

Initiativ 3.4

- Anbefalinger og Roadmap

Dato: 25.03.2014

Version: 0.8

Udarbejdet af: EAD

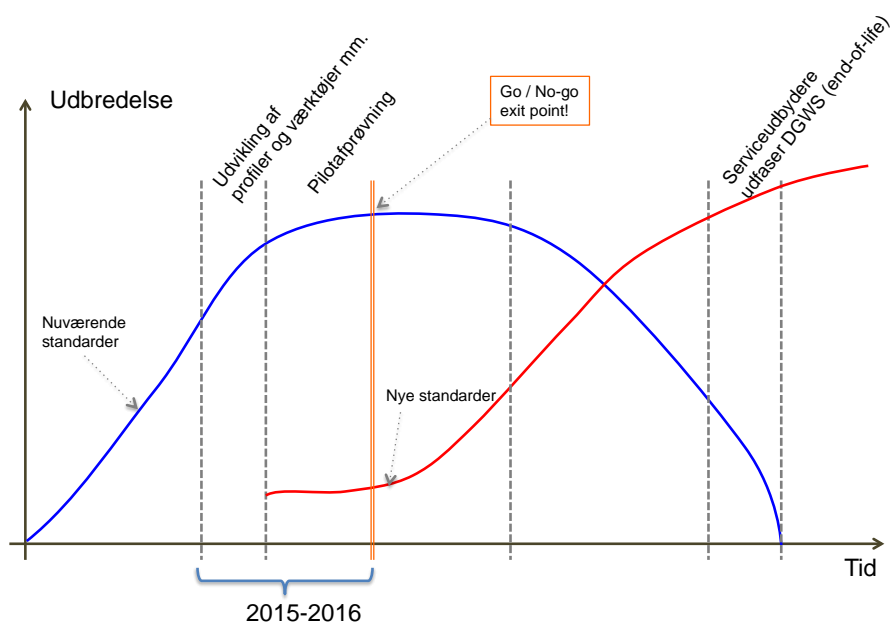
Statens Seruminstitut

Sektor for National Sundheds-IT

www.nsi.dk

Artillerivej 5

2300 København S



Resumé

Analysen har vist, at det vil være realistisk og fordelagtigt for sundhedsvæsenets parter at migrere fra de nuværende standarder til fællesoffentlige standarder. Migreringen vil kræve en række tiltag i både sundhedsdomænet som i fællesoffentligt regi.

Det anbefales at de nye standarder profileres og pilotafprøves i perioden 2015-2016. Det anslås at der skal investeres 8,35 mio. kr. for at gennemføre disse aktiviteter.

Analysen fremlægger et roadmap for migreringen. Det anbefales at forankre roadmappet hos styregruppen for den fællesoffentlige digitaliseringsstrategi.

Såfremt migreringen iværksættes i 2015 vil de nye standarder allerede være til rådighed i 2016, hvorefter de første gevinster vil vise sig i form af kompetencekonsolidering, færre forskelligartede sikkerhedsløsninger og bedre støtte til leverandører. Endelig udfasning af alle nuværende anvendelser af de eksisterende standarder vil dog næppe være tilendebragt før udgangen af 2020.

Den foreslåede migrering ventes ikke at rumme større eller særlige risici.

Introduktion og baggrund

Initiativ 3.4 i strategien for digitalisering af sundhedsvæsenet 2013-2017 blev netop iværksat for at afdække mulige gevinster ved at samordne og evt. modernisere standarderne og løsningerne indenfor og på tværs af domænerne. Formålet blev beskrevet således i kommissoriet:

Formålet med analysen er at:

- *afdække gevinster og omkostninger ved at samordne sikkerhedsstandarder og sikkerhedsløsninger i sundhedsvæsenet og det øvrige fællesoffentlige samarbejde.*
- *udpege mulige migreringsveje, barrierer og risici under hensyn til eksisterende fælles it-tjenester, f.eks. "Fælles Medicinkort" og "Sundhedsjournalen", med henblik på at sikre en omkostningseffektiv udvikling af sikkerhedsstandarder og sikkerhedsløsninger, der medvirker til at skabe sammenhængende, brugervenlige og sikre løsninger i det offentlige (herunder på sundhedsområdet).*

Nærværende notat opsummerer de anbefalinger, der kan gives efter at have gennemført initiativ 3.4.

Analysen har behandlet en række forskellige sikkerhedsløsninger, og har på den baggrund opstillet et målbillede, der viser hvorledes anvendelsen af sikkerhedsstandarder og -løsninger kan være fremover både indenfor sundhedsdomænet og imellem domæner.

Analysen er baseret på vurdering ud fra en række kriterier, der er opstillet for standarder og løsninger. Kriterierne er ikke alene tekniske kriterier, men omfatter f.eks. også modenhedsmæssige, styringsmæssige, udbredelsesmæssige, driftsmæssige og økonomiske perspektiver.

Analysen har behandlet samspillet mellem relevante internationale standarder og de fællesoffentlige standarder. Det har blandt andet ledt til nogle anbefalinger omkring tilpasning af den fællesoffentlige standard OIO IDWS.

Analysen rummer endvidere en afdækning af udbredelsen af de nuværende standarder i sundhedsdomænet. Denne afdækning ligger blandt andet til grund for udarbejdelsen af roadmappet, og for de økonomiske overvejelser i nærværende notat.

Analysen vurderes at være solid, set i relation til den afsatte tid og økonomi til analysen.

Dette notat foregriber den endelige analyserapport, der vil foreligge medio maj 2014.

Arbejdsgruppen, der har stået bag udarbejdelsen af analysen, har bestået af Digitaliseringsstyrelsen, kommunale-, regionale- og statslige repræsentanter af parterne på sundhedsområdet, MedCom og Sundhed.dk. Endvidere har man i analysen inddraget systemleverandører til sundhedsdomænet.

Gevinsterne ved at gennemføre anbefalingerne

I dag anvendes en række forskellige sikkerhedsstandarder i kommunikationen indenfor sundhedsdomænet og imellem sundhedsdomænet og andre domæner. Derudover er der etableret nye standarder og løsninger på fællesoffentligt plan (NemLogin) som til en vis grad overlapper med de standarder, der anvendes i sundhedsvæsenet i dag. Det bevirker blandt andet, at leverandører skal opretholde kompetencer indenfor flere sikkerhedsstandarder og -løsninger, hvilket i sidste ende kommer til udtryk gennem forøgede anskaffelsesomkostninger og især gennem forøgede support- og vedligeholdelsesomkostninger for sundhedsvæsenets parter.

Den Gode Web Service (DGWS) søger at standardisere kommunikationen indenfor sundhedsdomænet, men standarden har en række begrænsninger, der betyder at de enkelte projekter¹ har måttet definere deres 'egne standarder' for kommunikation af flere af de oplysninger, som er relevante i forbindelse med sikkerhedshåndteringen. Et af de områder, hvor begrænsningerne har kunnet mærkes tydeligst, vedrører den borgerrettede kommunikation. Her tillader DGWS rent faktisk ikke udstilling af borgerrettede services på samme måde som der i dag udstilles services til sundhedspersoner.

Følges anbefalingerne i dette notat vil disse forskellige måder at håndtere sikkerheden på ensrettes. Dermed vil det fremover blive lettere at fejlsøge og foretage ændringer på tværs af de enkelte systemløsninger, idet der ikke vil være en række specialtilfælde at skulle tage højde for. Der opnås også en gevinst i forhold til borgerne, idet der vil kunne ske en mere ensartet håndtering af privatlivsbeskyttelse, borgerens mulighed for indsigt, samtykke og frasigelsesmuligheder m.m..

DGWS er oprindeligt designet til at understøtte kommunikation mellem fagsystemer i sundhedsdomænet, der er forbundet via sundhedsdatanettet. Skal der kommunikeres med systemer uden for domænet eller via andre netværk er standarden ikke tilstrækkelig sikker (der mangler eksempelvis mulighed for at beskytte og begrænse brugen af de sikkerhedsbilletter, som der giver adgang til services). Der er også nogle stærke bindinger til en bestemt kryptografisk funktion (den såkaldte SHA-1 algoritme), der er ved at blive afløst af nyere og mere sikre algoritmer. Der er m.a.o. sikkerhedsmæssige grunde til at se på modernisering af DGWS eller se på alternativer til denne.

Med den anbefalede modernisering af standarder og værktøjer, vil systemudviklerne også have bedre muligheder for at benytte moderne udviklingsværktøjer², hvilket igen kan reducere udviklingsomkostningerne. Konsolideres brugen af standarder (bl.a. mellem sundhedsområdet og andre domæner) behøver udviklere ikke at mestre en så bred palette af kompetencer, og man vil kunne hente støtte i andres erfaringer med brug af samme standarder. Og man vil sammen kunne være med til at løfte udfordrin-

¹ FMK har defineret nogle dataelementer vedrørende brugerens kontekst (kaldende organisation, it systemets navn og version, evt. medhjælp og rolleinformationer) som bruges i forhold til adgangskontrol. I NPI projektet definerede man nogle overlappende kontekstinformationer, og Sundhed.dk har ligeledes haft behov for at definere kontekstinformationer.

² Hverken Den Gode Web Service eller OIO IDWS (og de værktøjer der understøtter disse) er i dag vedligeholdt, hvilket betyder, at det bliver sværere og sværere at etablere kommunikation med gængse udviklingsværktøjer. Følger sundhedsområdet fremover fællesoffentlige standarder, vil der være flere med til at sikre vedligeholdelsen af disse.

ger med understøttelse af nye udviklingsplatforme, eksempelvis til mobile enheder, på en sikker måde.

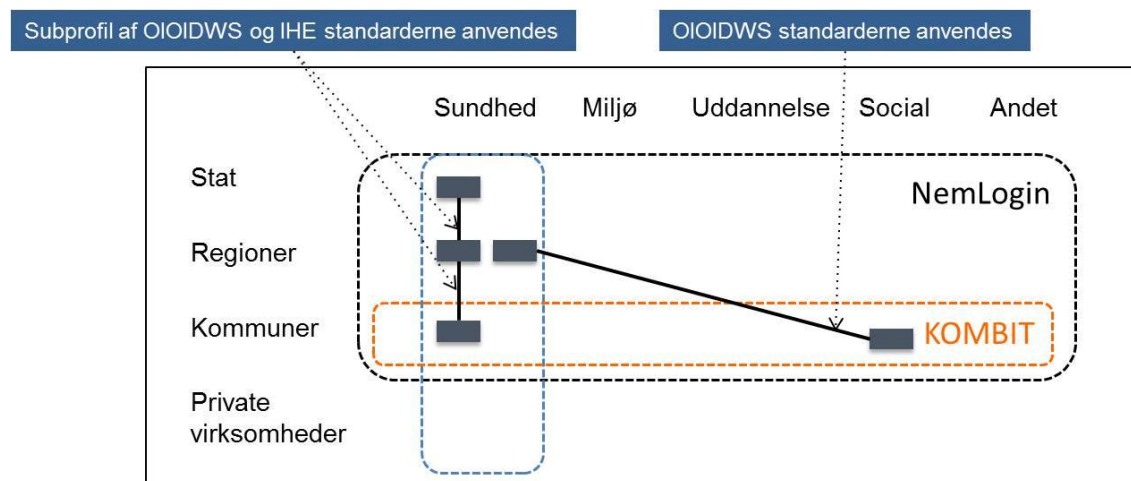
Da kommunikationen indenfor sundhedsområdet og mellem sundhedsområdet og andre domæner fremover vil følge fælles standarder, bliver opgaven med at skabe sammenhæng i løsninger på tværs af domæner (f.eks. en kommunal medarbejders adgang til en national service på sundhedsområdet) mere simpel.

Da kommunikationen på sundhedsområdet yderligere følger internationale standarder, vil det være lettere for udenlandske leverandører at tilpasse deres løsninger til danske forhold. Det vil således blive lettere for danske kunder at udnytte et internationalt marked af løsninger, hvilket igen må formodes at skabe billigere løsninger. Danske leverandører vil tilsvarende have lettere ved at udnytte mulighederne for at udbrede produkterne på et større (internationalt) marked.

Anbefalinger

Anbefalinger ift. standarder og løsninger

Den gennemførte analyse viser, at sundhedsvæsenet i fremtiden med fordel kan benytte de fællesoffentlige OIOWS og OIO SAML standarder. Det anbefales at anvende disse standarder såvel ved udstilling af services til andre domæner såvel som indenfor sundhedsdomænet. Dette er illustreret i nedenstående figur.



En forudsætning for tvær-domæne anvendelse af OIOWS er, at der gennemføres et 'serviceeftersyn' på de nuværende OIOWS standarder, hvor de blandt andet ajourføres i forhold til nyeste udvikling på internationalt plan.

En forudsætning for anvendelsen indenfor sundhedsdomænet er, at der gennemføres en såkaldt subprofilering af OIO IDWS. Det er afgørende for sundhedssektoren, at OIOWS standarderne kan sameksistere med de internationale IHE standarder. Analysen viser at standarderne kan sameksistere, såfremt der sker nogle ændringer i OIO-IDWS.

I overensstemmelse med referencearkitektur for informationssikkerhed i sundhedsvæsenet, understøtter ovennævnte standarder, at der etableres tillidsføderationer både indenfor sundhedsdomænet og imellem domæner. Disse føderationer skal dog baseres på et fælles "trust framework", som skal udarbejdes. Det anbefales at dette "trust framework" udarbejdes, høres og ratificeres, så der kan arbejdes videre med føderationsdannelse indenfor sundhedsdomænet og mellem sundhedsdomænet og andre domæner.

Som det fremgår af det målbillede, som analysen opstiller, vil sundhedsdomænet med udbredelsen af ovenstående standarder fortsat have behov for en national "Security Token Service" (STS) til verificering og evt. berigelse af sundhedsfaglige sikkerhedsattributter³. I takt med at lokale (fødererede) autentifikationsmekanismer vinder udbredelse i sundhedsvæsenet, anbefales det at overveje at opsplitte STS-funktionaliteten, så de nationale autentifikationsmekanismer (f.eks. kontrol af digital signatur) flyttes til det

³ attributter er sikkerhedsinformationer, der indgår i de tekniske "billetter" der medsendes i den tekniske kommunikation, for at give adgang til services

fællesoffentlige domæne (NemLogin⁴) med henblik på fælles drift og udviklingssynergi, mens de sundhedsspecifikke omvekslingsmekanismer forbliver på sundhedsområdet.

I relation til serviceanvendelser på tværs af domæner anbefales det, at services på sundhedsområdet, som udstilles for brugere i andre domæner, følger de fællesoffentlige OIOWS standarder. Der vil være yderligere gevinster at høste for alle parter, hvis øvrige domæner vælger at gøre det samme. For sundhedsvæsenets parter vil en sådan udvikling betyde, at man efter endt implementering af de nye standarder kun skal opretholde kompetencer inden for ét sæt standarder både i relation til services inden for sundhedsdomænet og uden for sundhedsdomænet.

I relation til støtte til udviklere hos leverandører til sundhedsområdet anbefales det fortsat at udvikle støtteværktøjer - herunder referenceimplementationer, eksempler og testmuligheder. Referenceimplementationerne skal udvikles som fungerende eksempler, der anvender moderne rammeværk og udviklingsværktøjer. Eksisterende støtteværktøjer til nuværende anbefalede standarder indenfor sundhedsdomænet (Den Gode Web Service, DGWS) overføres til den nye værktøjsunderstøttelsesportefølje i det omfang det giver mening. Afdækningen af leverandørernes udviklingsmiljøer viser, at den største støtte stadig kan opnås ved at understøtte i udviklingsplatformene Java og .NET. Det anbefales dog samtidig at igangsætte en analyse af, hvordan man bedst understøtter applikationer på mobile enheder.

Endelig anbefales det at undersøge hvorvidt 'sikker browser opstart' også er et behov i andre domæner, og om sundhedsdomænets løsning dermed kan gøres til en fællesoffentlige løsning.

Anbefalinger i forhold til governance

For at sikre den fornødne støtte og levedygtighed af de nye standarder, er det vigtigt at der i forbindelse med udarbejdelsen af de nye standarder også etableres en række styringsfora. Disse fora skal operere såvel indenfor sundhedsdomænet som på tværs af domæner, og de skal operere på forskellige niveauer, rækkende fra det strategiske niveau til det operationelle niveau.

Konkret anbefales det at:

- der udarbejdes en strategi for brugerstyring, som forankres i styregruppen for den fællesoffentlige digitaliseringsstrategi.
- der udarbejdes en referencearkitektur for brugerstyring på tværs af domæner, som forankres et nyetableret fællesoffentligt arkitekturforum i regi af Digitaliseringsstyrelsen. Samme forum skal også sikre udvikling og vedligeholdelse af de fællesoffentlige standarder.
- de nye subprofiler på sundhedsområdet lægges i kataloget af nationale standarder i sundhedsvæsenet, under styring hos NSI. NSI koordinerer de sundhedsspecifikke standarder, og sikrer at de kan sameksistere med fællesoffentlige standarder og relevante internationale standarder.
- der etableres vedligeholdelsesorganer (Change Advisory Boards, CAB'er) på sundhedsområdet og på tværs af domæner til behandling af ændringer i løsninger og hjælpeværktøjer.
- ejere af standarder og af værktøjer etablerer vidensfora (f.eks, netværk og grupper på digitaliser.dk), som modereres af udvalgte ressourcepersoner.

⁴ NemLogin er i dag begrænset til offentlige serviceudbydere. Dette skal indgå i overvejelserne.

Etablering af en sådan governance struktur vil kræve aktiv medvirken af sundhedsvæsenets parter og parter fra andre domæner.

Anbefalinger ift. juridiske problemstillinger

Målbilledet, som opstilles i rapporten, viser en fremtid, hvor sikkerhedsløsninger etableret indenfor et domæne kan anvendes af parter i et andet domæne. Dette kan give anledning til juridiske problemstillinger, f.eks. i forhold til udbudsmodeller konkurrenceudsættelse mv. Det anbefales at disse problemstillinger afdækkes og evt. juridiske barrierer behandles.

Anbefalinger ift. implementering

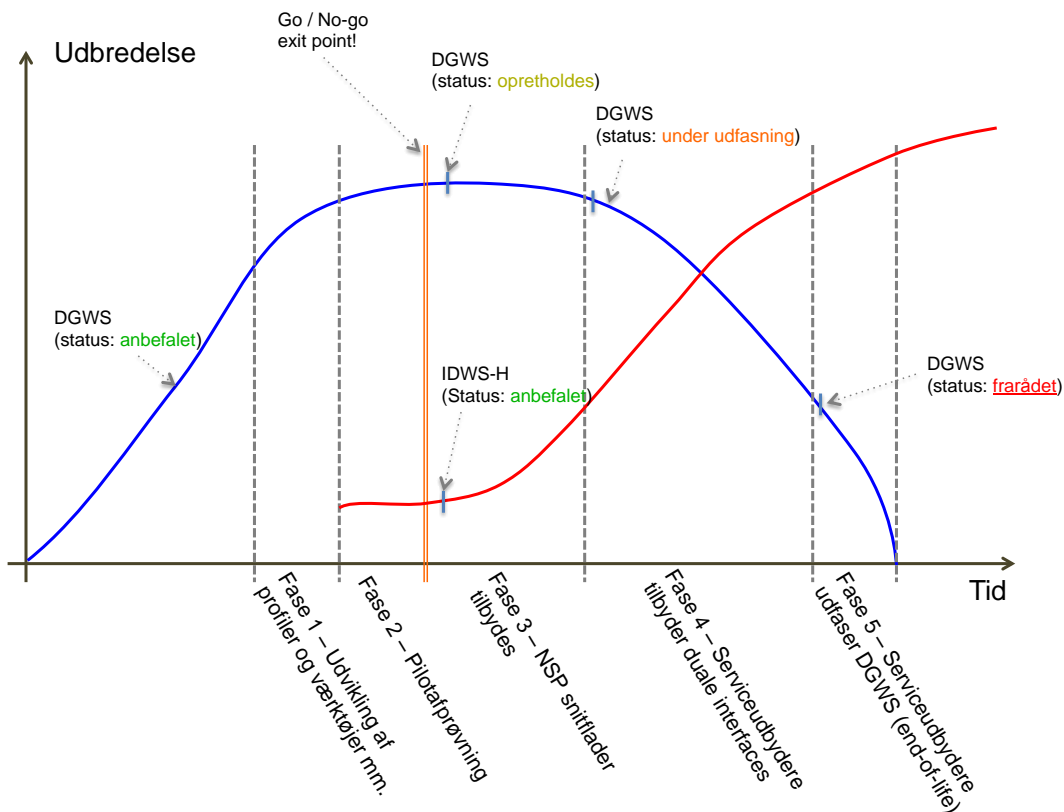
Implementering tænkes gennemført i to spor:

- **Spor 1 – Fællesoffentlig standardisering**, der har til hensigt at skabe de fornødne strategier, referencearkitekturer, tilpasninger af standarder og fællesoffentlige værktøjer samt etablering af fælles krav og politikker (trust frameworks), samt etablere sikkerhedsmekanismer (omveksling af security tokens mv.), der kan skabe sammenhæng mellem forskellige sikkerhedsdomæner.
- **Spor 2 – Nye standarder for sundhedsdomænet**, der har til hensigt at specificere, kvalitetssikre og implementere nye profiler af fællesoffentlige og internationale standarder, understøttende værktøjer mv. i sundhedsdomænet.

I begge spor anbefales det, at gennemføre pilotprojekter inden der foretages en bred implementering af standarder. Dette har til hensigt at kvalitetssikre standarder og værktøjer inden alt for mange parter kastes ud i anvendelsen af disse.

En pilotafprøvning har også til hensigt at skabe et godt grundlag for at beregne de faktiske omkostninger, som parterne kommer til at afholde i forbindelse med implementering og migrering af standarder. Man kan således planlægge den videre migreringsproces ud fra erfaring med, hvad det koster at migrere de enkelte løsninger, og pilotafprøvningen giver samtidig en 'exit' mulighed, såfremt det viser sig, at migreringen er forbundet med større omkostninger eller indebærer store risici, som parterne ikke kan acceptere.

Nedenfor illustreres det ideelle forløb, hvor den nuværende standard på sundhedsområdet (DGWS) løbende udfases og erstattes med ny standard. Afhængig af parternes fokus på udfasning, kan perioden efter pilotafprøvningen og indtil de gamle standarder er helt udfaset, gøres kortere eller længere.



Aktiviteter – spor 1

Nedenfor skitseres hvilke aktiviteter Digitaliseringsstyrelsen bør gennemføre i henhold til anbefalingerne. Der er to aktiviteter, der er forudsætning for at sundhedsområdet kan gå i gang med en migrering og som derfor bør gennemføres i 2014-2015. Den videre planlægning af aktiviteterne overlades til Digitaliseringsstyrelsen.

Spor 1 – Fællesoffentlig standardisering.

Aktiviteter i spor 1	Afhængigheder
Opdatering af OIOWS, vedligeholdelse af referenceimplementationer, oprettelse/moderering af communities mv.	Dette er en forudsætning for spor 2 fase 1
Udarbejdelse af strategi for brugerstyring på tværs af domæner	
Udarbejdelse af referencearkitektur for brugerstyring på tværs af domæner	
Afklaring af behov for fællesoffentlig løsning vedr. "sikker browseropstart"	
Udarbejdelse af fællesoffentligt "trust framework"	Dette er en forudsætning for spor 2 fase 1
Juridisk afklaring ift. udbudsmodeller,	

der sikrer at løsninger kan benyttes på tværs af offentlige aktører og mellem offentlige og private

Pilot med etablering af sikkerhedsstyring på tværs af domæner (billetomveksling, sikker browseropstart etc.)

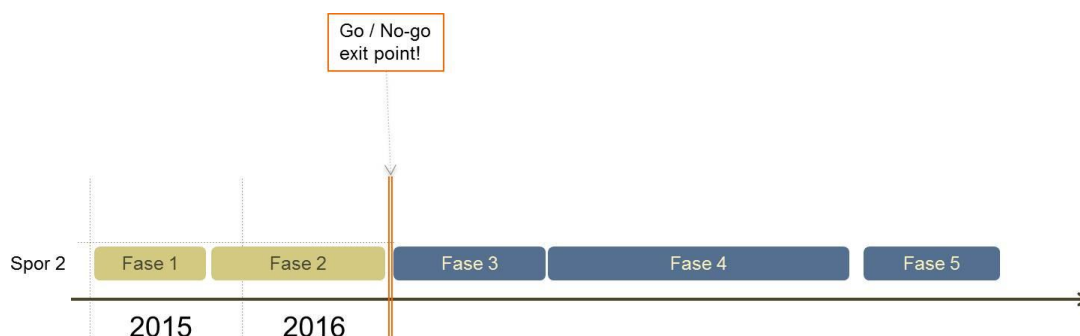
Dette forudsætter, at flere af aktiviteterne i spor 1 er gennemført. Såfremt piloten involverer sundhedsområdet vil det være hensigtsmæssige at spor 2 fase 1 og 2 er gennemført først

Det anbefales at undersøgelsen af nye teknologier, der er anvendelige i forhold til borgerrettede services og til understøttelse af mobile enheder gennemføres i forbindelse med formuleringen af en referencearkitektur.

Efter gennemførelsen af ovenstående aktiviteter, kan der etableres kommunikation på tværs af domæner baseret på fælles standarder.

Aktiviteter og anslåede omkostninger – spor 2

Aktiviteterne i dette spor forventes gennemført i et antal faser, hvoraf de første to gennemføres i 2015-2016:



Nedenfor beskrives aktiviteterne i hver fase. For hver aktivitet anslås omkostninger til aktiviteterne.

Spor 2 – Fase 1: Forberedelse til pilotafprøvning på sundhedsområdet

Denne fase forbereder standarder og hjælpeværktøjer til den efterfølgende pilotafprøvningsfase. En enkelt aktivitet (profilering af "trust framework") kræver inddragelse af parterne på sundhedsområdet. Der er ikke indregnet lønomkostninger for NSI eller andre parter i oversigten.

Aktiviteter i spor 2 fase 1	Part	Overslag (1000 kr.)
Subprofilering af OIOIDWS	NSI	200
Etablering af hjælpeværktøjer og vejledninger	NSI	800
Udvidelse og idriftsættelse af den eksisterende STS komponent inkl. projektledelse	NSI	1000
Øvrige ændringer til infrastrukturkomponenter (SOSI-GW, DCC, NSP etc.)	NSI	1.750
Profilering af "trust framework" til sundhedsdomænet	NSI	200
I alt	-	3.950

Forudsætningerne for at kunne gennemføre denne fase er, at OIOIDWS er tilrettet, så denne kan sameksistere med IHE standarderne. Endvidere er en forudsætning for profilering af "trust framework", at der er et fællesoffentligt (tvær-domæne) "trust framework" at profilere ud fra. Såfremt et sådant ikke skabes, kan sundhedsområdet skabe sit eget, men dette vil have større omkostninger end angivet, og som udgangspunkt kan dette ikke skabe tillid til kommunikation fra parter, der ligger udenfor sundhedsområdet.

Spør 2 – fase 2 er den konkrete **pilotafprøvningsfase**, hvor de nye standarder afprøves i produktion, men i lille skala.

Pilotprojektet vil gennemføre tilpasninger af en national service (f.eks. FMK) og tre anvendelsessystemer (f.eks. to lægepraksissystemer og et sygehussystem), der repræsenterer forskellige teknologivalg (udviklingsplatform) og forskellig brug af infrastrukturkomponenter.

Standarder og værktøjer tilpasses på baggrund af erfaringer fra pilotdriften, og etablering af de nødvendige governance tiltag iværksættes, dækkende fra strategisk forankring og monitorering til operationel støtte og vedligeholdelse.

Efter denne fase kan de første gevinster af migreringen høstes. Alle nye services i sundhedsdomænet vil bruge de nye standarder og værktøjer, der er tilpasset og understøttet af moderne udviklings-rammевærk. Desuden vil pilotfasen medvirke til at give mere sikre estimater på omkostningerne ved at migrere systemer og services (hvilket har betydning for planlægning af fase 4-5 i migreringsplanen).

Aktiviteter i Spør 2 fase 2	Part	Overslag (1000 kr.)
Gennemførelse af pilotprojekt	NSI	3.000
Tilpasning af standarder, vejledninger, hjælpeværktøjer og infrastrukturkomponenter	NSI	600
I alt	-	3.600

Beslutningspunktet

Pilotprojektets resultater dokumenteres, og fremlægges for sundhedsvæsenets parter. På baggrund af resultaterne vil det være muligt for parterne at afgøre, om det er fornuftigt at migrere fra eksisterende standarder til nye, hvilke mer-omkostninger der er forbundet med dette, og hvilken takt dette skal ske i. Dette kan lægges til grund for økonomiforhandlinger for de efterfølgende år.

Fase 3 – duale snitflader. Såfremt parterne ønsker at gå videre i migreringsplanen, foreslås det at der i fase 3 udarbejdes nye snitflader på NSP, så eksisterende services kan anvendes med de nye standarder⁵. Den pågældende bagvedliggende service ændres endnu ikke. Nye anvendelser af eksisterende services kan benytte disse services. Eksisterende anvendelser kan migreres hos de leverandører, der finder det opportunt

Gevinsterne efter denne fase ligger i konsolidering af standarder, og mulighed for brug af nye standarder på områder, hvor de gamle standarder har sine begrænsninger. Eksempelvis vil parterne på sundhedsområdet være i stand til at bruge de fællesoffentlige NemLogin, OIOSAML og OIOWS løsninger til borgerrettede services, og derved opnå et ensartet højt sikkerhedsniveau for denne type services.

⁵ Der etableres "smarte" viderestillingsservices på NSP, der kan konvertere mellem DGWS og IDWS-H (og evt. vice versa), inklusiv omveksling af "billetter".

Aktiviteter i fase 3	Part	Overslag (1000 kr.)
Udarbejdelse og idriftsættelse af NSP services	NSI	800
Support og vedligehold af eksisterende standarder	NSI	0 ⁶
I alt	-	800

I **Fase 4** tilføjer **serviceudbydere** nye snitflader, der overholder de nye standarder, til deres services⁷. Dette forventes at ske som led i den almindelige vedligeholdelse⁸ af servicen. I denne fase moderniserer systemleverandører også systemsnitfladerne, så de overholder nye standarder. Dette sker også som led i den almindelige udvikling og vedligeholdelse.

Serviceudbydere og serviceanvendere forventes i stigende grad selv ønske at anvende de nye standarder, bl.a. for at minimere kompetencevedligeholdelse til et sæt standarder og værktøjer. Samtidig vil leverandørerne i stigende grad få gavn af den støtte, som kan fås fra udvikler-communities mv.

Gevinsterne efter denne fase skal findes på virksomhedsniveau i form af konsolidering af og bedre adgang til kompetencer inden for de nye standarder, forbedrede værktøjsunderstøttelse og -support.

Der er i denne fase ikke behov for investering i nye services, infrastruktur eller lignende i relation til de nye standarder.

Fase 5 er **restimplementering** hvor resterende anvendelser af de gamle standarder udfases. Beslutning om igangsætning af denne fase skal ske på baggrund af en vurdering af, at det ikke længere kan betale sig at vedligeholde og supportere de gamle standarder, værktøjer og infrastrukturløsninger, i forhold til omkostningen ved at flytte de resterende service-anvendere og udbydere over på de nye standarder. Der gives 6-12 måneder til at migrere over til nye standarder. Herefter bortfalder support på gamle standarder - og nationale tjenester, der baserer sig herpå, lukkes.

NSI fastsætter anbefalingsgraden "frarådet" til de gamle standarder og kan overveje, om anbefalingsgraden på de nye standarder skal hæves til fra "anbefalet" til "obligatorisk" i en periode, for at sikre, at de sidste løsninger bliver migreret.

De sidste konsolideringsgevinster er hermed høstet.

⁶ Forventes dækket af eksisterende budgetter.

⁷ Samtidig ændres de etablerede viderestillingsservices på NSP, så disse ikke længere foretager konverteringsfunktioner mellem de forskellige standarder.

⁸ Der er tale om "pull implementering", hvor serviceudbydere selv driver tilpasningen til de nye standarder.

Investeringsbehov 2015 og 2016

Det er en ret lille del, ca. 0,5 mio. kr. af omkostningerne ved at gennemføre fase 2, der ventes afholdt i 2015. I alt er investeringsbehovet for 2015 altså 4,450 mio. kr..

Såfremt halvdelen af fase 3 kan gennemføres i 2016 og resten i 2017, vil investeringsbehovet i 2016 udgøre 3,5 mio. kr.. Det resterende investeringsbehov for den centrale infrastruktur vil i 2017 udgøre 0,4 mio. kr.

I årene efter pilotafprøvningen (dvs. fra 2017) må der påregnes ekstraomkostninger på ca. 0,5 mio. kr. årligt til support og vedligeholdelse af såvel nye som gamle standarder, hjælpeværktøjer mv.

Før der er gennemført pilotprojekter er det næppe muligt at give et pålideligt overslag over, hvad de samlede migreringsomkostninger (inklusive migreringsomkostninger for systemejere) er. Dette vil også afhænge af, hvor lang periode migreringen ønskes gennemført over. Ved at udstrække migreringsperioden over 3-4 år eller længere, opnås en række synergieffekter mellem migreringen og den almindelige udvikling og modernisering af systemer og services.

Risici

Opgaven med etablering af nye standarder og migrering til disse er relativt velforstået og indebærer ikke væsentlige risici. Såfremt anbefalingerne omkring gennemførelse af pilotprojekter inden bred implementering følges, kan der også opnås relativ stor sikkerhed om de implementeringsomkostninger, som det på nuværende tidspunkt ikke er muligt at give megen sikkerhed for.

Såfremt parterne formår at etablere og aktivere de ovenfor anbefalede styringsorganer, anses det samlede forløb derfor ikke for at være behæftet med særlige eller store risici.