vurderet til at være sikker nok til fremtidig brug, og er ved at blive udfaset af mange aktører til fordel for de mere sikre algoritmer SHA-256 og SHA-512.
2) DGWS bør ikke anvendes i usikre miljøer, da tokenet (SOSI idkortet) ikke er-krypteret og ikke er bundet til anvendelseskonteksten. Adgangsbilletten er fx ikke bundet til konteksten af den patient, der skal hentes data på, den service-aftager der skal hente patientens data, eller den service-udbyder der har data. Derimod kan den som besidder eller opsnapper adgangsbilletten anvende denne, og derfor kan adgangsbilletten i praksis kun anvendes i kontrollerede miljøer, dvs. hvor der stoles på, at adgangsbilletten kun anvendes til den aftalte kontekst. I

praksis betyder ovenstående at DGWS kun bør anvendes indenfor Sundhedsdatanet.

Manglende kompliance til standarder og markedet:

1) DGWS er en proprietær standard målrettet det danske sundhedsområde, som ikke understøttes af internationale markedsprodukter og standard programmeringsbiblioteker. Som konsekvens bliver det relativt dyrt, at integrere DGWS til nationale og internationale markedsprodukter. Det bliver ligeledes besværligt for leverandører, der leverer løsninger til flere fagdomæner eller som foretager integrationer på tværs af fagdomæner.
2) Ligeledes opnås ringe synergi fra nationale og internationale fremskridt med standarder, protokoller, værktøjer, "best practice" og øvrig innovation. Denne udvikling drives og finansieres alene af den danske sundhedssektor

Den omtalte analyse fra 2014 pegede på, at udfordringer ved DGWS bedst afhjælpes via migration til en ny sikkerhedsprofil, som baseres på den fællesoffentlige OIO IDWS standard og den internationale IHE XUA standard. For at samle erfaringer med migreringsopgaven blev det foreslået at gennemføre en praktisk migrering af et regionalt system, et kommunalt system og et lægepraksissystem.

Som følge heraf blev der nedsat et **profilerings- og afprøvningsprojekt**, hvis formål har været at tilvejebringe og afprøve den nye IDWS XUA sikkerhedsprofil og afprøve denne i tre piloter. Denne afprøvning er del af den fællesoffentlige digitaliseringsstrategis initiativ 7.2 "Fælles standarder for sikker udveksling af information".

Profilerings- og afprøvningsprojektet blev opstartet i 2017 og forventes afsluttet i maj 2019. Projektet er opdelt i 6 spor:

1. Profileringssporet, hvor profilering af OIO IDWS og IHE XUA til sundhedsområdet udformes. Profilen, der hedder "IDWS XUA profilen", ligger pt. i en version 0.91
2. Værktøjssporet, hvor hjælpeværktøjer og vejledninger til profilen udformes. Der er hjælpeværktøjer til .Net og Java. Hjælpeværktøjerne bygger på en tilpasning af værktøjer, som Digitaliseringsstyrelsen fik udarbejdet til grunddataprogrammet.
3. NSP-sporet, hvor NSP infrastrukturen tilpasses den nye profil. Der er etableret en STS og en IdP, som understøtter den nye profil.
4. It-system-sporet, hvor pilot-systemer tilpasses til det nye profil. To serviceudbydere (Fælles Medicinkort og DokumentDelingsServicen) er opdateret med IDWS XUA grænseflader og tre serviceaftagere (piloter) integrerer med disse. En regional pilot som tilgår DDS, samt en kommunal og en lægepraksis pilot som tilgår FMK.
5. Afprøvningssporet, hvor de tre piloter afprøver forskellige adgangsscenarier og erfaringer opsamles
6. Evalueringssporet, hvor governancemodel, migrationsplan og beslutningsoplæg udarbejdes

IDWS XUA profilen forelægges RUSA mhp. optagelse i kataloget over standarder med status "anbefalet", når profilen er tilstrækkelig afprøvet og har været i offentlig høring.

Endvidere vil forslag til migreringsproces fra DGWS til IDWS/XUA profilen blive forelagt RUSA og Den Nationale Bestyrelse med henblik på at træffe beslutning om omlægning af eksisterende services og systemer.

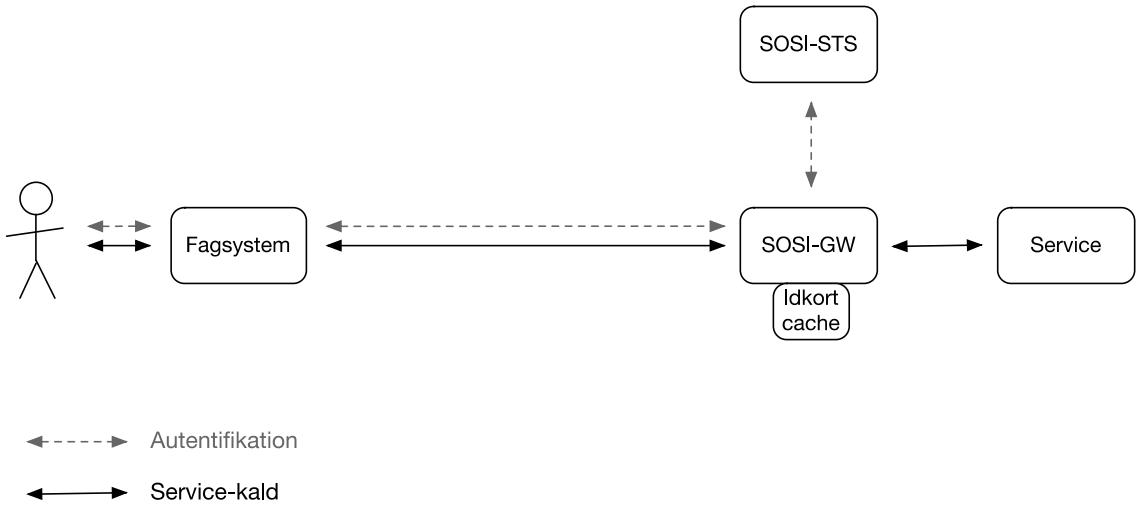
Forskelle mellem DGWS og IDWS XUA

Koncepterne bag DGWS og IDWS XUA ligner hinanden på væsentlige punkter. Begge profiler foreskriver, at brugeren af en service får adgang til denne ved at skaffe sig en adgangsbillet til servicen. Hvis serviceudbyderen kan verificere, at billetten kommer fra en billetudsteder, som serviceudbyderen har tillid til, da benyttes billettens oplysninger til at afgøre, om brugeren gives adgang til servicen.

DGWS konceptet

Men der er også væsentlige forskelle i koncepterne. I dag udstedes der en DGWS-billet til brugeren, når denne autentificerer sig hos SOSI-STS på den nationale serviceplatform ved hjælp af sin digitale medarbejdersignatur. Billetten kan bruges til alle nationale tjenester udstillet på serviceplatformen i indtil 24 timer. Såfremt DGWS-billetten opbevares sikkert, kan denne altså benyttes af brugeren til at få adgang til forskellige nationale tjenester gennem hele arbejdsdagen - uden at skulle logge på mere end en gang.

Opbevaringen af DGWS-billetten (også kaldet et SOSI-ID kort) kan ske i et fagsystem (serviceaftager) eller i en separat sikkerhedskomponent. Der er udviklet en fælles sikkerhedskomponent (SOSI-Gateway eller blot SOSI-GW), der opbevarer billetter og som vedhæfter disse, når der skal kommunikeres med en service. Dette er illustreret i nedenstående figur:

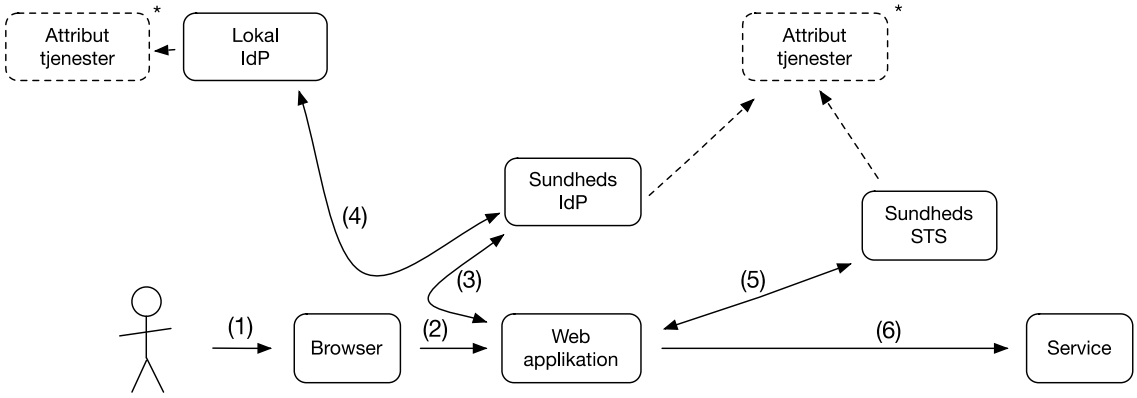


Figur 1: Eksempel DGWS integration

IDWS konceptet

I modsætning til DGWS anvendes i IDWS XUA to typer at tokens, nemlig såkaldte *bootstraptokens*, der udstedes til brugeren, når denne autentificerer sig (logger på), fx ved hjælp af en medarbejdersignatur, og *servicetokens*, der benyttes som adgangsbilletter til services. Bootstraptokens har som DGWS-tokens en relativ lang levetid, mens servicetokens har en ret kort levetid (f.eks. nogle minutter). Endvidere er servicetokens målrettet bestemte services. Bootstraptoken kan benyttes til at trække et servicetoken (hertil benyttes en STS (Security Token Service), der "omveksler" fra det ene til det andet). Skulle et servicetoken blive opsnappet af en uærlig part, vil det være begrænset, hvad tokenet vil kunne (mis-)bruges til og dette vil kun være muligt i en ganske kort periode.

I nedenstående figurer vises et af de mulige IDWS XUA anvendelsesscenarier, hvor en webapplikation får udstedt et bootstraptoken (3) fra en national sikkerhedskomponent, Sundheds-IdP (der i øvrigt her benytter en lokal sikkerhedskomponent/IdP til autentifikation), veksler dette bootstraptoken til et IDWS XUA token (5), der benyttes til at tilgå en service (6). Figuren viser også, at de enkelte tokenudstedere kan hente information fra forskellige autoriserede kilder (attributtjenester). Dette kan bl.a. benyttes ved omvekslinger, hvor oplysninger om brugers identitet (i et bootstraptoken), beriges med information om den pågældende brugers organisatoriske rolle eller sundhedsfaglige uddannelse og –autorisation, når der udstedes et service-token (5).



Figur 2: Eksempel IDWS integration

For en komplet oversigt over IDWS XUA anvendelsesscenarier henvises til 'Målarkitektur - identitetsbaserede serviceintegrationer på sundhedsområdet - v08'.

Teknisk set er der flere muligheder med IDWS XUA tokens (bootstraptokens og servicetokens) end der er med DGWS tokens (SOSI-IDkort). En udsteder af et IDWS XUA token kan kryptere indholdet af dette, så det kun er modtageren af tokenet, der kan læse det. Endvidere kan IDWS XUA tokens bindes kryptografisk til en webserviceaftager, således at det kun er denne, der kan benytte tokenet over for andre. Det kan således sikres, at et system, der modtager et bootstraptoken og servicetoken, er det eneste, der fremover kan benytte dette token til omvekslinger.

Infrastruktur

Forskellene i det tekniske koncept og design af DGWS og IDWS XUA afspejler forskellene i national infrastruktur på sundhedsområdet på det tidspunkt, hvor DGWS blev til og nu, hvor den nationale serviceplatform er udbredt (udbredelsen blev påbegyndt 2010). Før den nationale serviceplatform blev etableret, blev der kommunikeret med en centralt etableret sikkerhedskomponent (SOSI-STS), når brugeren skulle logge på / autentificere sig, og denne komponent udstedte et token/SOSI-ID kort, der blev opbevaret lokalt. Hvis den centrale sikkerhedskomponent var utilgængelig, kunne nye brugere ikke logge på, men alle, der havde logget på kunne fortsætte deres arbejde.

Som det fremgår ovenfor, kræver IDWS XUA hyppige tokenomvekslinger hos en tokenudsteder, som alle nationale services stoler på. Skulle man have forfulgt dette koncept tidligere, ville brugerne have været afhængige af, at en eksternt installeret sikkerhedskomponent ville være tilgængelig hele døgnet (da man ikke ville kunne kalde en service uden omveksling). Man kan altså sige, at behovet for sikkerhed omkring brugerens identitet og kontrollen med adgang til services er blevet balanceret med behovet for driftsstabilitet i DGWS.

Når man nu er klar til at styrke sikkerheden omkring identitet og adgang til services gennem hyppigere omvekslinger, sker det fordi den distribuerede NSP-infrastruktur muliggør lokale omvekslinger (man behøver således ikke at være afhængige af driftsstabilitet og performance af en ekstern sikkerhedskomponent).
Efter NSP infrastrukturen blev implementeret, blev SOSI-STS da også distribueret ud på de enkelte decentralt opstillede installationer af denne (med mulighed for fail-over på en ekstern/centralt opstillet NSP installation) for at højne tilgængeligheden af SOSI-STS. En ny STS (indeholdende omvekslingsfunktionalitet til IDWS XUA) vil ligeledes kunne distribueres på NSP installationerne.

Værktøjer

I forhold til understøttende værktøjer er der også sket ændringer. Da DGWS blev designet i 2005/2006 var der ikke samme understøttelse af webservices i standardværktøjer, som i dag. Derfor blev der udviklet en del kode i egne kodebiblioteker til Java og .NET platformene. I dag anvendes typisk standard rammeværk og kodebiblioteker i forbindelse med udvikling af- og integration til webservices, og det er uhensigtsmæssigt, at man ikke kan benytte samme værktøjer til udvikling af services og serviceintegrationer på sundhedsområdet. Faktisk overholder selve DGWS profilen ikke fuldt ud de underliggende internationale specifikationer (SAML, WS-Security), hvorfor det kan være svært at udvikle DGWS-løsninger i gennem anvendelse af standard-biblioteker out-of-the-box (disse standard-biblioteker er naturligvis tro mod internationale standarder).

IDWS XUA overholder i modsætning til DGWS profilen de underliggende internationale specifikationer og som en del af IDWS XUA afprøvningsprojektet, er der udviklet værktøjer og eksempler i Java og .NET, der bygger på standard rammeværk, som forventes at forankres i en fælles governance og support med Digitaliseringsstyrelsen.

Afkoblet fra autentifikationsmiddel og dermed forberedt på MitID

IDWS XUA profilens komplience til nationale og internationale standarder sikre en mere gennemtænkt og fremtidssikret profil, som gør det nemmere at leve op til eksisterende og kommende nationale, europæiske og internationale initiativer.
Her kan det fremhæves, at IDWS XUA profilen ikke stiller krav om, at et bestemt autentifikationsmiddel skal anvendes, modsat DGWS som afhænger af autentifikation via OCES certifikater. Der stiller kun krav om, at autentifikationsprocessen overholder et specificeret sikkerhedsniveau på NSIS-skalaen.
Afkobling til autentifikationsmiddel er på linje med kriterierne i det kommende MitID/NemLog-in3, hvor organisationer selv kan vælge og forvalte autentifikationsmidler for medarbejderne, samt foretage lokale autentifikationer i egne IdP'er. Organisationer kan i fremtiden kobles på den fællesoffentlige NemLog-in føderation ved at integrere deres egen lokale IdP til NemLog-in (under forudsætning af at NSIS kravene overholdes). I MitID behøver medarbejderautentifikationsmidler ikke nødvendigvis være OCES/PKI baserede.
Det forventes at flere organisationer indenfor sundhedsdomænet vil udnytte denne afkobling, og at IDWS XUA profilen dermed bliver en vigtig medspiller i transitionen til MitId. Det drejer sig både om store organisationer (regioner og kommuner), som får mulighed for at udfase en administrativ dyr OCES infrastruktur, men også små organisationer (lægepraksis), som udfordres at skærpede krav til udstedelse og opbevaring af autentifikationsbeviser.

En lang eller kort migrationsfases

En migrationsstrategi kan tage afsæt i enten en kort migreringsfase eller i en lang migreringsfase. Der vil være fordele og ulemper forbundet med begge typer strategier og de væsentligste er opstillet i nedenstående tabel.

	Lang migrationsfase	Kort migrationsfase
Økonomiske konsekvenser	**(Fordel)** Serviceaftagerne og -udbyderne kan skifte fra DGWS til IDWS, når det er mest fordelagtigt og ikke forsinker andre planlagte initiativer unødigt. Fx i forbindelse med øvrige opgraderinger, udbud, eller når der bliver behov for de forbedringer som den nye profil tilbyder. Den lange migrationsfase giver tid til at indarbejde migrationskravet i de fælles indkøbsaftaler (fx SKI). Det forventes derfor, at systemejerne kan opnå billigere og mere fordelagtige leverandøraftaler. **(Ulempe)** SDS skal igennem hele den lange migrationsfase drive og supportere DGWS standarder, værktøjer og infrastruktur samtidig med at skulle drive IDWS XUA infrastrukturen. Dette vil have ekstra omkostninger.	**(Ulempe)** Dette vil for mange af serviceaftagerne kræve, at de tilsidesætter andre prioriterede initiativer, samt laver ekstraordinære aftaler med deres leverandører vedr. migration. Som konsekvens heraf, må det forventes at migrationsudgiften bliver væsentlig højere. **(Fordel)** SDS kan slukke for DGWS infrastrukturen efter en kort migrationsfase.
Forretningsmæssige muligheder	**(Fordel)** Serviceaftagerne kan med en lang migrationsfase vente med at tage IDWS XUA i brug før der er forretningsmæssige gevinster forbundet hermed. Det kunne eksempelvis være, hvis serviceaftagersystemet integreres til andre services (måske baseret på IDWS fordi man ønsker en borgeradgang eller fordi der er krav til IHE XUA understøttelse) og dette sker via standardværktøjer. For en leverandør, der skal vedligeholde løsningen vil det være en fordel at håndtere webserviceintegrationer ensartet.	**(Ulempe)** Bortset fra, at der fjernes en sikkerhedsmæssig sårbarhed ved den nuværende kommunikation (og denne kunne fjernes på anden vis med en mindre indsats), er der ingen forretningsmæssige gevinster ved at ombygge et gammelt velfungerende system til at kunne det samme med en ny protokol.
Sikkerhedsmæssig konsekvens	**(Ulempe)** DGWS understøtter udelukkende SHA-1 til såkaldt hashing. Denne algoritme vurderes ikke sikker nok af flere kryptografer. Trusselen er er her, at tokenindhold kan manipuleres. DGWS tokens er bredt anvendelige og har en lang levetid. Hvis token opsnappes, vil konsekvensen heraf være relativ stor. Grundet begrænsninger af DGWS, er der i dag implementeret løsninger, der håndterer sikkerhedsmæssige aspekter på en egen måde og hvor sikkerheden afhænger af hvordan forskellige systemer og netværksinfrastruktur	**(Fordel)** De sikkerhedsmæssige svagheder ved DGWS udfases hurtigere. IDWS honorerer tidssvarende krav til sikkerhed, herunder brugen af nyere kryptografiske algoritmer. Fremover vil det også være lettere at gå over til nye kryptografiske algoritmer, da profilen er fleksibel i forhold til anvendelsen af disse. Sikkerheden vil også hæves ved at tage nye sikkerhedsmæssige muligheder i brug, f.eks. at beskytte følsomt indhold i adgangsbilletten via kryptering eller at binde adgangsbilletten til anvendelseskonteksten (dvs. at sikre, at adgangsbilletten kun anvendes på en bestemt patient, via

	håndterer beskeder. Fx overførers oplysninger om, hvem der arbejder på vegne af hvem, udenfor sikkerhedstokens til FMK så det er op til netværksforbindelserne at sikre, at disse oplysninger ikke kan manipuleres. Tilsvarende er gældende for oplysninger om brugskontekst og patientkontekst i forbindelse med sikker browseropstart. Truslen vurderes lille så længe de netværk og de systemer, der indgår i kommunikationen, sikrer integritet og konfidentialitet af beskeder og tokens. Over en lang migrationsfase kan der blive behov for at iværksætte styrkende foranstaltninger: -Enten ved at udfase SHA-1 algoritmen og dermed revidere DGWS profilen. Erfaringer fra en lignende øvelse fra NemId viser, at dette kræver en større indsats, da ældre kodebiblioteker ofte ikke understøtter SHA-256 og SHA-512 -Eller ved at stramme op på kontrollen, og dermed de processer som sikrer, at aftagerne, serviceudbydere og netværksejere har styr på deres administrative og driftsmæssige rutiner.	kald fra en bestemt service-aftager til en bestemt service-udbyder). Endelig kan der opereres med kortlevede adgangsbilletter uden at dette kræver hyppige re-logins af brugeren. Alt dette reducerer sikkerhedsrisikoen forbundet med, at adgangsbilletten opsnappes og anvendes på falsk grundlag.

Den korte migrationsfase vurderes at være svær at realisere, primært fordi det pålægger de involverede parter, at de tilsidesætter andre prioriterede initiativer samt laver ekstraordinære aftaler med deres leverandører om at gennemføre migrationen.

De omkostninger det har at drive og supportere to infrastrukturer vurderes at være relativt beskedne sammenlignet med omkostningerne til omlægning af systemer. Endvidere vurderes, at de tiltag der evt. skal iværksættes for at opretholde en tilfredsstillende sikkerhed gennem en længere migreringsperiode at være begrænsede.

På baggrund af ovenstående vurderes det, at en lang migreringsfase vil være at foretrække. Nedenfor udstikkes en overordnet plan for realisering af den lange migrationsfase.

Migrationsstrategi – lang migrationsfase

Migrationsstrategien udstikker en **overordnet plan**, som skal realisere det **strategiske mål** om at udfase DGWS til fordel for IDWS XUA profilen. Udfasningen vedrører kun eksterne integrationer fra en sundhedsorganisation til en national service indenfor sundhedsområdet. Dvs. brug af DGWS i forbindelse med interne integrationer indenfor en organisation er ikke omfattet af strategien.

Strategien skal senere følges op af en eller flere migrationsplan(er), som kommer med deltaljer vedr. migration af den enkelte serviceudbyder og serviceaftager.

Strategien nedbrydes i tre migrationsområder:

1. Sikkerhedsinfrastruktur (STS og sundheds-IdP), hjælpeværktøjer (.NET og Java) og tilslutningsaftaler
2. Nationale serviceudbydere inden for sundhedsområdet (fx FMK og DDS)
3. Serviceaftager inden for sundhedsområdet (fx regioner, kommuner og LPS'er)

Den overordnede strategiske plan fremgår af boksen nedenfor.

- Der foretages ikke større ændringer i DGWS og den infrastruktur der understøtter denne. Det kan betyde, at andre tiltag (f.eks. adgang til nationale tjenester baseret på lokal autentifikation) først kan gennemføres efter migrering til IDWS/XUA.
- For nye nationale services på sundhedsområdet er det strategien, at disse udelukkende udstilles via IDWS XUA grænseflader, da de aldrig tideligere har været tilgængelige via DGWS og dermed ikke påvirker eksisterende integrationer.
- Eksisterende nationale serviceudbydere tilbydes opkobling til NSP, hvor der udvikles proxyservice(s), der mapper fra IDWS XUA til DGWS. Proxyservices udfases ved migrationsperiodens afslutning og serviceudbydere skal derfor selv skabe IDWS-snitflader inden migrationsperiodens udløb. Tilsvarende skal en DGWS snitflade opretholdes indtil det sidste anvendersystem migreres. Serviceudbydere, der ikke ønsker udstilling via NSP-proxyservices skal etablere en IDWS-XUA snitflade indenfor en kort periode (f.eks. 1.5 år).
- "Serviceaftagerne indenfor sundhedsområdet" får en lang tidsfrist (f.eks. 6 år) og dermed optimale betingelser til at planlægge og gennemføre at skriftet fra DGWS til IDWS.

Nedenfor udfoldes den strategiske plan for de tre migrationsområder.

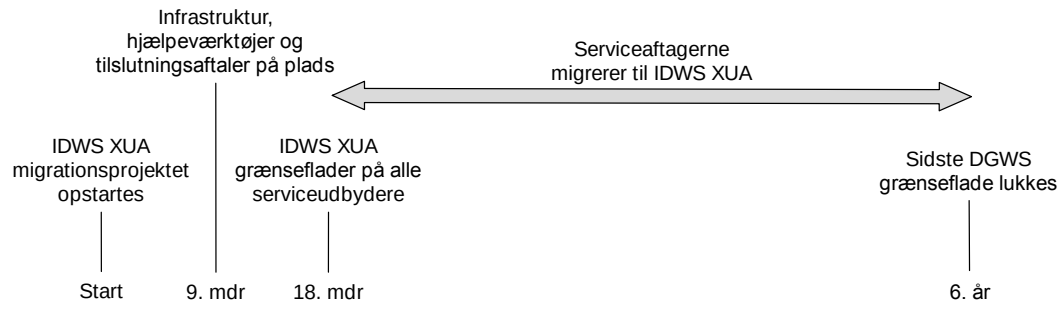
Sikkerhedsinfrastruktur, hjælpeværktøjer og tilslutningsaftaler skal etableres inden IDWS XUA profilen kan overgå til "produktion". Hovedparten af dette er allerede etableret i forbindelse med profilerings- og afprøvningsprojektet. Det udestår dog at få udarbejdet de formelle tilslutningsaftaler, som skal indgås mellem anvenderne af sikkerhedsinfrastrukturen. Endeligt vil der ligge et arbejde med at gøre sikkerhedsinfrastruktur feature-komplet og produktionsmoden. Det forventes, at ovenstående kan etableres indenfor en periode på et halvt år. Profilerings og afprøvningsprojektet vil levere yderligere materiale, der kan kvalificere dette.

De eksisterende **nationale serviceudbydere** som udstiller DGWS snitflader omfatter DokumentDelingsServicen (DDS), Fælles MedicinKort (FMK), Det Danske Vaccinationsregister (DDV), Tilskudsansøgningsservicen (TAS), Fødselsindberetningsservice (FIBS), Bivirkningsindberetning (BivWS), Dødsårsagsregister - Indberetningsservice

(SEI), Indberetning til Landspatienregisteret (LPR3), Henvisningshotellet, Medcom lægeblanket og støtteservices som National Adviseringsservice (NAS), BehandlingsRelationsService (BRS), Bemyndigelsesservice (BEM), Samtykkeservicen SAMT, MinLog, Stamdatamodul (SDM).
Det er strategien, at alle eksisterende serviceudbydere skal kunne tilgås via både den gamle DGWS og den nye IDWS XUA grænsefalde over en længere migrationsfase. Mere information om, hvordan en serviceudbyder kan bringes til at udstille DGWS og IDWS XUA samtidig findes i "Appendiks 1. Migration af udbydersiden"
Det forventes, at der kan etableres IDWS XUA grænseflader til alle DGWS serviceudbydere indenfor et år.
Nye nationale services på sundhedsområdet skal udelukkende udstilles via IDWS XUA grænseflader, da de aldrig tideligere har været tilgængelige via DGWS og dermed ikke påvirker eksisterende integrationer. Der vil være situationer, hvor det er en vurderingssag om eksisterende integrationer påvirkes eller ej. Fx ved en ny grænsefalde til en eksisterende service, som ikke erstatter den eksisterende DGWS grænseflade.

Serviceaftagere inden for sundhedsområdet er bl.a. regioner, kommuner, LPS, apotekere og Sundhed.dk. Aftagerne får en lang migrationsfase, således at serviceaftagerne kan skifte fra DGWS til IDWS, når det er mest fordelagtigt og ikke forsinker andre initiativer unødigt. Fx i forbindelse med øvrig opgradering, udbud, eller når der bliver behov for de forbedringer som den nye profil tilbyder. Det er dog vigtigt at migrationsfasen ikke bliver så lang, at serviceaftagerne udskyder deres interne migrationsplanlægning. Migrationsfasen bør heller ikke overskride den forventede holdbarhedstid for målarkitekturen. På baggrund af dialog med serviceaftagerne vurderes det, at en migrationsfase på 6 år er passende. Det skal dog nævnes at denne dialog stadig pågår.

Nedenfor illustreres den overordnede tidsplan for migrationen fra DGWS til IDWS XUA.

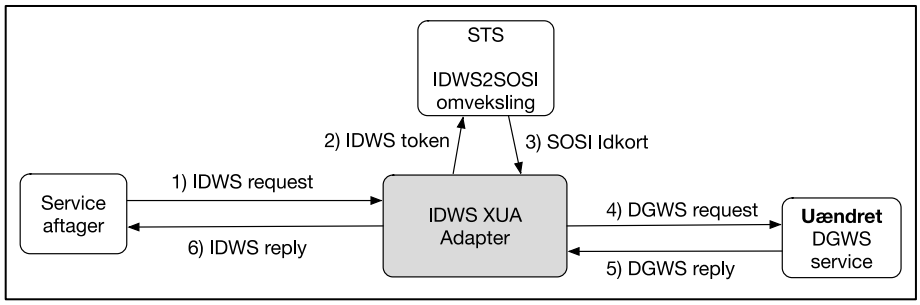


Figur 3: Tidsplan for migration til IDWS XUA

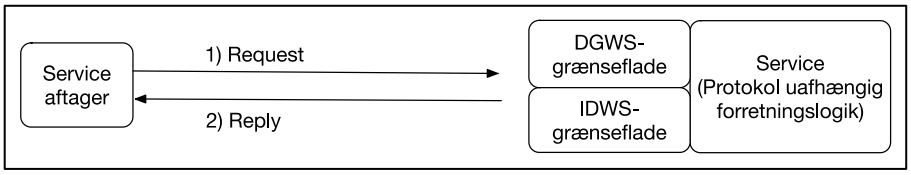
Appendiks 1. Migration af udbydersiden

Nedenfor skitseres tre generelle løsningsmodeller for, hvordan en serviceudbyder kan bringes til at udstille både en DGWS og en IDWS XUA grænseflade.

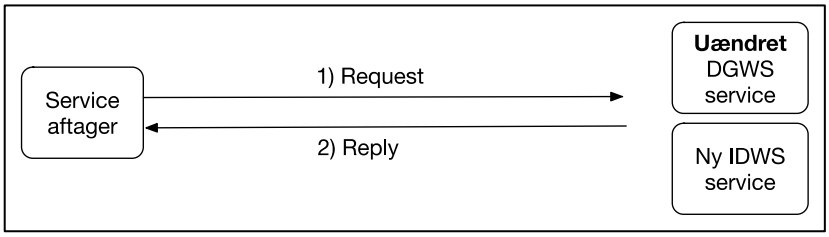
1. **IDWS XUA adapter**: Kan transformere indkommende beskeder fra IDWS til DGWS og udgående svar fra IDWS til DGWS. Fordelen ved adapter-modellen er, at DGWS servicen forbliver uændret. Det forventes, at adapteren kan etableres som en generisk komponent, der kan genbruges af alle serviceudbydere.



2. **Adskilt protokolhåndtering:** Kan anvendes af services som har isoleret sikkerhedsprotokol-håndtering fra selve forretningslogikken. Herved kan nye protokoller nemt indføres. Denne model anvendes for de services, som allerede har isoleret sikkerhedsprotokol-håndtering eller for services, hvor investeringen vurderes relevant.



3. **Dublet-service:** Den eksisterende DGWS service forbliver uændret og en tilsvarende IDWS XUA snitflade etableres som en ny service.



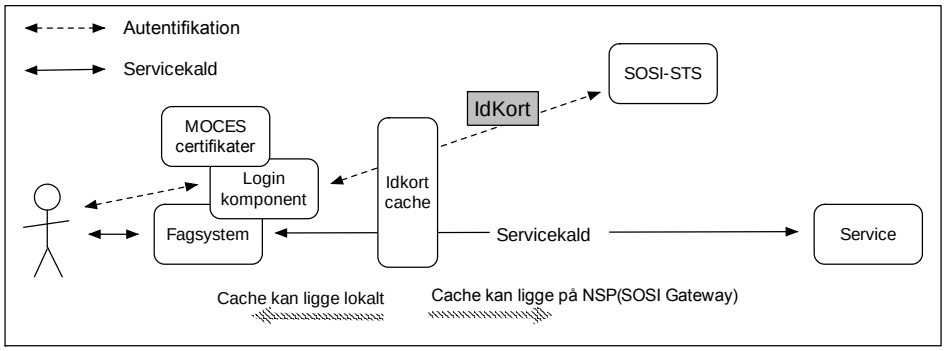
Der vil også kunne anvendes en kombination af ovenstående. Fx en IDWS XUA adapter som en midlertidig og billig løsning, og en af de to andre modeller på længere sigt.

FMK og DDS er via pilotprojekterne allerede i gang med at etablere IDWS grænseflader via ”Adskilt protokolhåndtering” løsningsmodellen. Alle de andre serviceudbydere vil kunne anvende adapter-modellen midlertidig og forventelig være på plads med denne indenfor et år. Herefter kan det for den enkelte serviceudbyder overvejes, om en mere permanent løsning i form af ”Adskilt protokolhåndtering” eller ”Dublet-service” skal implementeres.

Appendiks 2. Migration af aftagersiden

På Figur 4 illustreres AS-IS DGWS integrationsmodellen fra et fagsystem til en national serviceudbyder indenfor sundhedsområdet. Der er to trin i integrationen:

1) Udstedelse af SOSI Idkort via SOSI STS'en (NSP komponent). Medarbejder certifikat (MOCES) anvendes til signering af SOSI Idkort i forbindelse med udstedelsesprocessen. Det udstedte SOSI IdKort er gyldig i 24 timer og kan genanvendes hen over en typisk arbejdsdag.
2) Kald fra fagsystem til en DGWS beskyttet national service indenfor sundhedsområdet. Idkortet medsendes fra fagsystem til den nationale service via Idkort-cachen.



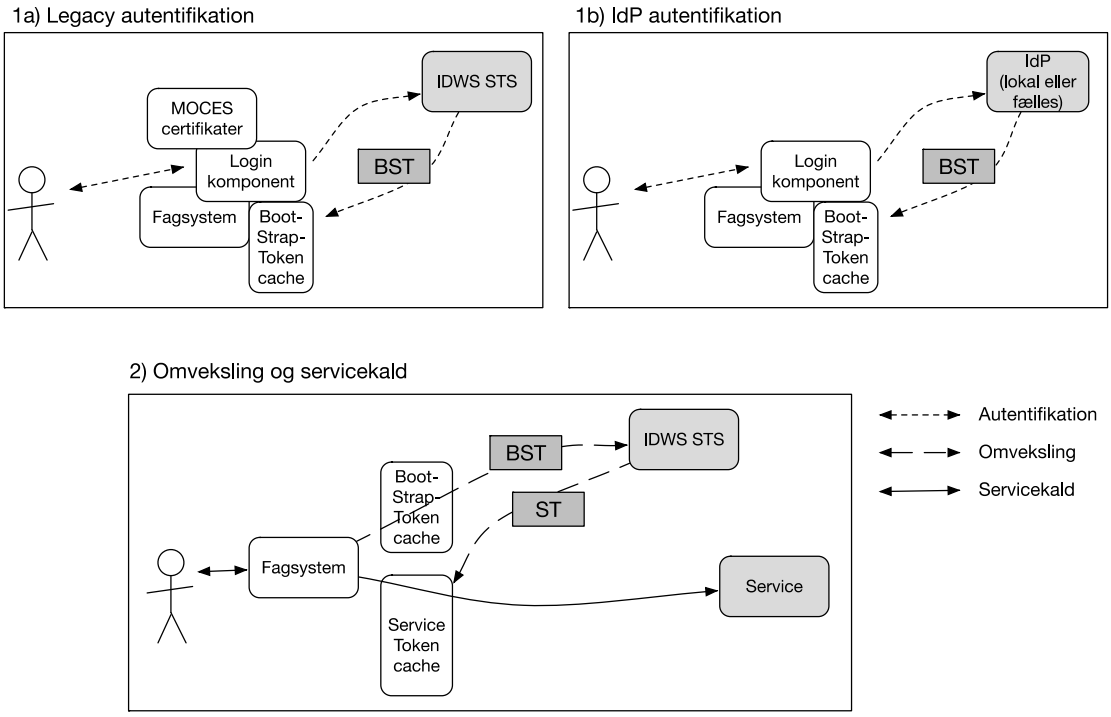
Figur 4: AS-IS DGWS aftager-integration

På figuren er fagsystem, loginkomponent, MOCES certifikater og Idkort-cache nedbrudt i fire adskilte logiske komponenter. I store organisationer, som regioner og kommuner, er denne logisk nedbrydning ofte realiseret via fysiske adskilte komponenter, således af flere fagsystemer kan anvende samme autentifikationsfunktionalitet. Eksempler på dette er opbevaring af MOCES signaturer i SignaturCentralen, håndtering af SOSI Idkort udstedelse i forlængelse af brugerens domæne-login ved arbejdsdagens begyndelse og opbevaring af SOSI Idkort på NSP SOSI Gateway'en.

I de fleste mindre organisationer, som fx lægepraksisser, håndteres hele autentifikationsfunktionalitet ofte indenfor fagsystemet og dermed ikke i fysisk afskilte komponenter. SOSI Idkortet udstedes når brugeren logger på fagsystemet og opbevares i en Idkort-cache tilknyttet til fagsystemet.

På **Fejl! Henvisningskilde ikke fundet.** illustreres TO-BE IDWS XUA integration fra t fagsystem til en national serviceudbyder indenfor sundhedsområdet. Der er tre trin i integrationsprocessen:

1. Udstedelse af et autentifikationsbevis (BootStrapToken (BST))
2. Omveksling til servicetoken
3. Kald af national service indenfor sundhedsområdet



Figur 5: TO-BE IDWS XUA aftager-integration

IDWS XUA infrastrukturen understøtter to modeller til udstedelse af autentifikationsbevis.

- 1a) Legacy autentifikation: Modellen ligger tæt op ad den eksisterende DGWS metode til udstedelse af SOSI Idkort. Først signeres et IDWS autentifikationstoken med brugerens signatur. Efterfølgende kaldes IDWS STS'ens autentifikationssnitflade med det brugersignerede token, og ved succesfuld validering returneres et STS signeret BootStrapToken(BST).
- 1b) IdP autentifikation: Modellen anvender en standard SAML IdentitetsProvider (IdP) til udstedelse af et BST. Brugeres browser redirectes til en IdP, som håndterer brugerautentifikation. Autentifikationsmekanismen skal ikke nødvendigvis være MOCES baseret, med skal dog leve op til et passende NSIS sikkerhedsniveau (National Standard for Identiteters Sikringsniveauer). IdP komponenten kan være placeret lokalt i organisationen eller være en fælles IdP (fx NemLog-in)

Gyldighedsperioden for et BST svarer til en arbejdsdag. BST'et bør derfor gemmes og genbruges via en lokal tilknyttet cache. I modsætning til SOSI infrastrukturen, så tilbyder IDWS XUA infrastrukturen ingen fælles NSP komponent til caching af BST's.

Bootstraptokenet skal omveksles til et ServiceToken (ST) i forbindelse med kald af en national service indenfor sundhedsområdet. Et ST har kort levetid og er bundet til kaldskonteksten. At være bundet til kaldskonteksten betyder, at tokenet kun kan anvendes af en bestemt bruger via et bestemt fagsystem, til at tilgå data for en bestemt patient via en

bestemt nationale service. Hvis en af de fire kontekstparametre ændres, så skal der omveksles til et nyt ST. ST'et bør også caches lokalt, så det kan genanvendes, hvis der er behov for flere servicekald indenfor den samme kaldskontekst. Fx flere kald til FMK på samme patient fra samme bruger via samme fagsystem.

Til IDWS XUA profilen er der etableret hjælpeværktøjer i form af kodebiblioteker, som gør det nemt at udstede BST, omveksle til ST samt kalder nationale services via IDWS XUA profilen. Værktøjerne er udviklet til .NET og Java platformene og virker "out-of-the-box".

Appendiks 3: Planlagt migrationsmodel pr. national service

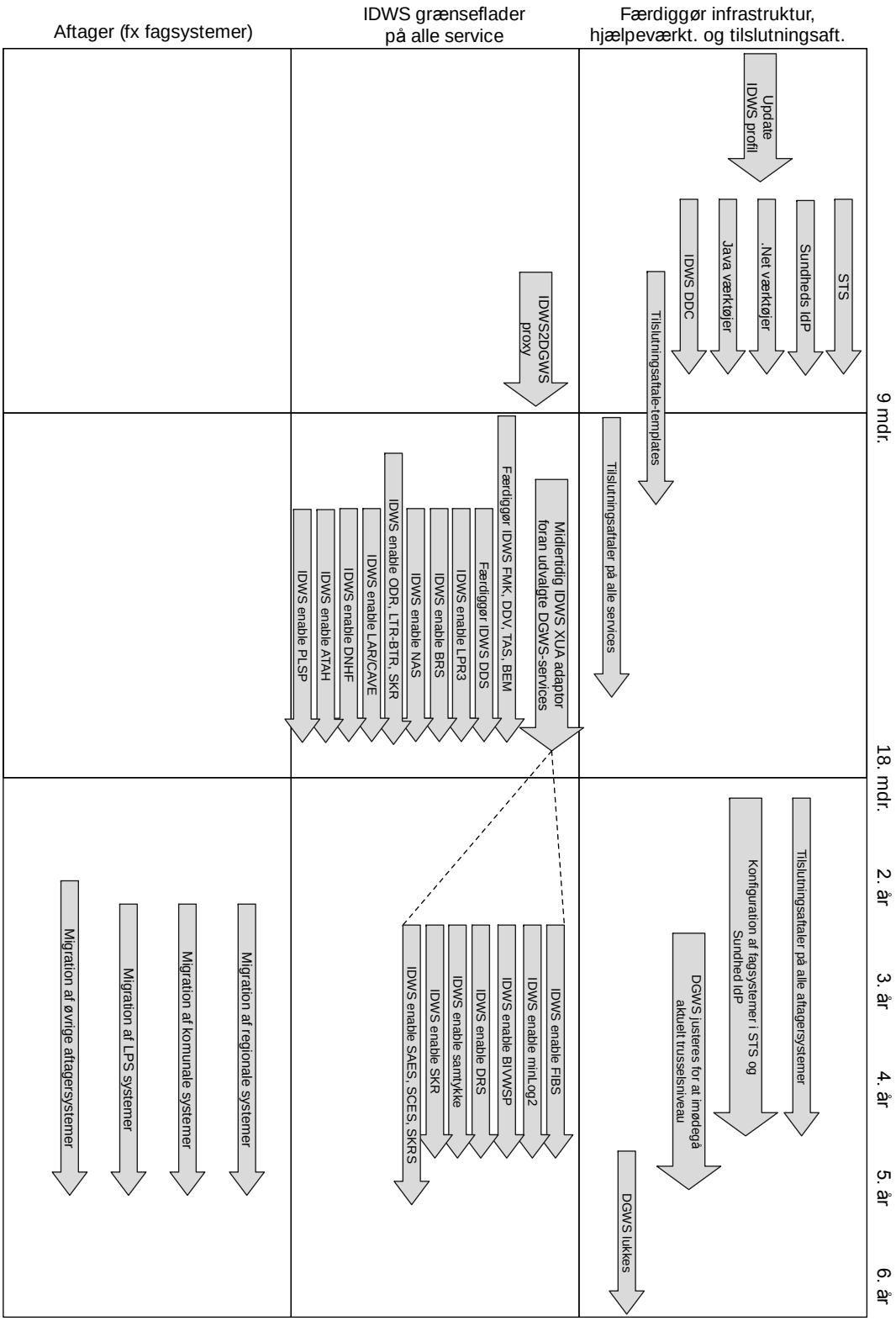
Nedenfor listes alle nationale services som skal migreres fra DGWS til IDWS XUA profilen. For hver service markeres: 1) om servicen driftes på NSP, NSP backoffice eller hos en anden part, 2) om servicen har DGWS medarbejder- og/eller system-snitflader, 3) om servicen har en borger-snitflade baseret på den eksisterende fællesoffentlige OIO IDWS 1.0, 4) hvilken IDWS XUA migrationsmodel (se appendiks 1) der planlægges på kort og langt sigt, og 5) bemærkning vedrørende servicen, herunder eksisterende planer med servicen (uafhængig af IDWS XUA planerne). Som udgangspunkt planlægges der med "IDWS XUA adapter" migrationsmodellen for alle services på kort sigt og "Adskilt protokolhåndtering" på langt sigt. Der er dog services, hvor det vurderes, at det kræver en lille indsat at implementere "Adskilt protokolhåndtering" på kort sigt, eller der er planlagt andre udviklingsinitiativer og "Adskilt protokolhåndtering" medtages i samme omgang.

Service	På NSP, NSP backoffice eller hos en anden part?	DGWS medarbejder-snitflade?	DGWS system snitflade?	IDWS 1.0 borger snitflade?	IDWS XUA Migrationsmodel på kort sigt	IDWS XUA Migrationsmodel på langt sigt	Bemærkning vedr. service og herunder eksisterende planer med service (uafhængig af IDWS XUA planerne)
Stamdata Autorisation Enkeltopslagsservice (SAES)	NSP	Nej	Ja	Nej	IDWS XUA adapter	Adskilt protokolhåndtering	Udvikling af ny importerframework (ikke DGWS) skal i udbud
Stamdata CPR Enkeltopslagsservice (SCES)	NSP	Nej	Ja	Nej	IDWS XUA adapter	Adskilt protokolhåndtering	Udvikling af ny importerframework (ikke DGWS) skal i udbud
Stamdata Kopiregisterservice (SKRS)	NSP	Nej	Ja	Nej	IDWS XUA adapter	Adskilt protokolhåndtering	Udvikling af ny importerframework (ikke DGWS) skal i udbud
Behandlingsrelationservice (BRS)	NSP	Nej	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Interface og forretningslogik ændringer (ikke sat i gang), så SOR understøttes, herunder konvertering fra Shak til SOR. Nye importere af LPR3 (er sat i gang)
Minlog Registration	NSP	Nej	Ja	Nej	IDWS XUA adapter	Adskilt protokolhåndtering	Skiftes til Minlog2 i år. EPJ systemer skal på sigt tilgå MinLog, hvilket kan resultere i opdateringer til MinLog medio 2020
Minlog Webservice/Lookup	NSP-BO	Nej	Ja	Nej	IDWS XUA adapter	Adskilt protokolhåndtering	Anvendes pt. af sundhed.dk og FMK-online
Fødselsindberetningsservice (FIBS)	NSP-BO	Nej	Ja	Nej	IDWS XUA adapter	Dublet-service	Implementeret som proxy med protokol- og format-transformation
National Adviseringsservice (NAS)	NSP-BO	Ja	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Reimplementeres pt. Laves så forretningslogik og sikkerhedsprotokol pænt opsplittes
BivirkningsWebServiceProxy (BIVWSP)	NSP-BO	Nej	Ja	Nej	IDWS XUA adapter	Dublet-service	Implementeret som proxy ovenpå grænseflade fra internationalt agentur. Proxy indeholder protokol- og format-transformation
Dokumentdelingsservice (DDS)	NSP-BO	Ja	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Del af IDWS XUA projektet. Men føres ikke helt til mål indenfor projektet

Dokumentregistreringsservice (DRS)	NSP-BO	Nej	Ja	Nej	IDWS XUA adapter	Adskilt protokolhåndtering	Implementeret som proxy ovenpå IHE standard grænseflader. Proxy indeholder protokol- og formattransformation. Anvendes til provide&registre for aftale repository.
Organdonorregister (ODR)	NSP-BO	Ja	Nej	Ja	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Servicen har en foranstillet proxy (der kan håndtere både DGWS og OIOIDWS) og som er planlagt til at blive erstattet af NSP handlers.
Livs- og behandlingstestamenteregister (LTR-BTR)	NSP-BO	Ja	Nej	Ja	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Servicen har en foranstillet proxy (der kan håndtere både DGWS og OIOIDWS) og som er planlagt til at blive erstattet af NSP handlers.
Stamkortregister (SKR)	NSP-BO	Ja	Ja	Ja	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Servicen har en foranstillet proxy (der kan håndtere både DGWS og OIOIDWS) og som er planlagt til at blive erstattet af NSP handlers.
Samtykkeservice - verifikation	NSP-BO	Ja	Ja	Nej	ingen migration	IDWS XUA only	Anvendes pt. kun fra DDS. Men der er planer om at andre også skal have adgang til servicen. Kan evt. udstilles som IDWS XUA only grænseflade
Samtykkeservice - administration	NSP-BO	Ja	Ja	Nej	ingen migration	IDWS XUA only	Anvendes pt. kun af sundhed.dk. Kan evt. udstilles som IDWS XUA only grænseflade
LAR/Cave (på vej)	NSP-BO?	Ja	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Designet mhp. at der kommer IDWS snitflade. Laver primært protokol og format konvertering. FHIR service med DGWS proxy på.
Bemyndigelsesmodul (BEM)	NSP-BO?	Ja	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Administrationssnitflade som er åben og kaldes af eksterne. Opslag kun FMK. IDWS XUA koncept fra FMK kan genbruges
Fælles MedicinKort (FMK)	anden part	Ja	Ja	Ja	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Del af IDWS XUA projektet, hvor en version af FMK grænsefladerne nu håndtere IDWS XUA
Det Danske Vaccinationsregister (DDV)	anden part	Ja	Nej	Ja	Adskilt protokolhåndtering	Adskilt protokolhåndtering	IDWS XUA koncept fra FMK kan genbruges
Tilskudsansøgningsservicen (TAS)	anden part	Ja	Nej	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	IDWS XUA koncept fra FMK kan genbruges
Landspatientregisteret (LPR3)	anden part	Nej	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	LPR har en række snitflader og kun en af disse understøtter DGWS. Der er en ITI-41 (provide&register) XDR-snitflade, som er baseret på SOAP 1.2 og "DGWS" (idkort + medcom header, men netop ikke SOAP 1.1). Snitfladen kræver STS-signerede systemidkort. Protokol-håndtering er afkoblet fra forretningslogikken og etablering af parallel IDWS XUA indgang er vurderet til en begrænset opgave.
Den nye henvisningsformidling (DNHF)	anden part	Nej	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	"Servicen har udelukkende systemsnitflader, som skal kaldes af regionale systemer, LPS'er, Praksys og Sundhed.dk (for borgere med trust). Adgang fra MinLæge app'en udestår (fase 2 aktivitet), men forventes at følge trust-modellen med systemidkort. CGI vurderer etablering af en seperat IDWS snitflade umiddelbart som en mindre udviklingsopgave "

Sundhedsdata-styrelsens Elektroniske Indberetningssystem (SEI2)	anden part	Nej	Nej	Nej	*Under udredning*	*Under udredning*	Under udredning
Beslutnigsstøttesystem (ATAH)	anden part	Nej	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	Servicen er en ren beregningsmaskine, der kan modtage inputparametre (ingen patient-ID'er) og generer output i form af anbefalinger til medicinering. Servicen har en REST + JSON baseret snitflade, hvor adgangsstyring foregår via klient-certifikat whitelisting. DGWS snitfladen er lavet som ren indpakning af REST-snitfladen med mapning fra XML til JSON. Servicen er ved at blive afprøvet i et pilotprojekt af en række aktører. Der overvejes nu om DGWS snitfladen overhovedet skal bibeholdes og ibrugtages, i og med der er tale om et helt nyt system kunne der med fordel anvendes IDWS (for SOAP snitfladen).
Primærsektorens Leverandør Service Platform (PLSP)	anden part	Ja	Ja	Nej	Adskilt protokolhåndtering	Adskilt protokolhåndtering	PLSP platformen udstiller pt. følgende services: Service til Min-Læge, forløbsplaner og API til LPS'er (til at lægge data på platforme) - men forventes udvidet med flere tjenester på sigt. I alle tre services er sikkerhedsprotokollen adskilt fra forretningslogikken, og der vurderes at etablering af en parallel IDWS snitflade vil være en overkommelig opgave

Appendiks 4: Roadmap figur



Appendiks 5: Budget for de første 18 mdr.

Nedenfor opstilles det forventede budget for de første 18 mdr. Dvs. faserne som er markeret med blå baggrund på roadmap'et i appendiks 4 og som vedrører færdiggørelse af infrastruktur og hjælpeværktøjer, opsætning af IDWS XUA grænseflader på alle services, pilotprojekter, samt udgifter til ledelse, udarbejdelse af DPIA og tilslutningsaftaler.
De enkelte budgetposter er estimeret ud fra en forudgående dialog med de enkelte leverandører samt erfaringer opsamlet undervejs i projektet. Der er spurgt ind til leverandørernes IT-arkitektur, men henblik på at forstå hvordan den konkrete opgave løses og kompleksiteten i dette. Det er desuden undersøgt om de enkelte leverancer kan kædes sammen med andre planlagte aktiviteter og dermed laves billigere. Enkelte leverandører har desuden uforpligtigende angivet deres forventning til omfang og udgift. Det er klart at de enkelte budgetposter derfor er forbundet med en vis usikkerhed, men det er samtidig urealistik at bede de enkelte leverandører om præcise estimater på dette tidspunkt i processen.
Den sidste kolonne i tabellen angiver hvem der forventes at afvikle udgiften. K=konsulentfirma, U.L.=udviklingsleverandøren, D.L.=driftsleverandøren og SDS=Sundhedsdatastyrelsen.

Færdiggør infrastruktur og hjælpeværktøjer	**Udgift**	**Hvem afvikler**
Ajourfør IDWS XUA profil	100.000	K
STS færdigudvikling og produktionsmodning	500.000	U.L.
Sundheds IdP (lokal kontekst i BST)	100.000	U.L.
.Net og Java værktøjer (udvikling og support)	300.000	U.L.
DCC klargjort til IDWS (SOAP1.2 og url-routning)	150.000	U.L.
Tilpas SEAL Java så det kan koeksisterer med IDWS XUA Java hjælpeværktøj	200.000	U.L.
Kom i gang guides: Anvenderrettet dokumentation, kodeeksempler og tilhørende testdata	300.000	K
I alt	**1.650.000**	
IDWS grænsefalder på alle service (på kort sigt)		
Implementering af IDWS XUA adapter (IDWS2DGWS)	500.000	U.L.
Opsætning og test af services på IDWS XUA adapter. Dvs. de ca. 7-9 services som på kort sigt opsættes med IDWS XUA adapter, samt efterfølgende test via generisk testklient. Udvikling af testklient er inkluderet i estimatet.	500.000	D.L.
Adskilt protokol håndtering for FMK, DDV, TAS og BEM	600.000	U.L.
Adskilt protokol håndtering for DDS	400.000	U.L.
Adskilt protokol håndtering for LPR3	300.000	U.L.
Adskilt protokol håndtering for BRS	200.000	U.L.
Adskilt protokol håndtering for NAS	200.000	U.L.
Adskilt protokol håndtering for ODR, LTR-BTR, SKR	300.000	U.L.
Adskilt protokol håndtering for LAR/CAVE	200.000	U.L.
Adskilt protokol håndtering for DNHF	200.000	U.L.
Adskilt protokol håndtering for ATAH	200.000	U.L.
Adskilt protokol håndtering for PLSP	200.000	U.L.
Øget udgifter til teknisk support i forbindelse med migreringsfasen. 500.000 kr. per år. Her kun medtaget et års support	500.000	D.L.
I alt	**4.300.000**	

Øvrige udgifter		
Projektledelse	1.000.000	K eller SDS
Udarbejdelse af tilslutningsaftaler, DPIA mm.	400.000	SDS (Jurist)
Kvalitetssikring og afprøvning og efterfølgende tilretning, når nye services tages i brug.	2.000.000	U.L.
I alt	**3.400.000**	
Budget i alt	**9.350.000**	

Bemærk: Når de præcise planer for overgang til nemID forligger, så kan det afføde yderligere behov, som ikke er afdækket på nuværende tidspunkt.

Appendiks 6: Erfaringstal og fagsystemer

I det følgende redegøres for det timeforbrug, som de enkelte pilotprojektleverandører har estimeret, der skal anvendes ved migration fra DGWS-grænseflader til IDWS XUA grænseflader.

Migrations af LPS
Når hele IDWS XUA konceptet er modent og fejlfrit, så vurderer lægepraksis-pilot-leverandøren (Aver&Lauritzen), at deres LPS (Ganglion) kan migreres til IDWS XUA på ca. 420-500 timer. Ganglion indeholder pt. 10 DGWS integrationer.
LPS-leverandøren vurderer at der skal anvendes en time pr. klinik til udrulning.

Migration af OEJ
Når hele IDWS XUA konceptet er modent og fejlfrit, så vurderer kommune-pilot-leverandøren (DXC), at deres EOJ system (VITAE) kan migreres til IDWS XUA på ca. 460 timer. VITAE indeholder pt. 3 DGWS integrationer.
Omkostningerne ved udrulning til den enkelte kommune er besluttet.

Regioner
Regionspiloten vedrørte ikke migration væk fra DGWS, da demo-applikationen ikke har DGWS-snitflader. Regionspiloten anvendte i alt 354 timer, hvoraf ca. 150 timer gik til IDWS XUA integrationen. Regionspiloten var i forvejen implementeret med SAML baseret sikkerhed, så arbejdet med IdP-baseret autentifikation (Sundheds IdP) var beskedent. De øvrige udgifter i pilotprojektet er gået til brugergrænseflade-features i demo-applikationen og integration til DDS'en.

Regionspiloten vedrørte en telemedicinklient, som henter dokumenter fra DokumentDelingsServicen, og derfor er der ingen erfaringstal for EPJ-området. Til gengæld har projektet været i dialog med to af regionernes leverandører - Systematic og Signaturgruppen.

Systematic er leverandør af EPJ til Region Nord, Midt og Syd. Systematic fortæller, at de tre regioner har tre forskellige integrationsløsninger til DGWS-infrastrukturen. Dvs. Systematic kan ikke lave én IDWS XUA integrationsløsning, som kan genbruges på tværs af de 3 regioner. Det formodes dog, at de erfaringer, som Systematic opsamler i forbindelse med den første IDWS XUA integrationsløsning, kan genbruges i arbejdet med de efterfølgende integrationsløsninger.

Region H og Sjælland har det amerikanske EPJ-system EPIC. EPIC kender ikke DGWS-infrastrukturen, men integrerer til DGWS-infrastrukturen via en integrationsløsning leveret af Signaturgruppen (MOCES2SOSI komponenten). Et lignende koncept vil kunne laves for IDWS XUA profilen, og Signaturgruppen forventer at udviklingsomkostningerne kan holdes indenfor 1000 timer.

Opsamling vedr. omkostninger

Spørgsmålet er så, hvorvidt disse erfaringstal kan overføres til andre LPS og EOJ systemer. Det kan man nok ikke direkte, da de forskellige systemer forventes at have forskellig intern systemarkitektur, men IDWS-projektet vurderer, at selvom de faktuelle omkostninger ved migrering af det enkelte system kan variere (måske med en faktor 2), så giver piloterne alligevel et godt billede af størrelsesordenen. Sagt med andre ord, koster migreringsindsatsen måske et sted mellem 0,5 og 1,5 mio. kr. (worst case) – men det er usandsynligt, at migreringen kommer til at koste flere mio. kr. pr. system. For alle system gælder at migrationsomkostningen er en engangsudgift. Med der vil være en efterfølgende omkostning for udrulning og konfiguration til den enkelte kommune eller lægepraksis. Denne udgift vil afhænge af leverandørens forretningsmodel.

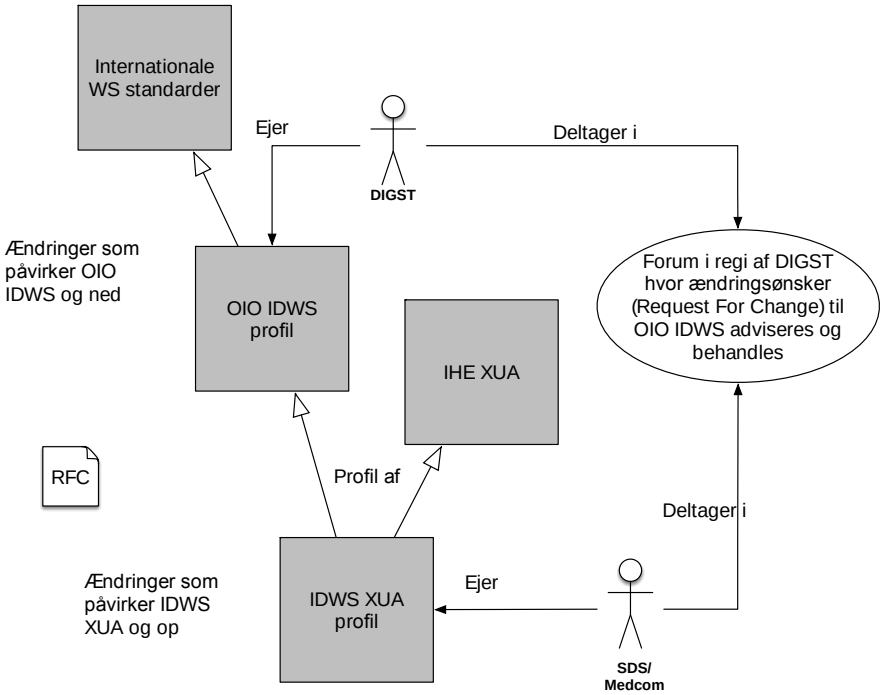
Nedenfor listet antallet af fagsystemer som kalder FMK via DGWS. Da FMK er den mest udbredte DGWS service, så forventes det, at listen også udgår de fagsystemer, som skal migreres fra DGWS til IDWS XUA. Listen er lavet på baggrund af informationer er hentet fra https://www.medcom.dk/standarder/godkendte-systemer

System-type	Antal
EOJ	6
EPJ	2
LPS	11
Apotekersystemer	3
Privat hospital systemer	1
Tandlæge systemer	3
Specialist systemer	2

Appendiks 7. Governance af profil og hjælpe-værktøjer

IDWS XUA profilen til sundhedsområdet er en profilering af den nationale OIO IDWS profil fra Digitaliseringsstyrelsen og IHE's internationale XUA profil. IDWS XUA hjælpeværktøjerne bygger på eksisterende hjælpeværktøjer fra Digitaliseringsstyrelsen. Governance af profiler og værktøjer vil ske i samarbejde mellem Digitaliseringsstyrelsen og Sundhedsdatastyrelsen. Indtil videre har DIGST og SDS følgende tanker omkring fælles governance af profil og hjælpeværktøjer.

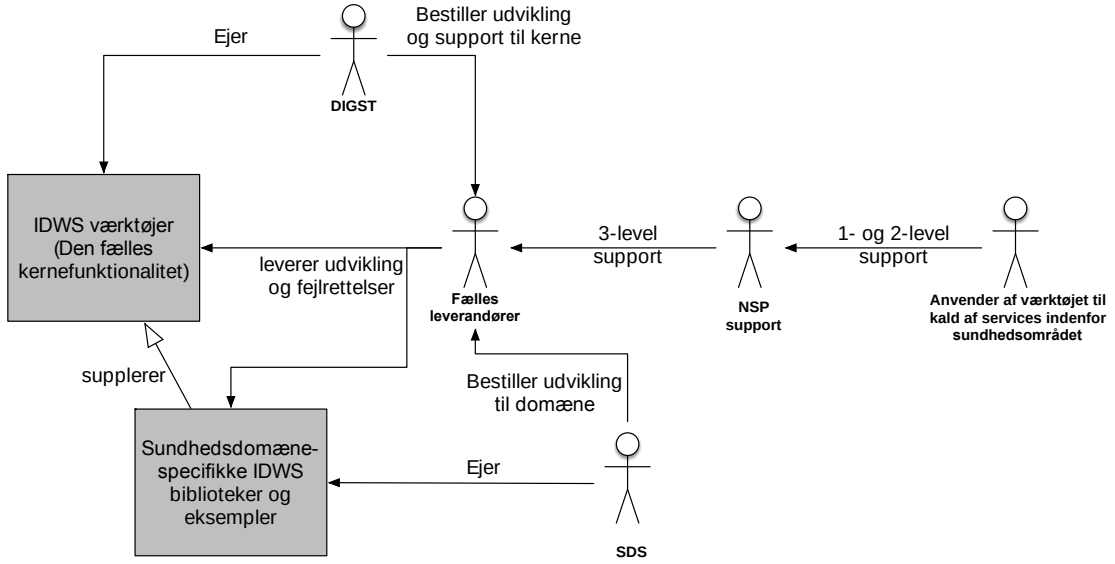
Governance af profil:
OIO IDWS profilen ejes, vedligeholdes og supporteres af Digitaliseringsstyrelsen. Såfremt, der sker ændringer i de internationale standarder, som OIO IDWS baseres på, er det DIGST's ansvar at påvirke disse ændringer og/eller (i samarbejde med brugerne af OIO IDWS – fx sundhedsområdet) at specificere ændringer til OIO IDWS, der sikrer fortsat overholdelse af internationale standarder.
Ændringsønsker til OIO IDWS profilen forventes relativt sjældent, da de underliggende webservice-standarder anses som stabile. Et forum til behandling af ændringsønsker kan derfor med fordel indplaceres i et eksisterende DIGST forum, hvor parterne mødes med jævne mellemrum. Det kunne fx være "Følgegruppen for fællesoffentlige systemkomponenter" eller lignende.



Figur 6: Governance af profil

Den sundhedsspecifikke profil tænkes ejet af en part på sundhedsområdet (f.eks. Sundhedsdatastyrelsen eller MedCom) og underlægges den eksisterende governance for fastlæggelse af standarder på sundhedsområdet.
Såfremt der sker ændringer i den internationale sundhedsspecifikke XUA standard, som profilen baseres på, er det profilejerens ansvar at påvirke disse ændringer og/eller (i samarbejde med profilens brugere) at specificere ændringer til profilen, der sikrer fortsat overholdelse af internationale standarder. Hvis foreslåede ændringer kræver ændringer i OIO IDWS for at kunne realiseres, er det profilejerens ansvar, at der anmodes om ændringer (Request for Change) heraf i overensstemmelse med den governance (change-proces) der fastlægges for OIO IDWS, forud for en eventuel beslutning om ændring af sundhedsprofilen.

Governance af værktøjer:
Sundhedsområdet har etableret .Net og Java værkstøjsunderstøttelse af sundhedsprofilen med udgangspunkt i de værktøjer DIGST har implementeret (som p.t. primært anvendes til at understøtte grunddataområdet). Dette arbejde er fra start koordineret med DIGST og samme leverandører er anvendt. Kodebasen er opdelt i en fælles kerne, som ejes af DIGST, samt domænespecifikke kodebiblioteker og kodeeksempler, som ejes af SDS. Det domænespecifikke vedrører kodebiblioteker til håndtering af attributter anvendt indenfor sundhedsområdet (fx sundhedsfaglig autorisation) samt kodeeksempler på kald til nationale sundhedsservices.



Figur 7: Governance af værktøjer

DISGT har ansvaret for kernefunktionaliteten, hvorimod SDS har ansvaret for de sundhedsspecifikke biblioteker og eksempler.
1- og 2-level support overfor sundhedsdomænets anvendere af hjælpeværktøjerne, håndteres via de eksisterende supportprocedurer på den Nationale Service Platform (NSP). NSP-support kan eskalere sager til 3-level support hos den fællesværktøjsleverandør.

Den fællesværktøjsleverandør dækker over en leverandør til .Net hjælpeværktøjerne og en leverandør til Java hjælpeværktøjerne, som alle parter kan købe ydelser fra via en fællesaftale. Dvs. DIGST kan købe vedligehold og support til kernefunktionaliteten, SDS kan købe vedligehold af de domænespecifikker biblioteker samt 3-level support til NSP, og en anvender (fx en region) kan købe tilslutningssupport til deres fagsystemer.

Alt vedligehold og support skal reguleres af én og samme aftale med leverandøren, således at den enkelte aftager ikke skal bøvle med at finde en egnet leverandør, aftaleindgåelse samt det faktum at governance er delt mellem DIGST og SDS. Det udestår på nuværende tidspunkt at få udpeget de to leverandører – evt. via udbud.

Hertil skal det nævens, at der allerede under udarbejdelse af projekt- og finansieringsgrundlaget (jf. projektinitieringsdokumentet) blev estimeret med forøgede vedligeholdelses- og supportomkostninger på 0,5 mio. kr. pr. år i migreringsperioden.