Bilag 5: Udkast til rapporten Fællesoffentlige brugerstyringsløsninger - En analyse af sikkerhedsstandarder og –løsninger.

(Bilag til dagordenspunkt 8, *Sikkerhedsstandarder og –løsninger på sundhedsområdet*).

Fællesoffentlige brugerstyringsløsninger

- En analyse af sikkerhedsstandarder og –løsninger

Indhold

Ledelsesresumé

Baggrund

Initiativ 3.4 i den Nationale Strategi for Digitalisering af Sundhedsvæsenet 2013 – 2017 - Digitalisering med effekt – består af en analyse af gevinster og omkostninger ved at samordne sikkerhedsstandarder og sikkerhedsløsninger i sundhedsvæsenet med det øvrige fællesoffentlige samarbejde.

Analysen er nu gennemført i regi af en arbejdsgruppe bestående af

- Regionale repræsentanter
- Kommunal repræsentant
- Digitaliseringsstyrelsen
- NSI
- Sundhed.dk
- MedCom

Analysens indhold er kvalificeret gennem høring af den regionale IT5-kreds (IT-direktørerne i de fem regioner) og i kommunernes it-arkitektråd efter høring i netværket af kommunale it-arkitekter.

Hvad viser analysen?

De sidste 10 år har det offentlige etableret en række sikkerhedsløsninger, der fungerer som fælles løsninger for systemer fra forskellige parter. Udviklingen af disse løsninger er sket forholdsvis ukoordineret, og der indtil i dag ikke været et samlet overblik over, hvilke arkitekturer og standarder de enkelte løsninger bygger på. De forskellige løsninger hænger ikke sammen, og det giver en udfordring, når systemer understøttet af en sikkerhedsløsning skal kommunikere med systemer og services understøttet af en anden sikkerhedsløsning (eksempelvis hvis en kommunal eller en regional løsning skal anvende en national eller statslig service).

Analysen viser, at der på trods af den forholdsvis ukoordinerede udvikling, er udviklet løsninger, som har store lighedspunkter i den overordnede arkitektur[1]. Langt hen ad vejen er der også stort sammenfald i anvendte standarder[2]. Det vurderes derfor, at man med en relativ beskeden indsats kan få de enkelte sikkerhedsløsninger til at hænge sammen.

For at sikre en koordineret udvikling fremover, hvor løsninger skabt af en part i højere grad kan anvendes af andre parter, foreslår arbejdsgruppen bag analysen, at der udarbejdes en fælles strategi med en fælles vision og fælles principper at bygge sikkerhedsløsninger efter.

Analysen går et skridt videre og viser, at det rent faktisk er muligt at opstille et fælles teknisk målbillede med afsæt i de nuværende løsninger og med øje for en fælles vision, som analysen peger på. Dermed har de enkelte løsninger noget mere konkret de kan orientere sig imod.

[1] Såkaldte føderationer der kommunikerer sikkerhedsoplysninger vha. "billetter"
[2] Hovedparten af løsningerne baseres eksempelvis på de internationale standarder: SAML2 og WS-Trust.

Samlet anbefaler analysen at gennemføre følgende aktiviteter i fællesoffentligt regi (under Digitaliseringsstyrelsens ansvar):

Fællesoffentlige aktiviteter	Afhængigheder til aktiviteter på sundhedsområdet
Opdatering af OIOIDWS, vedligeholdelse af referenceimplementationer, oprettelse/moderering af communities mv.	Forudsætning for fase 1 (se senere)
Udarbejdelse af strategi for brugerstyring på tværs af domæner	
Udarbejdelse af referencearkitektur for brugerstyring på tværs af domæner, indeholdende bl.a. borgervendt kommunikation på mobile enheder	
Afklaring af behov for fællesoffentlig løsning vedr. "sikker browseropstart"	
Udarbejdelse af fællesoffentligt "trust rammeværk"	Forudsætning for fase 1 (se senere)
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.)	Såfremt piloten involverer sundhedsområdet vil det være hensigtsmæssige at fase 1 og 2 (se senere) er gennemført på sundhedsområdet først

Anbefalinger i forhold til sundhedsområdet

Arbejdsgruppen har set på en af de standarder, der er etableret på sundhedsområdet (Den Gode Web Service, DGWS). Arbejdsgruppen finder, at der er behov for at modernisere denne inden for en årrække. Arbejdsgruppen finder endvidere, at man med fordel kan lægge sig op ad eksisterende fællesoffentlige og internationale standarder. Arbejdsgruppen peger på, at der hermed skabes øget konkurrence og bedre mulighed for at udnytte et internationalt marked.

Det anbefales derfor, at sundhedsområdet etablerer en ny web service profil[3] til afløsning for DGWS. Det anbefales at denne profil overholder såvel den fællesoffentlige standard OIO IDWS som de krav til webservices, der stilles af den internationale organisation IHE. Analysen peger på at dette er muligt med en mindre justering af OIO IDWS.

Analysen anbefaler at denne profil i lighed med DGWS understøttes af en række vejledninger, værktøjer mm.. Efter dialog med leverandører på området foreslås det dog at orientere hjælpen mere mod anvendelsen af markedsprodukter frem for at bygge sine egne værktøjer.

Samlet anbefaler analysen at gennemføre følgende aktiviteter på sundhedsområdet (NSI ansvarlig):

Aktiviteter på sundhedsområdet	Fase
Subprofilering af OIOIDWS	1

[3] En profil er populært sagt en beskrivelse af, hvilke standarder der anvendes til hvad. En profil er i sig selv en standard.

Etablering af hjælpeværktøjer og vejledninger	1
Udvidelse og idriftsættelse af den eksisterende STS komponent inkl. projektledelse	1
Øvrige ændringer til infrastrukturkomponenter (SOSI-GW, DCC, NSP etc.)	1
Profilering af "trust rammeværk" til sundhedsdomænet	1
Gennemførelse af pilotprojekt	2
Tilpasning af standarder, vejledninger, hjælpeværktøjer og infrastrukturkomponenter	2
Udarbejdelse og idriftsættelse af NSP services	3
Support og vedligehold af eksisterende standarder	3

Implementeringsovervejelser

Den største værdi ved standardisering vurderes af leverandørerne til at være konsolidering af kompetencer og konsolidering af løsninger. De ekstra kræfter leverandørerne af løsninger bruger på at opretholde kompetencer og værktøjer til forskelligartede løsninger giver sig udslag i forøgede omkostninger til vedligeholdelses og support aftaler.

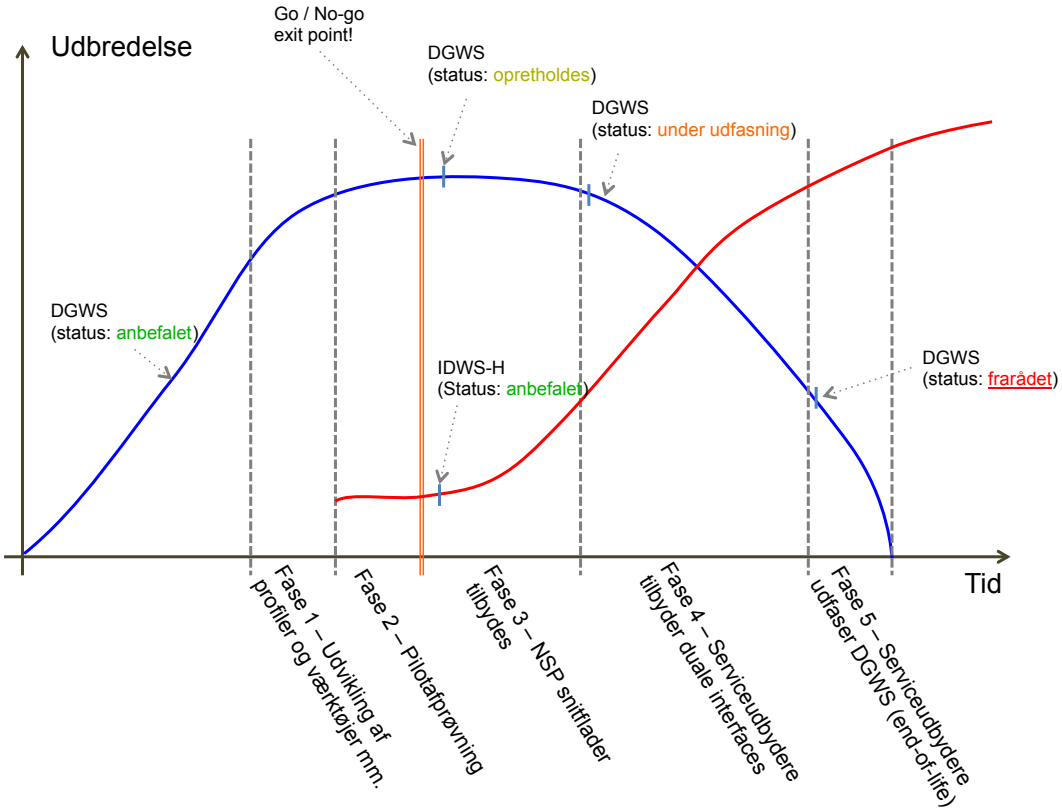
Arbejdsgruppen peger yderligere på, at jo længere tid der går inden DGWS moderniseres/erstattes, jo sværere bliver det at understøtte DGWS med moderne udviklingsværktøjer (hvilket også vil give en forøget omkostning i forbindelse med vedligeholdelse af løsningerne). På et tidspunkt vil DGWS stærke binding til ældre teknologier også udgøre en sikkerhedsmæssig risiko.

Analysen anbefaler derfor, at der påbegyndes en migreringsproces, der udfaser DGWS til fordel for de anbefalede profiler. Det anbefales, at denne migreringsproces påbegyndes snarest. Jo længere tid der går før migrering påbegyndes (og jo mere DGWS udbredes), jo større og mere risikofyldt bliver opgaven.

Analysen har afdækket ca. 50 parter, der benytter DGWS. Der er i dag implementeret forretningskritiske services (f.eks. FMK) og antallet af kald af services på den nationale serviceplatform ligger pt. på 13-14 mio. kald pr. måned. Det anbefales derfor at indlede med at gennemføre en pilot, der har til formål at kvalitetssikre nye standarder, vejledninger og værktøjer inden disse gøres til genstand for bred implementering.

Der lægges derfor op til en migreringsstrategi, hvor den videre udbredelse af DGWS stoppes ved 1) at etablere og kvalitetssikre nye standarder, så nye services kan baseres på nye standarder og 2) etablere nye snitflader til eksisterende services, så nye systemer ikke behøver at udvikle integrationssnitflader baseret på gamle standarder for at kunne benytte de eksisterende services. Når videre udbredelse af DGWS er stoppet og man gennem pilotprojektet har fået konkrete erfaringer med, hvor stor migreringsopgaven er for systemer og services, kan parterne aftale en hensigtsmæssig migreringstakt for de eksisterende systemer og services.

Den samlede migreringsproces beskrives i nedenstående figur:



Fasedelingen giver mulighed for at stoppe op og korrigere i processen, hvis det viser sig hensigtsmæssigt. Hvis man efter pilotafprøvning af den ene eller anden grund ikke finder det hensigtsmæssigt at påbegynde migrering, kan processen afbrydes inden fase 3 påbegyndes (markeret i figuren som et exit-point).

Økonomiske konsekvenser

Arbejdsgruppen har vurderet, at det ikke er muligt på det foreliggende grundlag at estimere de samlede omkostninger og gevinster knyttet til en udskiftning af DGWS med en mere moderne standard (inklusiv udskiftning i alle systemer og services[4]).

Omkostninger til etablering af nye standarder, tilhørende værktøjer og gennemførsel af pilot vurderes i størrelsesordenen 8,5 mio. kr. over en to-årig periode fra igangsættelsen. Investeringen vil sikre, at der foreligger en ny standard understøttet på en sådan måde, at migreringen for de resterende systemer kan foretages med mindst muligt risiko og på et stærkere økonomisk fundament.

En efterlevelse af analysens anbefalinger – og bevilling af midler til etablering af nye standarder og gennemførsel af pilot – vil således være en grundinvestering til sikring af en forsvarlig migrering af de ca. 50 kørende systemer i produktion, hvoraf flere er forretningskritiske.

[4] Før pilot er gennemført er det for usikkert, hvad migrering af et system eller en service koster. Med 50 løsninger vil en sikkerhed på bare +/- 0,1 mio. pr. løsning vil give en usikkerhed på 10 mio. kr. for den samlede migrering.

Fra det tidspunkt en ny profil/standard tages i produktion (og indtil DGWS er endeligt udfaset) vil der skulle påregnes 0,5 mio. kr. årligt i forøgede support og vedligeholdelsesomkostninger af standard og understøttende vejledninger og værktøjer.

Indledning

Baggrund

De sidste 10 år har det offentlige etableret en række sikkerhedsløsninger, der fungerer som fælles løsninger for systemer fra forskellige parter. Udviklingen af disse løsninger er sket forholdsvis ukoordineret, og der haves ikke i dag et samlet overblik over, hvilke arkitekturer og standarder de enkelte løsninger bygger på. De forskellige løsninger hænger ikke sammen, og det giver en udfordring, når systemer understøttet af en sikkerhedsløsning skal kommunikere med systemer og services understøttet af en anden sikkerhedsløsning (eksempelvis hvis en kommunal eller en regional løsning skal anvende en national eller statslig service).

Formål

Analysen medvirker til at besvare en række spørgsmål. Hvad skal der eksempelvis til for, at man i højere grad fremover kan udnytte erfaringer på tværs og anvende fælles standarder, hvor markedssituationen tilsiger det? Er det fremover muligt at skabe sammenhæng i sikkerhedsløsningerne, så brugerne bl.a. undgår at skulle "logge på" flere gange, og så oplysninger om brugere ikke skal vedligeholdes flere steder? Hvad skal der til for at skabe en sådan sammenhæng? Kan løsningerne fremover se sig som en del af en samlet sikkerhedsløsning, og vil det være muligt at koordinere udviklingen, så delløsninger etableret af nogle parter i højere grad vil kunne anvendes af andre parter? Kan der ske en konsolidering af nogle allerede anvendte standarder og (del-)løsninger?

Kommissoriet for analysen beskriver formålet således[5]:

- At afdække gevinster og omkostninger ved at samordne sikkerhedsstandarder og sikkerhedsløsninger i sundhedsvæsenet og det øvrige fællesoffentlige samarbejde.
- At 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).

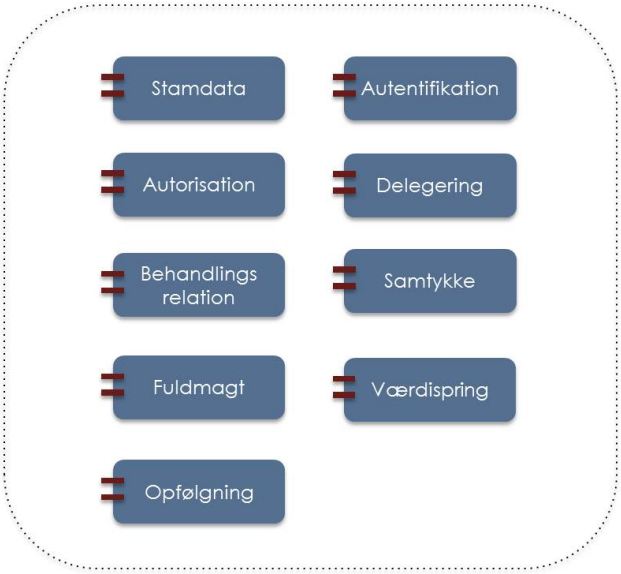
Analysen vil komme med en række anbefalinger. Nogle af disse vil være konkrete anbefalinger i forhold til ændringer i standarder, løsninger, ejerskab, drifts- og supportorganisation, governance etc., der med fordel kan gennemføres indenfor strategiperioden. Analysen vil give et bud på, hvad der skal til for at realisere sådanne konkrete ændringer. Analysen vil også komme med anbefalinger af mere principiel karakter. Disse leder ikke umiddelbart til ændringer, der kan tids- og prisfastsættes her og nu, men vil kræve yderligere behandling af parterne.

[5] Det samlede kommissorium og teknisk bilag til dette er vedlagt som appendiks 1 og 2.

Analysens indhold og afgrænsning

Standarder for sikkerhed (informationssikkerhed) dækker mange ting. Er der tale om standarder for den fysiske indretning af driftscentre med nødstrøm, videoovervågning, alarmer og brandanlæg? Eller er der tale om standarder for, hvordan man organiserer og gennemfører sikkerhedsarbejdet, herunder gennemfører risikoanalyser samt opbygger og vedligeholder et nødberedskab?

Denne analyse vil have fokus på standarder, der understøtter og sætter rammerne for udvikling af infrastruktur, systemer og services. Den på sundhedsområdet udviklede referencearkitektur for informationssikkerhed [ReferenceSikkerhed] peger i denne sammenhæng på følgende logiske sikkerhedskomponenter:



Figur 1 - Logiske komponenter, som it-sikkerhed i sundhedssektoren består af.

Behandlingsrelation er et begreb, der er specifikt for sundhedsområdet, og som handler om sikkerheden for, at der er en aktuel behandlingsrelation mellem den behandlende og den behandlede, og at det således er relevant for den behandlende at se helbredsinformationer vedrørende patienten. Mere generelt handler det altså om sikkerheden for, at tilgangen til data er nødvendig for, at den der tilgår data kan udføre sine arbejdsmæssige opgaver.

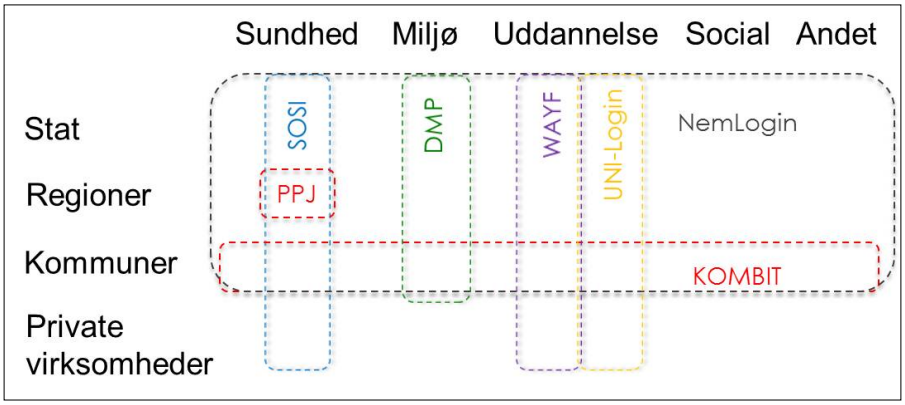
Autentifikation, autorisation, delegering, behandlingsrelation/nødvendighed, samtykke, fuldmagt og værdispring vedrører alle, hvad man populært kalder bruger- og adgangsstyring (eller *credential and identity management*, CIM og *access control*, AC). Analysen vil have sit hovedfokus på standarder, der understøtter dette. De logiske komponenter stamdata og opfølgning vil kun blive dækket i det omfang, at de er forudsætninger i forhold til bruger- og adgangsstyring (eksempelvis stamdata i forhold til overførsel af sikkerhedsinformation / sikkerhedsatributter).

Selvom det er tekniske og logiske sikringsforanstaltninger, der er i fokus, er det ikke muligt at afgrænse sig til standarder, der alene sætter tekniske krav til løsninger. Opereres eksempelvis med standardiseret sikkerhedsinformation, der beskriver niveauer af sikkerhed for, at en

bruger har den identitet, som vedkommende giver sig ud for (såkaldt Assurance Levels), stiller dette også krav til organisation og arbejdsgange f.eks. vedrørende udstedelse, udlevering og anvendelse af akkreditiver som digitale certifikater. Referencearkitekturen for informationssikkerhed [ReferenceSikkerhed] peger da derfor også på standarder (f.eks. Kantara Identity Assurance Framework), der regulerer mange andre sikkerhedsaspekter end de tekniske og indholdsmæssige, men som udgør et fundament for de tekniske og indholdsmæssige standarder.

En anden afgrænsning, det har været nødvendig at foretage, vedrører hvilke sikkerheds*løsninger* der kigges på. Det er ikke sikkerhedsløsninger ved enkelte parter (f.eks. den enkelte region , kommune eller statslige institution), der er genstand for analysen. Det er udelukkende fælles løsninger, dvs. løsninger, der anvendes af flere parter, som analyseres. Nogle af disse er knyttet til et bestemt fagområde, eksempelvis sundhedsområdet, socialområdet, undervisningsområdet eller miljøområdet, men andre er tænkt som fælles løsninger på tværs af fagområder. Nogle af sikkerhedsløsningerne benyttes til at skabe sikkerhed omkring bestemte parters it-systemer og services, f.eks. fælleskommunale systemer - mens andre benyttes af flere parter, f.eks. alle offentlige virksomheder eller af såvel offentlige som private virksomheder.

Systemlandskabet kan beskrives af følgende kort:



Figur 2 - Kort over forskellige sikkerhedsløsninger, og hvilke "virksomhedstyper" og fagområder, de dækker.

Kortet beskriver, hvilke system- og serviceudbydere, der er dækket af hvilke sikkerhedsløsninger. Eksempelvis kan alle offentlige myndigheder og institutioner få deres løsninger dækket af NemLogin. Det kan private virksomheder ikke.

Analysen beskriver de kortlagte sikkerhedsløsninger på et overordnet niveau, herunder den konceptuelle og logiske arkitektur, anvendte standarder m.m.. Herefter analyseres forskelle og fællestræk ved de forskellige løsninger, og på baggrund af dette (samt nogle mere strategiske overvejelser) formuleres et bud (målbillede) på en fremtidig sammenhængende sikkerhedsarkitektur (med mulighed for single sign-on og genbrug af registrerede brugeroplysninger).

[Husk MedCom beskeder, Fælles offentlig datafordeler, NemHandel, og evt. andre sektorer?]

Herefter fokuserer analysen på de sikkerhedsløsninger, der anvendes på sundhedsområdet, dvs. SOSI-infrastrukturen, sikkerhedsløsningen bag Præhospitals Patientjournal (PPJ), Kombits fælleskommunale sikkerhedsløsning og NemLogin. Og med udgangspunkt i vurderede omkostninger og gevinster ved migrering af løsninger over i den fremtidige målarkitektur, gives anbefalinger i forhold til fremtidig anvendelse af sikkerhedsstandarder og løsninger på området.

Metoderamme

[Strategisk afsnit – lånt fra referencearkitektur]
[Identifikation af aktører og løsninger – se appendiks]

Målgruppe

Læsevejledning

Tilblivelsesproces

Denne rapport beskriver resultatet af analysen. Bag rapporten står en arbejdsgruppe bestående af Digitaliseringsstyrelsen, kommunale-, regionale- og statslige repræsentanter af parterne på sundhedsområdet, MedCom og Sundhed.dk. Endvidere har man i analysen inddraget systemleverandører til sundhedsdomænet.

Rapporten er blevet til i en proces, hvor konsulenter, arbejdsgruppens deltagere og gæster er kommet med oplæg til de emner, der er blevet diskuteret i arbejdsgruppen. Efterfølgende er der skrevet afsnit, der dækker behandlingen af emnerne og arbejdsgruppen har haft lejlighed til at kommentere de enkelte afsnit.

Viden om de enkelte standarder og løsninger er blevet indhentet fra konsulenter med indgående kendskab hertil og gennem offentliggjort materiale. I enkelte tilfælde har det også været nødvendigt at indhente information fra ejerne af standarder og løsninger.

Overordnet begrebsramme

Dette afsnit har til formål at give en fælles forståelse af, hvad brugerstyring er. Der gives en overordnet beskrivelse af, hvilke bestanddele en brugerstyringsløsning består af, og hvordan disse dele hænger sammen. Denne fælles forståelsesramme skal bl.a. benyttes til at beskrive og sammenligne de konkrete brugerstyringsløsninger, som indgår i analysen.

Ser man på de begreber, som benyttes i forskellige standarder og rammeværk i dag, så benyttes de ikke helt på samme måde[6]. Vi har i denne analyse lagt os op ad forståelsen i [NIST] når det drejer sig om basale begreber vedr. akkreditiver og identitetssikring og forståelsen i [WS Federation] når det drejer sig om web teknologier.

En samlet liste med ordforklaringer findes i Appendiks 7: Ordliste.

Elementer i et sikkerhedsdomæne

Når to parter, personer eller IT-systemer, udveksler information, er der altid en afsender og en modtager. I dette dokument betegnes afsenderen *serviceudbyder* (engelsk: Service Provider, SP) og modtageren *serviceaftager* (engelsk: Service Consumer, SC). Information kan have en begrænset modtagerskare, og når dette er tilfældet, har serviceudbyderen behov for at sikre sig, at serviceaftageren må modtage informationen (eller sagt mere generelt: Om serviceaftager skal have adgang til den udbudte service). Dette kan bl.a. ske ved, at serviceudbyderen afkræver serviceaftageren et bevis for dennes identitet.

Vi kender det fra posthuset, hvor det kræver et kørekort eller lignende at få udleveret en pakke (posthuset er udbyder af en pakkeudleveringsservice). Et sådan identitetsbevis betegnes *akkreditiv* (engelsk: Credential) og det er blevet tildelt af en Credential Service Provider (CSP), i eksemplet med kørekortet, Rigspolitiet.

At fastslå en identitet ud fra udstedte akkreditiver, kalder vi *autentifikation*. I eksemplet med postkontoret kontrollerer postmedarbejderen, at kørekortet er:

1) Ægte, dvs. udstedet af en myndighed, postmedarbejderen har tillid til
2) Validt, dvs. ikke udløbet eller frakendt
3) Udstedt til serviceaftageren, dvs. at ejeren af kortet ligner billedet på det og at underskriften på kortet ligner den, serviceaftageren sætter på kvitteringen.

Hvis alle disse check falder positivt ud, kan postmedarbejderen have tillid til hvem personen er. Herefter checker postmedarbejderen:

4) at pakken er stilet til den pågældende person eller at vedkommende har en fuldmagt fra den person, som pakken er stilet til
5) at vedkommende kan fremvise postvæsenets udsendte advisering af pakkeforsendelsen

[6] Det er især begreber som akkreditiver (credentials) og token, der benyttes lidt i flæng, og det er forståelsen af, hvad en Identity Provider og en Security Token Service er (og hvordan de adskiller sig), der varierer mellem forskellige standarder og rammeværk.

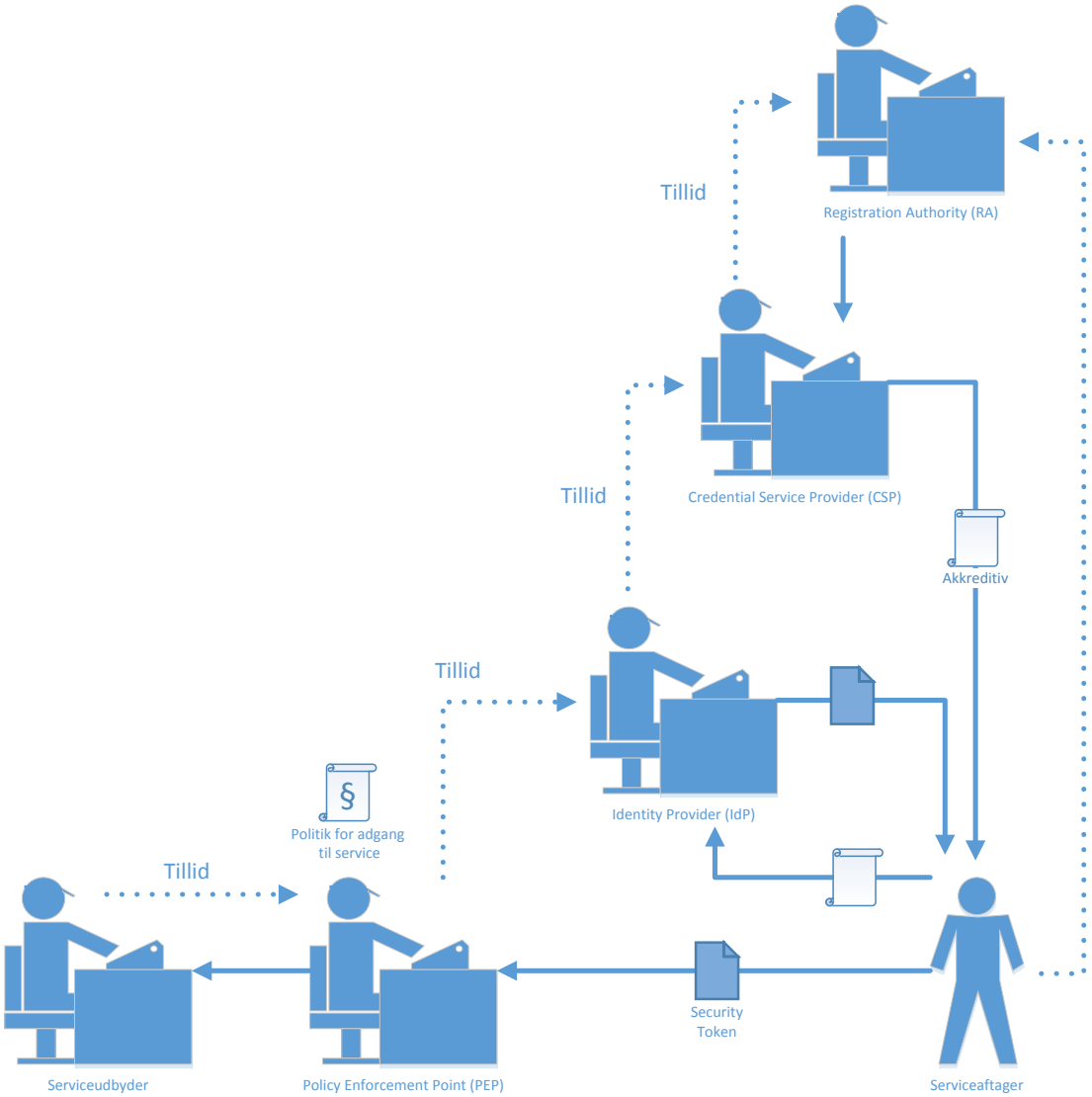
Hvis dette er tilfældet, taler vi om, at vedkommende er *autoriseret* til at modtage pakken (har autoriseret adgang til servicen). At afgøre, om en person er autoriseret til en service eller ej, betegner vi *adgangskontrol* (engelsk: Access Control). Adgangskontrollen følger en formuleret *politik* (engelsk: Policy) for kontrol i forbindelse med anvendelse af servicen. I det beskrevne eksempel fremgår denne af forretningsbetingelser (for privatpakker) formuleret af Post Danmark.

Den (logiske) komponent i et sikkerhedsdomæne, som varetager autentifikation, kaldes en *Identity Provider* (IdP) og adgangskontrol baseret på eksplicitte adgangspolitikker foretages af et såkaldt *Policy Enforcement Point* (PEP). Bemærk, at der er tale om logiske komponenter, der fysisk kan realiseres på forskellig vis. I eksemplet med pakkeforsendelsen blev kontrol af modtagerens identitet (autentifikation), kontrol af adkomst til pakke (autorisation) og udlevering af pakke (udbudt service) varetaget af samme postmedarbejder.

En serviceudbyder kan også selv stå for at udstede akkreditiver. Dette kendes fra mange systemer i dag, som har deres egen brugerstyring. Her oprettes en bruger typisk med et brugernavn og et kodeord gældende for det enkelte system. Hvis en serviceaftager skal tilgå flere systemer og services bliver denne model hurtigt upraktisk. For hver serviceudbyder / system skal brugeren nemlig have et akkreditiv med det administrative ekstraarbejde dette medfører for hver enkelt serviceudbyder og for serviceaftager, der skal holde styr på alle de forskellige akkreditiver (f.eks. brugernavne og kodeord), som måske er ret forskellige og som måske udløber og skal fornyes på forskellige tidspunkter.

I større organisationer med mange systemer og services, har man derfor arbejdet på at konsolidere brugerstyring, således at de enkelte brugere kun skal anvende ét akkreditiv (typisk brugernavn og kodeord) indenfor organisationen. Med NemID er der nationalt etableret et sæt af akkreditiver (certifikater med nøgler). Her er det Nets DanID A/S der er Credential Service Provider (CSP). DanID har en række betroede (lokale) registreringsenheder (engelsk: Registration Authority, RA), der varetager den fysiske identifikation og registrering af personer (eller systemer), og DanID udsteder på baggrund af disse registreringer et certifikat, som den registrerede kan benytte til at bevise sin identitet med overfor andre (såkaldt Relying Parties, RP), der har tillid til DanID som CSP.

De væsentligste elementer og deres sammenhæng kan illustreres med nedenstående figur:



Figur 3: Væsentlige begreber i et servicekald og deres sammenhæng

Bemærk, at serviceudbyders tillid til at det er de rette personer (eller systemer) der får adgang til en service beror på en række faktorer. Serviceudbyderen skal have tillid til at adgangskontrollen (Policy Enforcement Point) kun videregiver servicekald, der overholder politikken for adgangen til servicen. Adgangskontrollen (PEP) bygger på tillid til, at en Identity Provider (IdP) på en sikker måde har kunnet fastslå serviceaftagers identitet (autentificere vedkommende). Identity Provideren har tillid til, at den der har udstedt akkreditiverne (dvs. Credential Service Provider, CSP) har gjort dette til de rette personer (nemlig de samme personer, som registreringsenheden, RA, har identificeret og registreret oplysninger på), og Credential Service Provideren har tillid til, at registreringsenhederne har kunnet foretage en sikker identifikation (og registrering) af serviceaftagerne (den stiplede pil til højre i figuren).

Som det fremgår af figuren optræder et såkaldt *security token*. Dette udstedes af Identity Provideren (IdP) og benyttes i kommunikationen til serviveudbyderen (med dennes adgangskontrol, Policy Enforcement Point, PEP). Et security token er en slags ”billet” med

tidsbegrænset gyldighed til en eller flere services. Det er billetten, der giver adgang til servicen - ikke det akkreditiv som er udstedt til serviceaftager.

Situationen kan sammenlignes med det at købe en billet til en bus eller et tog. Her lægges et bevis (akkreditiv) for betaling (kontanter, betalingskort, kreditkort, check, etc.) ved et billetbureau, kiosk eller lignende, og der printes og udleveres (udstedes) en billet (security token) som er gældende i en tidsbegrænset periode til en rejse i et antal zoner (servicen). En billetkontrollør eller en chauffør (adgangskontrol) sørger for, at det kun er folk med gyldig billet, der benytter sig af servicen. Fordelen ved at have adskilt billetbetaling og adgangskontrol er, at alle kontrollører ikke behøver at kunne håndtere alle mulige betalingsformer. Vedkommende skal kun kunne afgøre gyldigheden af billetten. Kommer der fremover nye betalingsformer (f.eks. betaling via mobiltelefon), er det kun billetbureauet eller kiosken, der fremover skal kunne håndtere dette; kontrollørernes arbejde er uændret.

Hvis man holder funktionaliteter adskilte, når man implementerer sikkerhedsløsninger opnår man tilsvarende fordele. Det vil eksempelvis være muligt at understøtte nye autentifikationsprotokoller ved at ændre i eksisterende Identity providers (IdP'er) eller ved at etablere nye IdP'er – uden at dette kræver ændringer ved de enkelte serviceudbydere (eller adgangskontroller). En løsere kobling mellem de enkelte funktioner tillader også, at man kan implementere funktionerne ved forskellige parter og på forskellige niveauer. Eksempelvis har der været en gevinst ved at gå sammen om etablering af en udsteder af digitale certifikater (Credential service Provider), mens registreringsenheder bedst er blevet placeret der, hvor man har styr på hvem, der er medarbejdere i organisationen, altså lokalt.

Med udveksling af akkreditiver og security tokens mellem forskellige parter er der endnu et par faktorer, der har betydning for den samlede tillid til, at serviceaftager er, hvem vedkommende giver sig ud for, og at serviceaftager har lov til at benytte den udbudte service. F.eks. skal man sikre sig, at akkreditiver og billetter ikke kan være forfalskede (dvs. være produceret af andre end de autoriserede udstedere, altså CSP'en og IdP'en, eller at der efterfølgende er ændret på hvor længe akkreditiv eller security token er gyldigt, hvem der må benytte det, eller hvilke services det må bruges til) og at de ikke er stjålne (dvs. benyttes af andre end de er tiltænkt, altså dem de er udstedt til, og dem der retmæssigt har modtaget dem). Den teknologi, som akkreditiver og security tokens baseres på, har stor betydning for, hvor lette eller svære de er at forfalske, og den måde, hvorpå akkreditiver og security tokens opbevares, anvendes og transporteres, har stor betydning for, hvor lette eller svære de er at stjæle.

Ingen kæde er stærkere end det svageste led, så selvom man baserer en løsning på stærk autentifikation (f.eks. baseret på anvendelsen af kryptografiske nøgler), så er der kun lav tillid til, at serviceaftager er, hvem vedkommende giver sig ud for, hvis man ikke har høj tillid til, at det security token, der medsendes, rent faktisk kommer fra den mekanisme (IdP) som har foretaget den stærke autentifikation af serviceaftager og ikke er blevet ændret undervejs.

Vi har i det foregående lagt megen vægt på sikring af serviceaftagers identitet, som grundlaget for at afgøre adgang til en service. Lovkrav til logning kan også gøre dette nødvendigt. Men det ikke er altid, at en serviceudbyder har brug for at kende identiteten af serviceaftageren, for at afgøre dennes adgang til en service. Ved et køb af billet til bus eller tog, er der som tidligere

skrevet et behov for levere et bevis for betaling, men ikke nødvendigvis for kundens identitet (med mindre det er et periodekort med dertilhørende rabatter til samme person – her udgør et stamkort bevis for identitet).

Digitaliserer man folketings-, kommunal- og regionsvalg vil man – udover en række andre sikkerhedsmæssige elementer – kræve, at borgeren kan afgive sin stemme, uden at man efterfølgende kan spore hvad den enkelte borger har stemt. Her vil man nøjes med et bevis for, at borgeren har valgret, samt at borgeren ikke har afgivet sin stemme tidligere, og ikke har overdraget sin stemme til andre. Denne anonymisering er kendt fra de manuelle valgprocesser, der anvendes i dag, hvor man skiller kontrollen af identitet ud fra valgkortet med kontrollen af stemmesedler.

Da forskellige services har brug for forskellige "beviser" (forskellige billetter / security tokens), er der brug for, at man kan få udstedt nye[7]. Ved denne lejlighed ønsker man ikke nødvendigvis at brugeren igen skal autentificere sig ved brug af sine akkreditiver (man ønsker m.a.o. ikke at foretage sign-on hver gang en tjeneste skal anvendes). Har man allerede et gyldigt security token, kan dette benyttes som bevis for, at man tidligere har autentificeret sig, og dette security token kan derfor medsendes til den service, som udsteder det nye security token. En sådan service, der "veksler" security tokens, kaldes en *Security Token Service* (STS).

En Security Token Service kan veksle mellem token formater (som forstås af forskellige services), den kan verificere information i det modtagne security token ved at sammenholde med kilder, som den har tillid til, den kan supplere et security token med information fra kilder den har tillid til, eller den kan fjerne information fra et security token (sidstnævnte kan være relevant, hvis serviceaftager ikke har tillid til serviceudbyderens håndtering eller anvendelse af security tokens eller information i disse). Information i security tokens kaldes *attributter*, og kilder som STS'en benytter og har tillid til, kaldes *attribute providers* (og disse udbyder såkaldt *attribute services*).

En registreringsenhed (RA) eller en udsteder af akkreditiver (CSP) vil ofte udstille information om brugere og om akkreditiver (f.eks. om akkreditivet er gyldigt) gennem en attributservice. Men også andre registre kan være betroede kilder til information (eksempelvis kan Sundhedsstyrelsens autorisationsregister levere autoritativ information om en person har en af Sundhedsstyrelsens udstedt sundhedsfaglig autorisation eller ej).

Vi har igen en kæde af tillid, der udgør forudsætningen for at en tjenesteudbyder (eller dennes adgangskontrol) har tillid til at en serviceaftager må få adgang til en service. En tjenesteudbyder (dennes adgangskontrol) har tillid til den Security Token Service, STS, som leverer security tokenet. Denne STS har tillid til de attribut services, som den benytter til at verificere eller indhente sikkerhedsinformation, og den har tillid til den Security Token Service eller Identity Provider (IdP), som den modtager et security token fra. Et token kan således veksles igen og igen af forskellige Security Token Services, når blot hver af disse har tillid til den Security Token Service, som de modtager et security token fra. Det første security token (der ikke stammer fra en STS, men eksempelvis fra autentifikation ved en IdP) kaldes et *bootstrap token*.

[7] Med mindre forskellige serviceudbydere har bestemt sig for at benytte samme security token.

Kæden af etablerede tillidsrelationer (og derved mulige omvekslinger af security tokens ved Security Token Services) kræver særlig opmærksomhed. Hvis en serviceudbyder kræver stærk autentifikation af serviceaftageren, og denne kun har skaffet sig et security token gennem svag autentifikation, da må det ikke være muligt at omveksle det svage token til et stærkere token uden at dette er sket ved re-autentifikation. Sker dette ved en fejl, kan denne svaghed udnyttes af personer, der ønsker at skaffe sig uretmæssig adgang til en service.

Situationen kan sammenlignes med det at få udstedt et navnebevis. I gamle dage var det sognepræsten, der førte protokol over, hvem der beboede sognet (herunder var blevet født og som var døde, eller som var tilflyttet eller fraflyttet sognet), og vedkommende havde et personligt kendskab til beboerne. Skulle man flytte eller rejse, kunne sognepræsten udfylde et navnebevis. Men efterhånden som sognene blev større og færre kom fast i kirke og folk flyttede mere rundt, da var det vigtigt at kunne fastslå identitet på en anden måde end gennem personligt kendskab. Hvis en person henvendte sig til et sognekontor, og blot kunne oplyse navn og fødselsdato som eneste bevis for identitet, og på den baggrund kunne få udstedt et navnebevis, da ville navnebeviset efterfølgende kunne bruges til at få udstedt et pas (hvis man vel om mærke kunne omgå øvrige kontroller på pas-kontoret). Dette ville man så igen kunne bruge til at oprette en bank konto og få udstedt et kreditkort (altså igen hvis det er muligt at omgå bankens øvrige kontroller).

Noget af det, der gør det svært at opretholde sikkerheden i en kæde af tillidsrelationer er, at en udsteder af et akkreditiv ikke nødvendigvis ved, hvad dette bruges til efterfølgende. Eksempelvis anvendes kørekort og sundhedskort til rigtig mange ting, og såfremt proceduren for udstedelse af disse beviser ændres, da kan det have konsekvens for andre parters processer.

Sikkerhedsdomæner og føderationer

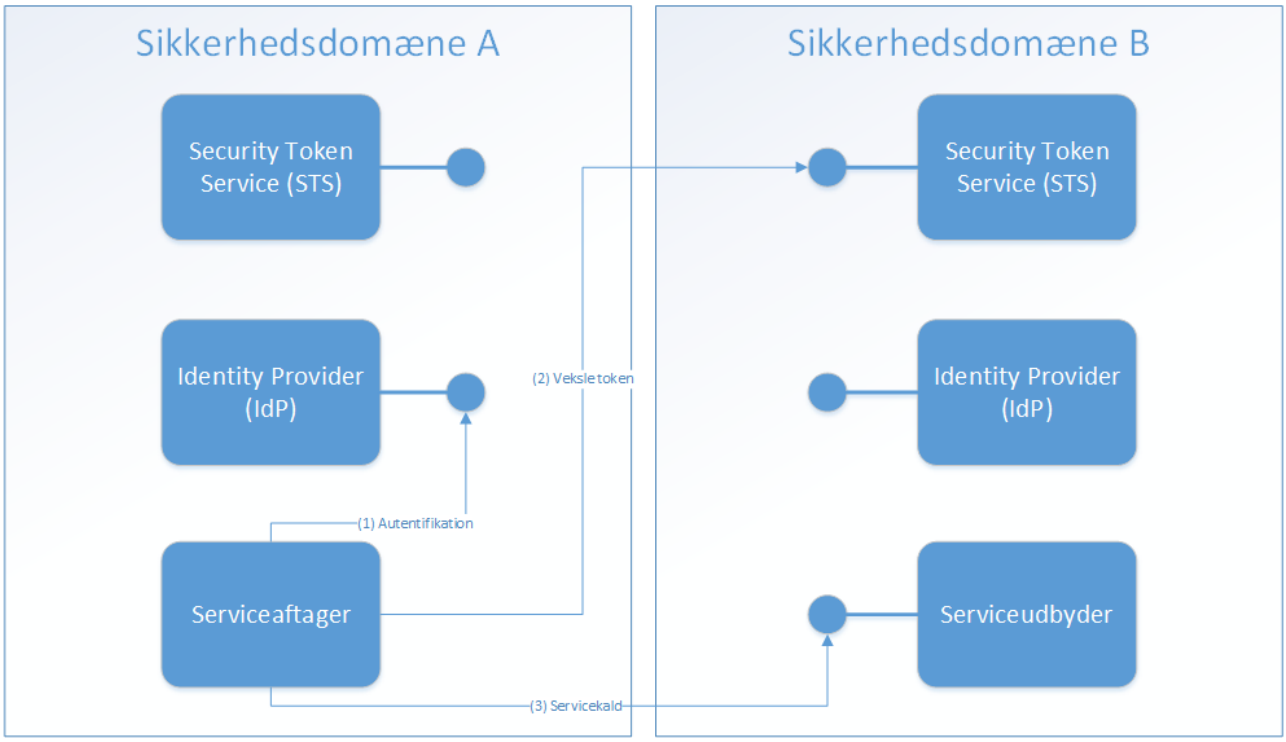
Serviceudbydere, der har tillid til de samme security tokens (og dermed til de udstedende IdP og STS services) siges at befinde sig i samme sikkerhedsdomæne.

Når parter i to forskellige sikkerhedsdomæner enes om fælles standarder for identiteter, fælles sikkerhedspolitikker og aftaler, og tilbyder servicekald på tværs af sikkerhedsdomænernes grænser, siges der at være etableret en føderation. En sådan føderation er altid baseret på tillid mellem de parter, der indgår i føderationen. En føderation kan siges at være et sikkerhedsdomæne i sig selv, men et sikkerhedsdomæne er ikke nødvendigvis en føderation.

I de analyserede modeller er SOSI f.eks. en føderation af serviceudbydere i Sundhedssektoren. En sådan serviceudbyder kunne være Sundhedsstyrelsen, der udstiller en service til indberetning af bivirkninger ved brug af lægemidler. Sundhedsstyrelsen har sit eget sikkerhedsdomæne, men er ikke i sig selv en føderation. SOSI har også sit eget sikkerhedsdomæne, der indeholder f.eks. både bivirkningswebservicen og Det Fælles Medicinkort (FMK).

I en føderation kan en serviceaftager anvende tokens udstedt af en IdP i ét sikkerhedsdomæne til at aftage services hos en serviceudbyder i et andet sikkerhedsdomæne. Ofte vil to sikkerhedsdomæner have forskellige tokenformater, og for at en serviceaftager kan kalde services hos en serviceudbyder i et andet sikkerhedsdomæne, kan der derfor være behov for at veksle et token. Vekslinger af tokens foretages af en Security Token Service (STS), der kender til de forskellige tokenformater, samt hvordan man oversætter imellem dem. Denne kan enten være placeret i det ene sikkerhedsdomæne eller i det andet sikkerhedsdomæne, eller udenfor disse (men stadig i føderationens sikkerhedsdomæne).

Figuren nedenfor illustrerer et eksempel, hvor omvekslingen sker ved STS'en i serviceudbyderens sikkerhedsdomæne:



Figur 4: Eksempel på kommunikation mellem to sikkerhedsdomæner i samme føderation

I figuren ovenfor autentificerer en serviceaftager i sikkerhedsdomæne A sig imod sin lokale IdP (1). Dette resulterer i et token for sikkerhedsdomæne A, men da serviceaftageren ønsker at tilgå en service hos en serviceudbyder i sikkerhedsdomæne B, som anvender et andet token-format, skal dette token veksles. STS'en i sikkerhedsdomæne B kender til sikkerhedsdomæne As IdP og der eksisterer et tillidsforhold mellem de to. Serviceaftageren veksler derfor sit token hos STS'en i sikkerhedsdomæne B (2) og kalder til slut serviceudbyderen i sikkerhedsdomæne B med dette token (3).

Kommunikationen kunne etableres på andre måder. Eksempelvis kunne serviceaftager i sikkerhedsdomæne A først få vekslet tokenet ved egen STS inden det omveksles ved STS'en i sikkehedsdomæne B. Så behøver STS i domæne B kun at forsikre sig om, at security tokenet kommer fra en kilde (nemlig STS'en i domæne A). Eller STS'en i A domænet kan veksle til et fælles mellemformat, som også STS'en i sikkerhedsdomæne B forstår. Dette vil være en fordel, hvis servicen i B skal udstilles til flere sikkerhedsdomæner; da skal STS B alene kunne

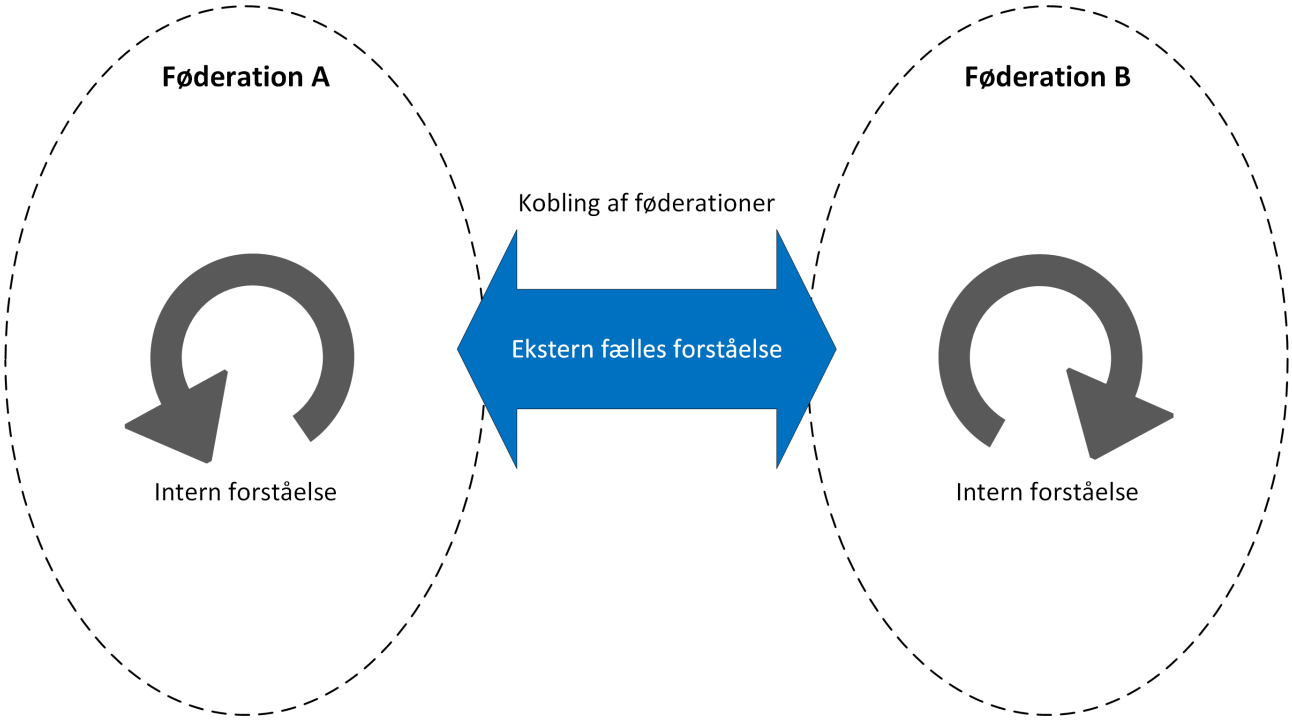
omveksle fra mellemformatet til serviceudbyder B's format frem for at have viden om formater i alle sikkerhedsdomænerne. Det svarer lidt til, at hvis personer fra mange forskellige lande skal mødes, da vil det være en fordel, om der er et fælles sprog, som alle kan forstå frem for at alle deltagerne skal kunne forstå alle sprog.

Føderationer internt og eksternt

På samme måde, som security tokens kan benyttes til at skabe sammenhæng mellem forskellige sikkerhedsdomæner, kan de også benyttes til at skabe sammenhæng mellem føderationer (der jo i sig selv udgør et sikkerhedsdomæne). Men kommunikation og omvekslinger af security tokens gør det ikke alene.

I den videre diskussion af føderationer og arkitekturmønstre belyses koblingen af to eller flere føderationer, og hvad det tekniske og organisatoriske fundament er for dette. Vi får brug for at skelne mellem, hvad der ligger "indenfor" en etableret føderation i termer af anvendte politikker, standarder og teknologier, samt hvad der ligger "imellem" de føderationer, der skal kobles sammen. I det efterfølgende vil vi anvende begreberne hhv. "internt" og "eksternt", til at fremhæve forskellen.

Figur 5 illustrerer dette:



Figur 5: Intern vs. ekstern forståelse af tekniske og organisatoriske procedurer, specifikationer og standarder

Denne analyse giver et bud på, hvad der skal på plads for at etablere den eksterne fælles forståelse som udgør fundamentet, hvorpå sammenhæng kan skabes. Internt er der fortsat mulighed for at operere med sin egen interne forståelse af tillid, security tokens, standarder mm., når bare den fælles eksterne forståelse lægges til grund for kommunikation på tværs med samarbejdende føderationer.

Det er kun for sundhedsområdet (primært SOSI-føderationen), at analysen vil komme med anbefalinger i forhold til eventuelle ændringer af den interne forståelse af sikkerhedsløsninger og –standarder.

Specifikt vil analysen komme med anbefalinger i forhold til standardisering af:

- Protokoller for kommunikation af tokens (*hvordan* security tokens kommunikeres)
- Tokens med information (token *indhold*) opstillet på en bestemt måde (token *format*)

Strategiske overvejelser

Før der kan gives et bud på hvad der skal til for at skabe sammenhæng mellem de etablerede føderationer (SOSI, NemLogin, Uni-login m.fl.) samt komme med anbefalinger i forhold til sundhedsområdets brug af standarder og løsninger (herunder overveje, om der kan ske en konsolidering op mod standarder og løsninger etableret af andre føderationer), er det vigtig at gøre sig nogle overvejelser om, hvilken retning udviklingen tager, ikke mindst udviklingen af sikkerhedsløsninger internationalt.

Ellers risikerer man at den fremtidige nationale udvikling kommer ud af trit med den europæiske udvikling, hvilket vil give problemer, når der fremover skal ske tættere integration af systemer på europæisk plan. Og man risikerer at konsolidere omkring standarder, der er på vej ud af markedet.

Dette kapitel indledes med at beskrive de væsentligste begrundelser for at gøre noget ved den nuværende situation. Herefter beskrives en række tendenser, som en fremtidig udvikling er nødt til at holde sig for øje. Ud fra disse overvejelser formuleres en vision om en fremtid, der tager højde for tendenserne og som leverer svar på den nuværende situations udfordringer.

Visionen fungerer derfor som et fælles pejlemærke for den overordnede udvikling. Skal der skabes sammenhængende løsninger, er der imidlertid behov for konkretisering og operationalisering af visionen. Det starter med en række fælles principper (beskrevet i dette kapitel) og ud fra vision og principper, beskrives et mere konkret teknisk målbillede og anbefalinger til et såkaldt trust rammeværk, der skal understøtte det tekniske målbillede (selvstændige kapitler i denne rapport).

Den nuværende situation og behov for ændring

Utilstrækkelig koordinering og styring

Den grundlæggende motivation for at gennemføre denne analyse er 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) – jf. Appendiks 1: Kommissorium for analyse vedr. sikkerhedsstandarder og -løsninger.

I det omkostningseffektive ligger naturligvis spørgsmålet om man i tilstrækkelig grad har skabt en koordineret udvikling, hvor erfaringer gjort på et område, kommer andre områder til gode, og om løsninger fundet på et område kan genbruges indenfor andre områder (frem for "at den dybe tallerken skal genopfindes" mange gange). Flere forskelligartede løsninger på det samme problem kan også give ekstra omkostninger til vedligehold og det vil være mere ressourcekrævende at skabe sammenhæng indbyrdes.

I første omgang må spørgsmålet om tilstrækkelig koordinering besvares som et "nej". Der er ikke formuleret en fælles strategi med en fælles vision og fælles principper at bygge

sikkerhedsløsninger efter. Der er heller ikke formuleret en arkitekturvision eller et fælles teknisk målbillede, som de enkelte løsninger kan orientere sig i forhold til.

Denne analyse viser, at det rent faktisk er muligt at opstille et fælles målbillede med afsæt i en fælles vision, men det er ikke en øvelse man gør en gang for alle. Strategi, vision, principper, målbillede, fælles standarder mm. er noget som løbende skal vedligeholdes i processer, der sikrer involvering af parterne. Men styregruppen for det Fællesoffentlige Brugerstyringsprojekt er nedlagt og erstattet af en mere driftsnær NemLogin styregruppe, der p.t. ikke er virksom. OIO komitéen for arkitektur og standarder, der før stod for den standardisering, der gik på tværs af domæner er nedlagt og ikke erstattet af en anden gruppe.

Den fælles udvikling har ikke kunnet understøtte de enkelte domæners behov tilstrækkeligt

På sundhedsområdet er kerneydelser som undersøgelse, behandling og pleje ikke noget som kan automatiseres på samme måde som nogle afgørelser kan automatiseres indenfor forskellige forvaltningsområder. Skal man digitalisere sundhedsvæsenet handler det derfor i højere grad om at skabe it-systemer, der understøtter fagpersoner i at løse deres opgaver. Dette sker via specialiserede fagsystemer. En væsentlig del af digitaliseringsindsatsen består derfor i at lade fagsystemer få adgang til data der ligger i andre systemer. Sundhedsområdets fokus har derfor været på system-til-system kommunikation. Man har derfor siden 2008 kunnet lave sikker web service integration baseret på security tokens udstedt af en IdP/STS. Det er først her i 2014 at tilsvarende bliver muligt via NemLogin.

På undervisningsområdet har det været nødvendigt at understøtte løsninger med børn, unge, deres forældre samt ansatte på institutioner som brugere. Uni-login understøtter autentifikation af brugere ud fra Nemlogin, men da en del af deres brugere er unge, er dette ikke eneste mulighed (NemId gives kun til personer over 15 år). Uni-Login har i dag over 1 mio. brugere.

Såvel undervisnings- som sundhedsområdet har brug for at dække private tjenesteudbydere. Eksempelvis er der data i praksissystemer, apotekssystemer, hospitalssystemer på private sygehuse og klinikker, nationale telemedicinske løsninger (f.eks. "sår-journalen"), der ejes og drives af private. NemLogin dækker ikke i dag sådanne private serviceudbydere. Det betyder ikke, at man ikke kan anvende NemID, der dækker både offentlige og private virksomheder. Det betyder bare, at private selv må etablere sin autentifikationsløsning. Men denne vil ikke fungere som Single Sign-On til offentlige tjenester.

I regi af det fællesoffentlige brugerstyringsprojekt, er der etableret et "fælles bruger-rettighedssystem" (FBRS). Denne kan benyttes af mindre virksomheder, men understøtter ikke integration til større virksomheder (som regioner og kommuner, hvor man i forvejen har egne brugeradministrationsløsninger). Der er også etableret en fælles fuldmagtsløsning. Denne er tænkt som en fællesoffentlig løsning rettet mod borgerne, men der haves pt. ikke erfaringer med brug heraf.

På sundhedsområdet er der etableret en række sikkerhedsløsninger, der understøtter Sundhedslovens krav til brugerstyring (vedr. behandlingsrelation og negativt samtykke, og bemyndigelse/delegering af sundhedsfagligt arbejde). Disse befinder sig på forskellige stadier: Udvikling, pilotafprøvning og egentlig drift, og anvendelsen heraf varierer.

Samlet set, kan man ikke sige, at de enkelte fagområders (domæners) behov primært er blevet dækket gennem den tværgående, fælles udvikling – heller ikke selvom der har været etableret et fællesoffentligt brugerstyringsprojekt. En strategi, som tager udgangspunkt i aktivt at nyttiggøre de løsninger, der skabes i de enkelte fagområder til det fælles bedste vil måske være mere holdbar end en strategi, der prøver at skabe nye fælles løsninger på områder, hvor der allerede er etableret lokale løsninger.

Vedligeholdelsesbyrden vokser

Danmark er langt med digitaliseringen sammenlignet med andre lande. Omkostningerne ved at have været tidligt ude med digitale løsninger er imidlertid, at man har skabt egne løsninger på de digitaliseringsudfordringer man har mødt. Hvis ikke man løbende migrerer over på markedsløsninger og –standarder, efterhånden som disse fremkommer, da risikerer man at binde mange ressourcer til vedligeholdelsen og supporten af stadig flere løsninger (eller man risikerer, at løsningerne ikke vedligeholdes i samme omfang som markedsløsningerne).

Utilstrækkelig sikkerhed

Løsningerne har i dag ikke brugeren i centrum. Serviceudbydere har ofte deres egne registre over brugere[8]. Borgeres muligheder for at administrere identitetsinformation, der er videregivet til en serviceudbyder, er begrænsede (eller ikke eksisterende).

Samme person har brug for at huske brugernavne og kodeord på en lang række tjenester (privat og arbejdsmæssigt). Da dette ikke er muligt for et så stort antal tjenester, genbruges brugernavne og kodeord mellem de forskellige tjenesteudbydere. Kommer man til at registrere sig ved en uærlig tjenesteudbyder, har man derved givet akkreditiver som tjenesteudbyderen kan bruge til at få adgang (i dit navn og eventuelt med din betaling) til en række andre tjenester. Serviceudbydere, der opbevarer identitetsinformation er også mål for angreb. Selv store private og offentlige registre med identitetsinformation er blevet hacket, og informationen herfra er blevet brugt til at skaffe sig uberettiget adgang til andre tjenester. Dette er ikke alene en privat risiko der løbes her, identitetsinformation kan også bruges til at skaffe sig adgang til systemer på ens arbejdsplads.

Dansk IT har for nylig udsendt en pressemeddelelse, hvor man gør opmærksom på problemer med håndtering af CPR-numre. Her nævnes, at der ifølge Datatilsynet er omkring 70 sager årligt (en syvdobling på 6 år), hvor offentlige myndigheder er kommet til at lække oplysninger om CPR-numre, og at 47.000 danskere ifølge Danmarks Statistik udsættes for identitetstyveri (hvor andre personer udgiver sig for at være en). En stor andel af misbruget sker ifølge Dansk IT med afsæt i et cpr-nummer. Med en andens cpr-nummer i hånden kan en it-kriminel ofte få lov til at købe varer ind i andres navn, oprette låneaftaler og få fat i personfølsomme oplysninger.

[8] Med etableringen af NemID er man begyndt at ændre på denne situation, og NemID løsningen passer da også fint ind i en vision for fremtidig brugerstyring (se senere). NemID er dog mest benyttet til borgerrettede løsninger (og primært i den finansielle sektor og i den offentlige sektor). Internt i private og offentlige virksomheder benyttes fortsat en række forskelligartede sikkerhedsløsninger.

I den amerikanske "National Strategy for Trusted Identities in Cyberspace" [NSTIC] refereres til tal, der siger, at over 10 mio. amerikanere hvert år er ofre for identitetstyveri (vurderet 2010) og at konsekvensen for en borger let løber op i 130 timers arbejde (vurderet 2006) med at etablere nye identitetsoplysninger og akkreditiver.

Hvis der er en tjeneste, som en borger ønsker adgang til, sker dette altså i dag ud fra en kalkuleret risiko i forhold til beskyttelsen af personinformation.

Sårbarhed

Hvis løsninger alene bygges op omkring en enkelt eller få Credential Service Providers og Identity Providers, så bliver man meget sårbare overfor angreb eller fejl. I 2013 oplevede man hvordan en række offentlige tjenester var utilgængelige, da NemID ikke fungerede efter en Java-opdatering.

Tendenser

Forretningsmæssige tendenser

Tendens 1: Bedre udnyttelse af data er en afgørende faktor for bedre offentlig service

Det er kendetegnende for de offentlige digitaliseringsstrategier, at mere end halvdelen af de opstillede initiativer handler om deling af oplysninger på tværs af organisationer og sektorer. De offentlige aktører betragter alle effektiv dataforvaltning og -adgang som en forudsætning for effektivisering og kvalitetsudvikling af såvel forvaltning som levering af service/ydelser.

På sundhedsområdet forventes den største gevinst at kunne realiseres i forbindelse med den enkelte patients pleje og behandling. Når patientens forløb gennem sundhedsvæsenet bliver mere sammenhængende kan de enkelte parter basere sig på oplysninger der allerede findes hos andre parter. Det kan føre til færre gentagne undersøgelser, færre forgæves plejebesøg hvis patient er blevet indlagt, og unødvendige kontrolbesøg hvis patients egne målinger kan vurderes af klinisk personale uden at patienten møder fysik op.

Andre gevinster vedrører bedre styring og planlægning. Deling af oplysninger på tværs af parter kan biddrage til et bedre og sammenhængende billede af hvilke indsatser i forhold til fx kvalitet og kapacitet der er behov for. De samme oplysninger ønsket anvendt både på overordnet statsligt niveau, på et organisatorisk niveau hos regioner og kommuner samt på et lokalt niveau på de enkelte afdelinger, plejehjem og lægepraksisser.

Endelig er der en række gevinster der kan hentes ved mere effektiv tilvejebringelse af oplysninger. Der foregår stadig en del dobbelt-registreringer, hvor både behandler, plejer og borger efterhånden forventer at oplysninger afgivet til en part også er tilgængelig for andre parter. Hvor det tidligere ofte udelukkende var de sundhedsfaglige personers ansvar at registrere oplysninger, ses der nu også en tendens til at lade borgeren selv registrere en række af oplysninger til brug ved pleje og behandling.

Tendens 2: Mod borgercentriske løsninger

Digitaliseringen skal understøtte overgangen til et sundhedsvæsen, der i højere grad lægger vægt på forebyggelse. Det er i den forbindelse vigtigt at stille relevante oplysninger til rådighed for den enkelte borger, og hjælpe vedkommende i selve forebyggelsesindsatsen samt evaluere og følge op på denne. Digitaliseringen skal herunder lette den enkeltes adgang til at se og afgive egne oplysninger, gå i dialog og danne netværk med andre patienter og sundhedsprofessionelle. Patienter med kroniske sygdomme skal gives mulighed for aktivt at påvirke sin egen helbredstilstand fx gennem shared care-løsninger, monitorering og behandling i hjemmet mm.. Inddrages borgeren som et aktiv i egen behandling vil det være naturligt (nødvendigt?) at skabe sikringsforanstaltninger, der inddrager borgeren mere aktivt i styring af informationsstrømmen.

Tendens 3: Øget kriminalitet i Cyberspace

Efterhånden som samfundet digitaliseres og værdifulde ydelser og betalinger kan leveres elektronisk over Internet, er kriminaliteten også flyttet herover. Senest vurderes kriminaliteten også at være statsstøttet (industrispionage).

I den aktuelle trusselsvurdering fra Center for Cybersikkerhed [CFCS-trusselsvurdering] nævnes, at centret har viden om såkaldte APT-angreb (Advanced Persistent Threat) på danske myndigheder, organisationer og virksomheder.

Et forholdsvis avanceret cyber-angreb ramte således Erhvervs- og Vækstministeriet i 2012. Det lykkedes her angriberen at få indblik i infrastrukturen bag de forskellige net tilhørende ministeriet, få adgang til centrale servere og data og til net, som kunne skabe forbindelse til underliggende styrelsers net. For at stoppe og håndtere angrebet måtte Erhvervs- og Vækstministeriet i en periode lukke en række it-systemer ned.

Tilsvarende avancerede målrettede angreb har siden fundet sted mod private virksomheder (herunder virksomheder af betydelig størrelse og betydning for Danmark) og organisationer i Danmark. Center for Cybersikkerhed er således bekendt med kompromittering af flere virksomheder indenfor højteknologiske sektorer. Samtidig vurderer centeret, at det er meget sandsynligt, at flere virksomheder allerede er blevet kompromitteret af APT-grupper uden at vide det.

Teknologiske tendenser

Tendens 4: Fra lokale til globale sikkerhedsløsninger

Den forretningsmæssige tendens med at udnytte data bedre (og anvende dem i flere sammenhænge) afføder et behov for flere og tættere integrationer af systemer. Dette betyder også, at sikkerhedsløsninger flytter sig fra at være knyttet til det enkelte system over mod at være enterpriseløsninger (IM-løsninger, directory services etc.). Og nu skal sikkerhed også håndteres på tværs af organisationer.

Referencearkitekturen for informationssikkerhed peger på, at systemløsninger og enterpriseløsninger, der ikke passer ind i en fælles ramme, gør det svært at realisere visionerne om tilgængelighed af data på tværs af parter. Referencearkitekturen giver et meget

overordnet og teknologineutralt bud på en ramme for sikkerhedsløsninger på sundhedsområdet. Denne analyse er med til at konkretisere rammen i forhold til web teknologier (men ser altså ikke alene på sundhedsområdet).

Sikkerhedsløsninger på enterprise niveau bygger typisk på en arkitektur, hvor brugerdatabaser løbende synkroniseres. Dette er en velegnet arkitektur, når der skal skabes sammenhæng i mange forskelligartede løsninger (og hvor muligheden for at ændre i de enkelte løsninger måske er begrænsede) indenfor samme organisation. Men arkitekturen giver en række udfordringer, når sikkerhedsløsninger skal hænge sammen på tværs af mange selvstændige offentlige og private parter.

Såfremt kommunikation mellem parter baseres på web teknologi er der imidlertid fremkommet et alternativ. Her er der standarder, der understøtter fødererede løsninger modnet (d.v.s. løsninger, der bl.a. baseres på brugeradministration og autentifikation ved andre parter), og der er opstået et marked for sådanne løsninger.

Hvor man for 5-10 år siden ville basere udviklingen af en national infrastruktur på synkonisering af brugerkataloger, har markedsudviklingen og modningen af standarder betydet, at man i dag vil gå i en fødereret retning.

Tendens 5: Fra computernetværk mod "The Internet of Things"

Hvor internettet oprindeligt var en sammenbinding af stationære computere, benyttes det i dag af en række enheder.

Antallet af mobile enheder (tablets, smartphones etc.) med adgang til Internet overstiger således i dag antallet af stationære computere (servere, desk top PC etc.) med adgang til Internet. Udviklingen og billiggørelsen af små microprocessorer med så lavt strømforbrug, at de kan holdes i gang i mange år af et lille batteri og/eller solceller, har betydet at mange ting udstyres med computerkraft i dag, hvad enten der er tale om måleapparater (f.eks. i armbånd, implantater, vandpumper, termostater, el-målere, eller hårde hvidevarer), fjernsyn, kameraer eller meget andet.

Dette har betydning for sikkerhedsløsninger på flere områder. Eksempelvis skal sikkerhedsløsninger fremover fungere på flere platforme. Samtidig ændres der grundlæggende ved sikkerhedsmodellerne; det bliver sværere at beskytte data og it-systemer gennem opretholdelse af "perimetersikkerhed". Vejen ind i et privat netværk går ikke nødvendigvis gennem en firewall opstillet mellem netværket og internetforbindelsen. En hacket smartphone med adgang til et lokalnet kan give udefrakommende adgang til ressourcerne på det private netværk. En hacket vandpumpe, der rapporterer måledata ind til vandværkets netværk kan give hackerne adgang til vandværkets netværk og servere.

Tendens 6: Mere og mere standardiseres

Når løsninger specificeres undersøger man typisk, om der findes standarder at bygge løsningerne på. Er dette ikke tilfældet, bygger man ikke-standardiserede løsninger eller løsninger, der bygger på egne standarder. Dette er eksempelvis sket på området, hvor man i

2005-2006 definerede sin egen web service profil (Den Gode Web Service). Efterfølgende er der fremkommet tværoffentlige og internationale profiler af web services. Så skulle man i dag have fastsat en standard for sundhedsområdet, ville det blive med udgangspunkt i en eller flere af disse.

Dette er en generel tendens. Med en stigende grad af digitalisering følger også en stigende grad af standardisering. Men standardiseringen "halter" altid bagefter de første løsninger. Først når der er opnået erfaringer med forskellige løsninger og der opnås konsensus med hvad der er den bedste måde at løse digitaliseringsudfordringerne på, udvikles der standarder, der kan bruges til at bygge fremtidige løsninger på.

Vision

Visionen skal bidrage til at skabe enighed om, hvad vi gerne vil arbejde hen imod. Den skal give et billede af den fælles retning, som kan kommunikeres til andre i et klart sprog. Der er tale om et idealbillede– måske kan visionen aldrig opfyldes helt, og måske ændres den undervejs, men man arbejder alle i samme retning.

Forretningsvision

Borgeren har frihedsgrader i forhold til hvem de vil betro identitetsinformation og andre personlige oplysninger, som skal benyttes til at få adgang til services. Disse gør det muligt for serviceudbydere at få verificeret sikkerhedsinformation, men der videregives kun selektiv (for servicen nødvendig) information og kun med borgerens samtykke hertil. I den amerikanske "National Strategy for Trustet Identies in Cyberspace" udtrykkes dette i princippet om, at "Identity Solutions will be Privacy-Enhancing and Voluntary". Der gives følgende eksempel:

"Antonio, age thirteen, wants to enter an online chat room that is specifically for adolescents, between the ages of twelve and seventeen His parents give him permission to get a digital credential from his school. His school also acts as an attribute provider: it validates that he is between the age of twelve and seventeen without actually revealing his name, birth date or any other information about him The credential employs privacy-enhancing technology to validate Antonio's age without informing the school that he is using the credential Antonio can speak anonymously but with confidence that the other participants are between the ages of twelve and seventeen." [NSTIC] s. 11.

En medarbejder i en offentlig eller privat virksomhed kan få adgang til information og services ved andre virksomheder uden først at skulle autentificere sig igen, endsige benytte forskellige akkreditiver hertil. Medarbejderen ved, at ens arbejdsmæssige adgang til services logges, men vedkommende kan være sikker på, at der ikke overføres oplysninger, som kan misbruges til at skade medarbejderen som privatperson.

Hvad enten der er tale om medarbejdere i en virksomhed eller borgere i landet, så er autentifikationen fleksibel og tilpasset den situation man står i. Mobile enheder benyttes aktivt som led i autentifikation (eksempelvis kan besiddelsen af en mobiltelefon eller et smart card være en del af autentifikationen).

Arkitekturvision

Arkitektonisk er visionen at skabe et "økosystem", hvor dele udvikles af forskellige offentlige og private parter, og hvor de udviklede dele bidrager til at skabe det samlede system. Gennem brug af standarder skabes løs kobling mellem de forskellige dele (CSP, IdP, STS og Serviceudbydere etc.), som medvirker til, at nye løsninger kan tilføjes og gamle løsninger kan fases ud med en minimal effekt på det samlede system. Serviceudbydere og serviceaftagere kan gøre brug af forskellige CSP'er og IdP'er etableret af forskellige parter.

Betroede kilder til sikkerhedsinformation og/eller til verifikation af sikkerhedsinformation (dvs. Attribute Providers) findes ligeledes ved forskellige parter. Oplysninger om Sundhedsfaglig autorisation kan hentes fra Sundhedsstyrelsen, oplysninger om ansættelsesforhold og arbejdsfunktion kan hentes fra arbejdsgiver, oplysninger om kreditværdighed kan hentes fra banker og kreditvurderingsbureauer etc.. Sikkerhedsinformation kan fremskaffes fra forskellige kilder, og serviceudbyder kan have forskellige grader af tillid til disse.

Økosystemet skal indeholde mekanismer til lokalisering af Credential Service Providers, Identity Providers og Attribute Providers, og til fremskaffelse af oplysninger om disse, der gør det muligt for serviceudbydere at vurdere hvilken grad af tillid de kan have til information herfra.

Økosystemet giver en robusthed. Hvis en kilde til sikkerhedsinformation er utilgængelig, kan serviceaftager vælge en anden kilde, som serviceudbyder har tillid til. Eksempelvis kan en Løn- og Personalefunktion på et sygehus udtale sig om en persons sundhedsfaglige autorisation, da denne blev verificeret i forbindelse med ansættelse. Informationen har ikke samme kvalitet, som et opslag i Sundhedsstyrelsens autorisationsregister, da dette er den mest opdaterede kilde til informationen (personen kan efter ansættelsen have fået indskrænket eller frataget sin autorisation), men kan for mange tjenester være tilstrækkelig (især i en nød-situation). Tilsvarende vil SKAT kunne sandsynliggøre et arbejdsmæssigt tilknytningsforhold til en organisation (f.eks. ansættelsesforhold), selvom den kilde man kan have størst tillid til, ligger ved den arbejdsgiver der indgår en aftale med personen.

Værdier

[Afventer bidrag fra arbejdsgruppe (kommune, region og sundhed.dk)]

Overordnede principper

I de efterfølgende kapitler opstilles en målarkitektur (og der peges på standarder) der konkretiserer ovenstående vision. Denne konkretisering bygger på en række principper:

Princip	Genbrug så vidt muligt eksisterende løsninger
Rationale	Såfremt løsninger nyder stor udbredelse kan de ikke udskiftes fra den ene dag til den anden, men må være udgangspunktet for en migreringsstrategi, der flytter området fra den nuværende situation til den ønskede fremtidige situation (beskrevet ved vision og målbillede). Samtidig bør afholdte investeringer så vidt muligt beskyttes (under

	respekt for at ændringer kan være nødvendige for at opnå den ønskede fremtidige sammenhæng og synergieffekt).
Implikationer	

Princip	Benyt de standarder, som har den bedste markedsdækning
Rationale	Anvendelsen af standarder muliggør udskiftning af løsninger eller delløsninger. Ved at bruge markedsløsninger står man ikke alene med udvikling, support og vedligehold af løsningerne.
Implikationer	Lad markedsunderstøttelse indgå i kriterierne for valg af standarder. Dette sikres i denne undersøgelse ved brug af det europæiske CAMMS rammeværk. For sygehusvæsenet, der arbejder meget internationalt, og som derfor ofte kan understøttes af internationale løsninger, er det væsentligt at lægge sig op ad de internationale standarder, som markedet understøtter.

Princip	Sikkerhedsløsninger, som ikke er brugervenlige, er ikke sikre
Rationale	Hvis det bliver for besværligt at løse sine opgaver, omgås sikringsforanstaltningerne (hvis mange forskellige personlige kodeord eksempelvis skal huskes, vil man enten skrive dem ned, eller benytte samme kodeord flere steder).
Implikationer	Understøt flere akkreditiver, som brugeren kan vælge imellem. Understøt Single Sign-on (SSO) på tværs af parter.

Princip	Driftseffektivitet (tilstrækkelig performance) er en forudsætning for at løsninger anvendes
Rationale	En brugervenlig og sikker løsning, der giver en god understøttelse af arbejdsgange vil ikke blive anvendt, hvis den er for langsom.
Implikationer	Undgå alt for mange eksterne opslag, benyt infrastrukturen til at optimere performance, undgå unødvendige parsninger (herunder mapninger, kryptering og dekryptering) af beskeder, indfør kun mapninger, hvis det kan gøres tilstrækkeligt effektivt.

Brugsscenarier

Hovedparten af kommunikation foregår i dag indenfor de enkelte organisationer, men tendensen er at data i større og større omfang skal kommunikeres på tværs af forskellige parter (jf. tidligere beskrivelse af tendenser). Dette afføder et behov for at kunne kommunikere på tværs af eksisterende sikkerhedsløsninger. Dette afsnit beskriver nogle konkrete scenarier, der skal kunne understøttes af fremtidige sikkerhedsløsninger.

Sundhedsjournalen

Regionernes svar på udfordringen med at give adgang til patientoplysninger på tværs af forskellige elektroniske patientjournaler (EPJ) er at give sundhedspersoner adgang til opslag i den fællesregionale sundhedsjournal (web applikation på den fællesoffentlige sundhedsportal, Sundhed.dk). Skal dette fungere i praksis, er det nødvendigt at gøre det let for sundhedspersonerne at foretage opslag i Sundhedsjournalen direkte fra eget EPJ-system.

Såfremt en sundhedsperson har autentificeret sig via eget EPJ-system på et tilstrækkeligt højt niveau til at få adgang til Sundhedsjournal og nationale services, da skal vedkommende ikke re-autentificere sig ved opstart af Sundhedsjournal, eller hvis denne henter data fra bagvedliggende nationale tjenester. Tilsvarende skal det være muligt at overføre oplysninger om hvad det er for en patient man kigger på fra EPJ-systemet til sundhedsjournalen (oplysninger om patientkontekst), så man ikke her skal til at fremsøge den samme patient igen.

Regionerne ønske også at Sundhedsjournalen kan tilgås direkte (ikke via EPJ-system eller andet fagsystem). Da brugere af sundhed.dk i dag autentificeres ved brug af den fællesoffentlige login-tjeneste, NemLogin, da skal de ikke re-autentificeres for at få adgang til nationale tjenester. Dette kræver at kommunikationen beriges med de samme sikkerhedsoplysninger om brugeren, som man ville have fået ved at foretage sign-on på den nationale service fra sit EPJ-system.

[Ovenstående scenarium suppleres med et scenarium, hvor kommunalt system skal tilgå en national service på sundhedsområdet]

Teknisk beskrivelse af eksisterende løsninger

Dette kapitel prøver at give et overblik over de løsninger, som er medtaget i analysen.

Overblikket bruges dels til at sikre, at målbilledet for sammenhængende sikkerhedsløsninger formuleres med afsæt i de eksisterende løsninger (jf. de overordnede principper). Endvidere benyttes overblikket til at identificere de standarder og løsningskomponenter, som analysen skal forholde sig til efterfølgende.

Systemlandskabet, som det ser ud i dag, består af en lang række IT-systemer, sikkerhedsdomæner og føderationer, hvor indenfor man har søgt at skabe Single Sign-On (SSO). Der er overordnet to scenarier, som har interesse for denne analyse:

- Det ene scenarium vedrører 'web services', der tillader IT-systemer at lave system-til-system integrationer. Her er et kendt eksempel sundhedsområdets SOSI-føderation.

- Det andet scenarium vedrører 'web applikationer', hvori en SSO løsning tilbyder Single SignOn til alle brugervendte systemer, der er inkluderet i føderationen og som tilgås via en Internet web browser. Scenariet er måske bedst kendt i dag fra NemLog-in føderationen.

Dertil kommer en række mere specifikke scenarier, der på forskellig vis går på tværs af de to ovennævnte teknologier. Grundlæggende er der to tværgående scenarier, nemlig a) at en web applikation kalder en bagvedliggende web service - uden at brugeren, der har autentificeret sig overfor webapplikationen behøver at re-autentificere sig overfor web servicen og b) at et IT-system, der tidligere har autentificeret en bruger, kan starte en web applikation uden at brugeren behøver at re-autentificere sig overfor denne[9].

Endelig er der et tredje overordnet scenarium, hvor fokus indtil videre ikke har været på brugerautentifikation og SSO:

- Dette tredje scenarium vedrører (asynkron) forsendelse af elektroniske beskeder fra et system til et andet

Der er i dag implicit tillid til at det system, som afsender en besked har sikret, at den sendte information er skabt af en autoriseret bruger og tilsvarende er der implicit tillid til, at det system, der modtager en besked, kun gør information herfra tilgængelig for personer, som har retmæssig adgang hertil.

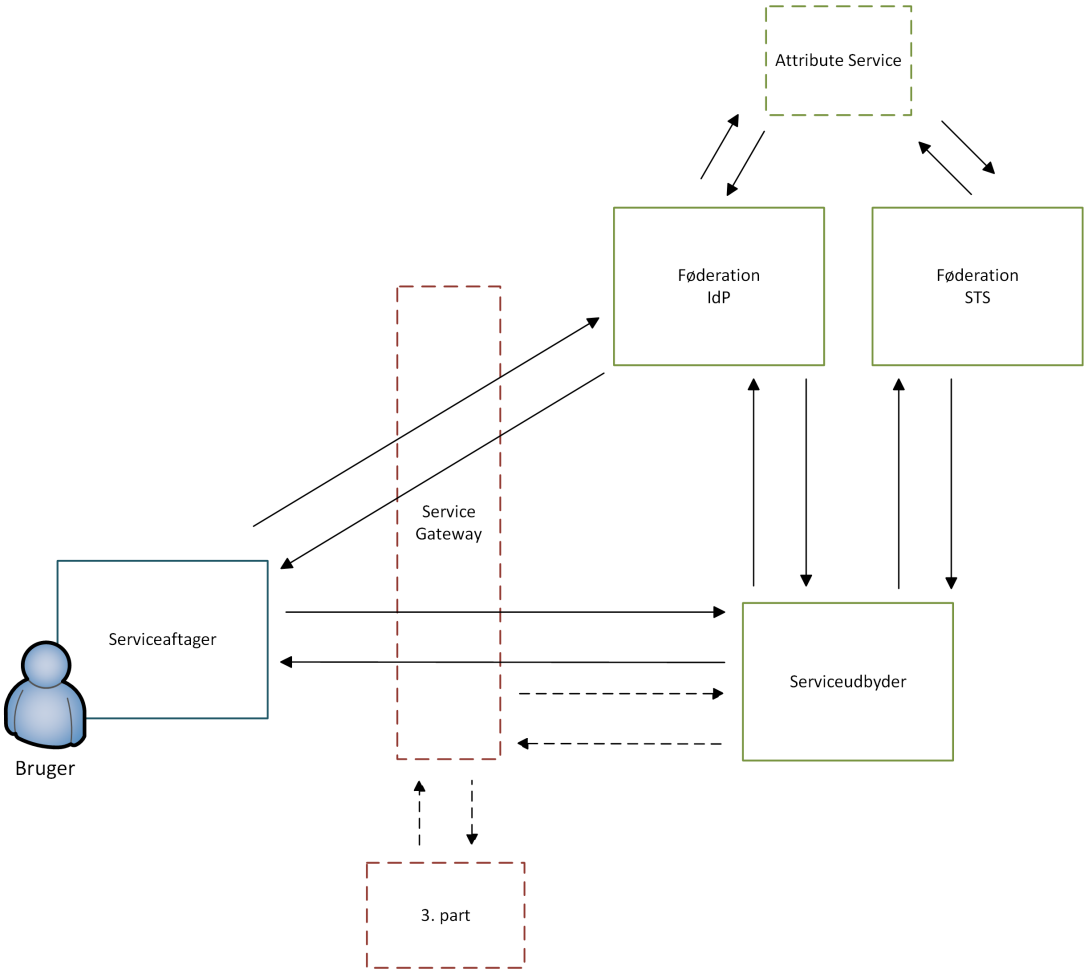
Ønsker man at styrke sikkerheden ved eksempelvis eksplicit at sende elektronisk bevis for, at det er en autoriseret læge, der har sendt en recept, da er det ligeså relevant at overføre det

[9] Der er ikke nogen gængs betegnelse for at overføre oplysninger vedrørende en brugersession i et IT-system til en session i en web applikation. Digitaliseringsstyrelsen betegner scenariet "Rich Client to Browser Scenario" (se eksempelvis [OIO-SAML-client-browser]), mens sundhedsområdet har benyttet betegnelsen "Sikker browseropstart". Internationalt er der på sundhedsområdet arbejdet med løsninger, der ikke blot kan overføre oplysninger fra én brugersession til en anden, men som kan holde oplysningerne om eksempelvis bruger og patient synkroniserede mellem sessioner i forskellige applikationer. Denne proces betegnes *Context Management* og den understøttes af udbredte standarder og profiler (f.eks. HL7's CCOW standard og IHE profilen Patient Synchronized Applications, PSA).

bevis, som systemet fik ved autentifikation af brugeren til den sendte besked, således at det ikke er nødvendigt for brugeren at re-autentificere sig, når der skal afsendes en besked.

Det har vist sig, at alle de analyserede løsninger har kunnet beskrives ved samme overordnede (konceptuelle) arkitektur.

Figur 6 nedenfor illustrerer således en generisk arkitektur for SSO løsninger, der rummer alle systemkomponenter, som optræder i en føderation eller et sikkerhedsdomæne i et konkret scenarie.



Figur 6: Generisk arkitektur - alle sikkerhedskomponenter

Centralt i figuren er serviceudbyderen (SP), der udstiller en service til en serviceaftageren. Serviceudbyder kender til hhv. føderationens Identity Provider (IdP) og føderationens Security Token Service (STS). Serviceaftageren anvender IdP'en og STS'en til at blive autentificeret og autoriseret. Serviceudbyderen anvender IdP'en og STS'en til at sikre sig at en serviceaftager har adgang til serviceudbyderens udstillede ressource.

IdP'en og STS'en kan i nogle tilfælde kommunikere med Attribute Services, som indeholder informationer om identiteter og som IdP'en eller STS'en kan anvende til at "blive klogere på" de serviceaftagere, der ønsker at blive autentificeret og/eller autoriseret.

Service Gateway'en er en komponent, der kan være til stede i en føderation, og som er med til at skabe en afkobling mellem serviceudbydere og serviceaftagere (såvel indenfor føderationen som mellem forskellige føderationer), således at de standarder, hvormed en serviceaftager kommunikerer med en service ikke behøver at være de samme, som den pågældende service bygger på (service gateway'en kan oversætte mellem forskellige standarder).

Figuren beskriver principielt også scenariet med asynkron forsendelse og modtagelse af elektroniske beskeder (og man kan da også implementere et sådant scenarium vha. web service teknologi). Sprogbrugen med serviceaftager og serviceudbyder kan dog give anledning til forvirring her (det er modtagesystemet der udstiller en modtageservice og dermed agerer serviceudbyder, og afsendersystemet der dermed agerer serviceaftager).

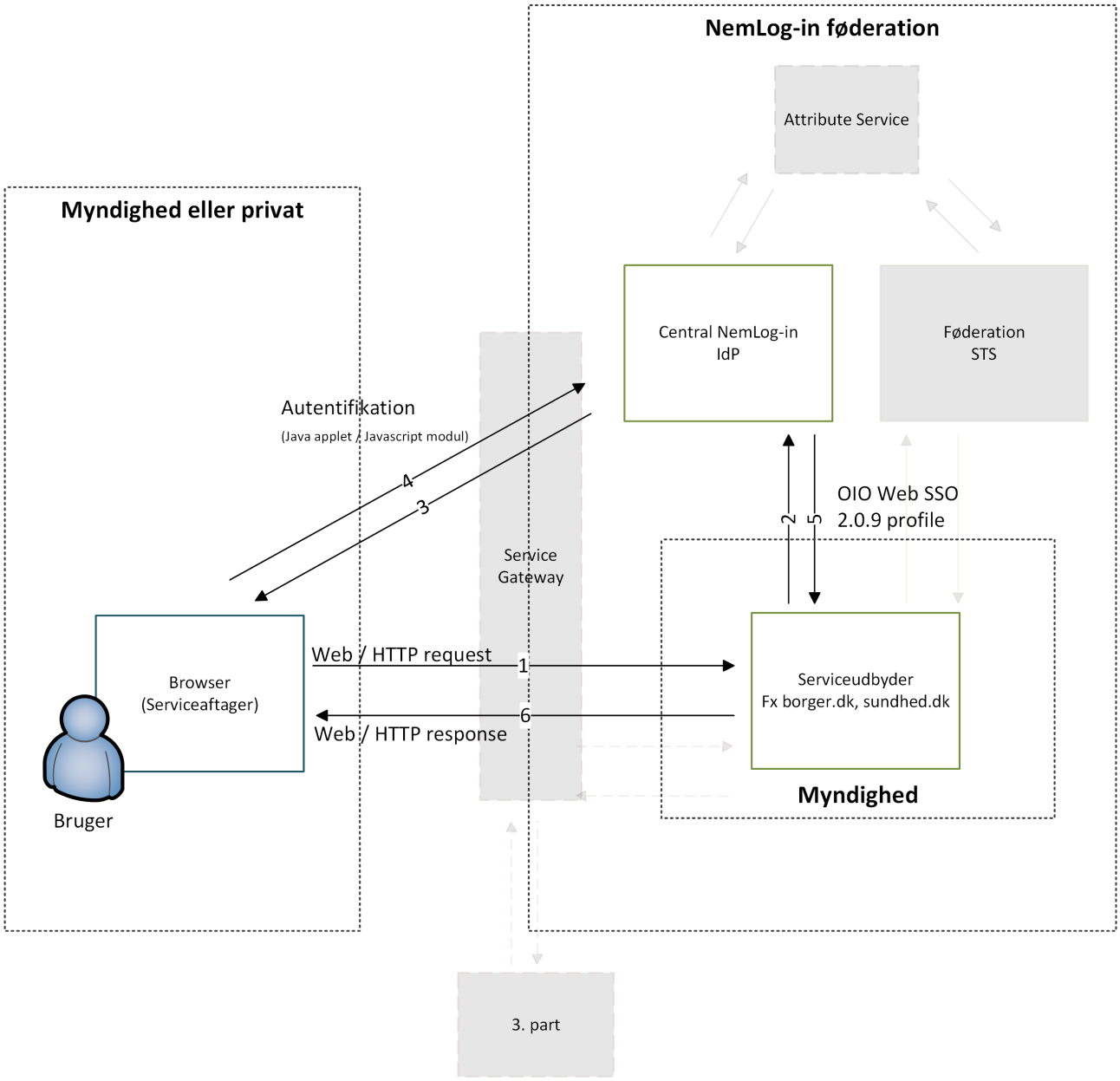
Beskrivelse af føderationer

De konkrete løsninger, der belyses i denne rapport, er alle varianter af den ovenstående generiske arkitektur for SSO. I de efterfølgende afsnit beskrives hvordan de tre eksisterende føderationer, som denne rapport har i særligt fokus, ser ud. Dette beskrives ud fra ovenstående generiske arkitekturbillede.

NemLog-in føderationen

NemLog-in føderationen rummer en række brugervendte IT-systemer, og faciliterer Single Sign-On mellem de inkluderede IT-systemer. NemLog-in føderationen etablerer aktuelt en STS til i højere grad at supportere 'webservice'-scenariet, men denne findes i skrivende stund ikke endnu. NemLog-in føderationen er bygget op omkring en central IdP der realiserer IdP-delen af bl.a. OIO Web SSO profilen [OIO-SAML].

NemLog-in føderationens arkitektur er skitseret i nedenstående figur:



Figur 7: NemLog-in føderationens konkrete SSO løsning

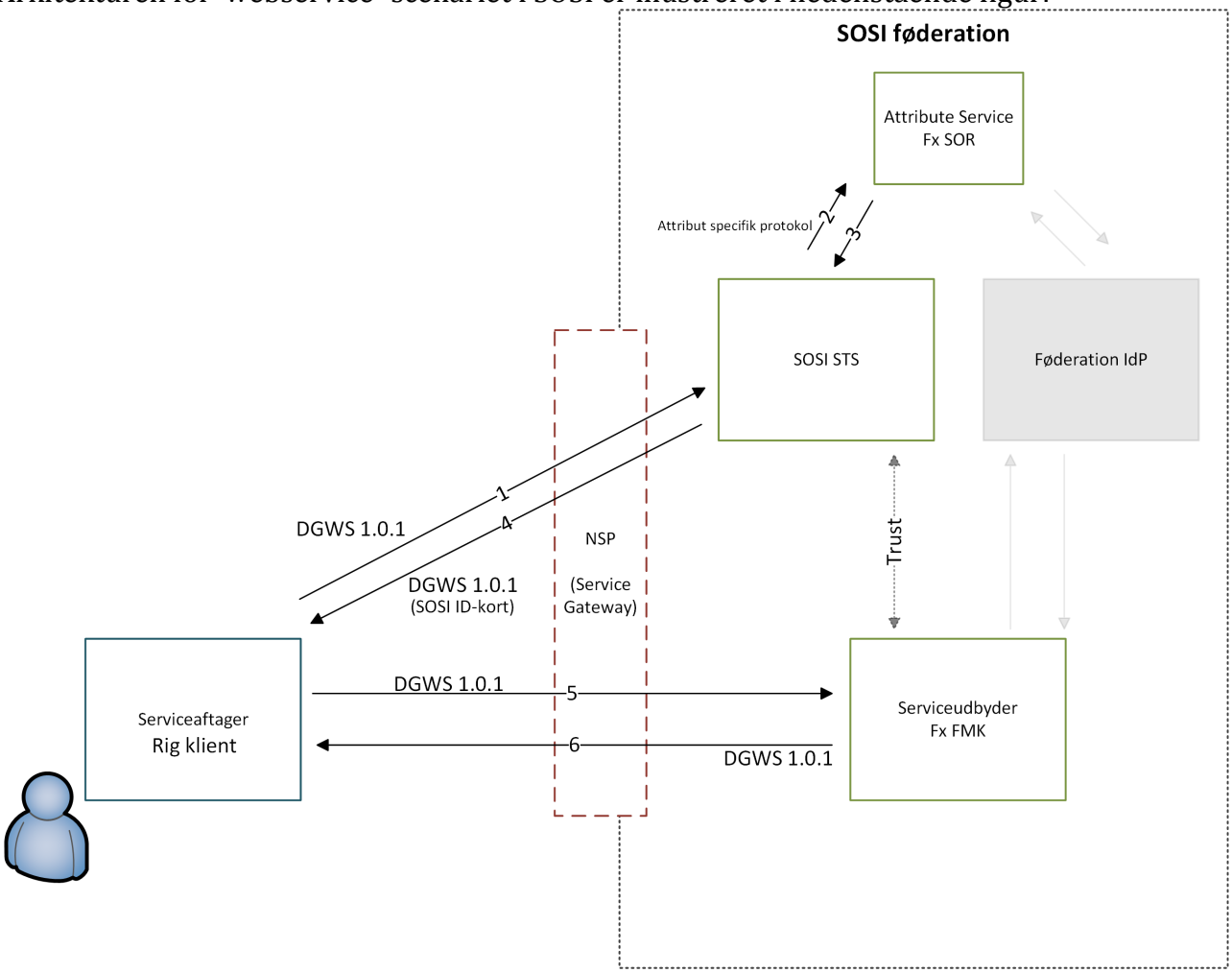
Figur 7 viser hvordan NemLog-in føderationen realiserer den generiske arkitekturmodel for 'web'-scenariet. I NemLog-in føderationen kan brugere tilgå et brugervendt system (skridt 1), som kan anvende NemLog-in IdP'en til at autentificere brugeren (skridt 2+3). Det brugervendte system modtager et token fra IdP'en (skridt 4), som kan anvendes til at autorisere brugeren i systemet. Der opnås Single Sign-On når en bruger tilgår mere end ét brugervendt system, idet brugerens session deles via NemLog-in IdP'en.

I forhold til den generiske arkitekturmodel, er brugeren (og dennes browser) serviceaftager. Serviceudbyderen er et brugervendt IT-system under føderationen, som f.eks. borger.dk eller sundhed.dk. IdP rollen varetages af den centrale NemLog-in IdP. NemLog-in føderationen har som nævnt ikke endnu en STS.

SOSI-føderationen

SOSI-føderationen eksisterer primært i forbindelse med system-til-system integrationer, og har ikke udbredt anvendelse af 'web'-scenariet. Der anvendes typisk 'webservice'-scenariet, der tilllader IT-systemer at kalde andre SOSI-fødererede services ved brug af SOSI sikkerhedstokens (såkaldte "Id-kort"). En undtagelse til dette findes i et hybrid scenarie, hvor der tilbydes Single Sign-On på tværs af 'webservice'-scenariet til 'web'-scenariet. Dette er også kendt som "Sikker browseropstart" og vil blive belyst i detalje senere.

Arkitekturen for 'webservice'-scenariet i SOSI er illustreret i nedenstående figur:



Figur 8: SOSI føderationens konkrete SSO løsning

Figur 8 viser hvordan SOSI føderationen realiserer den generiske arkitektur for 'webservice'-scenariet. SOSI føderationen har en "SOSI STS", der varetager tokenveksling indenfor SOSI føderationen (skridt 1-4), sådan at udefrakommende IT-systemer kan tilgå IT-systemer, der er "dækket" af SOSI føderationen (skridt 5+6), som f.eks. FMK.

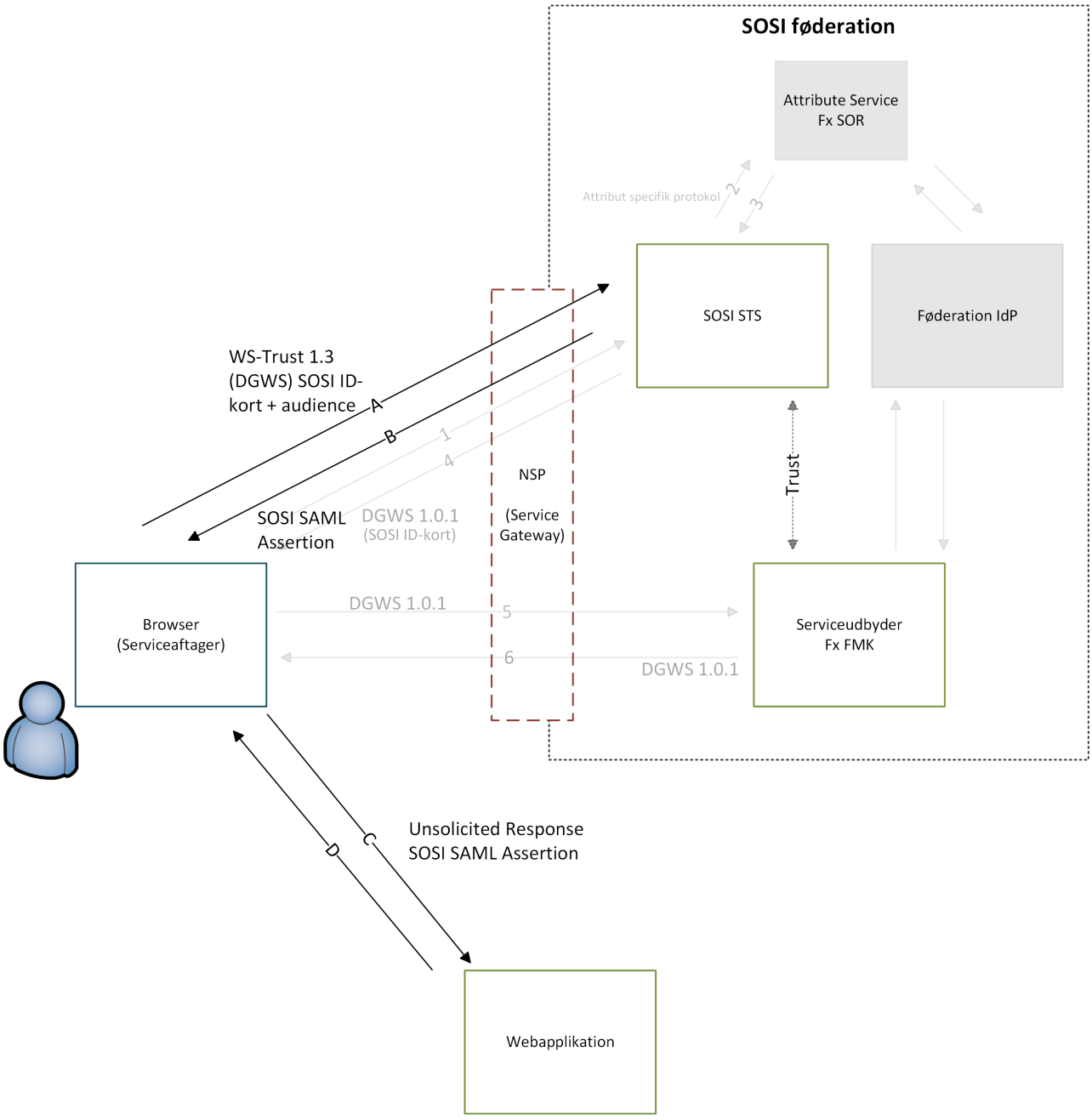
I forhold til den generiske arkitekturtegning tager SOSI STS'en rollen som både Føderations IdP og Føderations STS, idet den står for autentifikation såvel som udstedelse af tokens. Serviceudbyderen kan eksempelvis være FMK, og føderationens IdP og STS gør brug af forskellige Attribute Services, f.eks. Sundhedsstyrelsens Autorisationsregister og RID-CPR

tjenesten hos Nets/DanID. I scenariet illustreret på Figur 8 udfyldes Service Gateway rollen af NSPen.

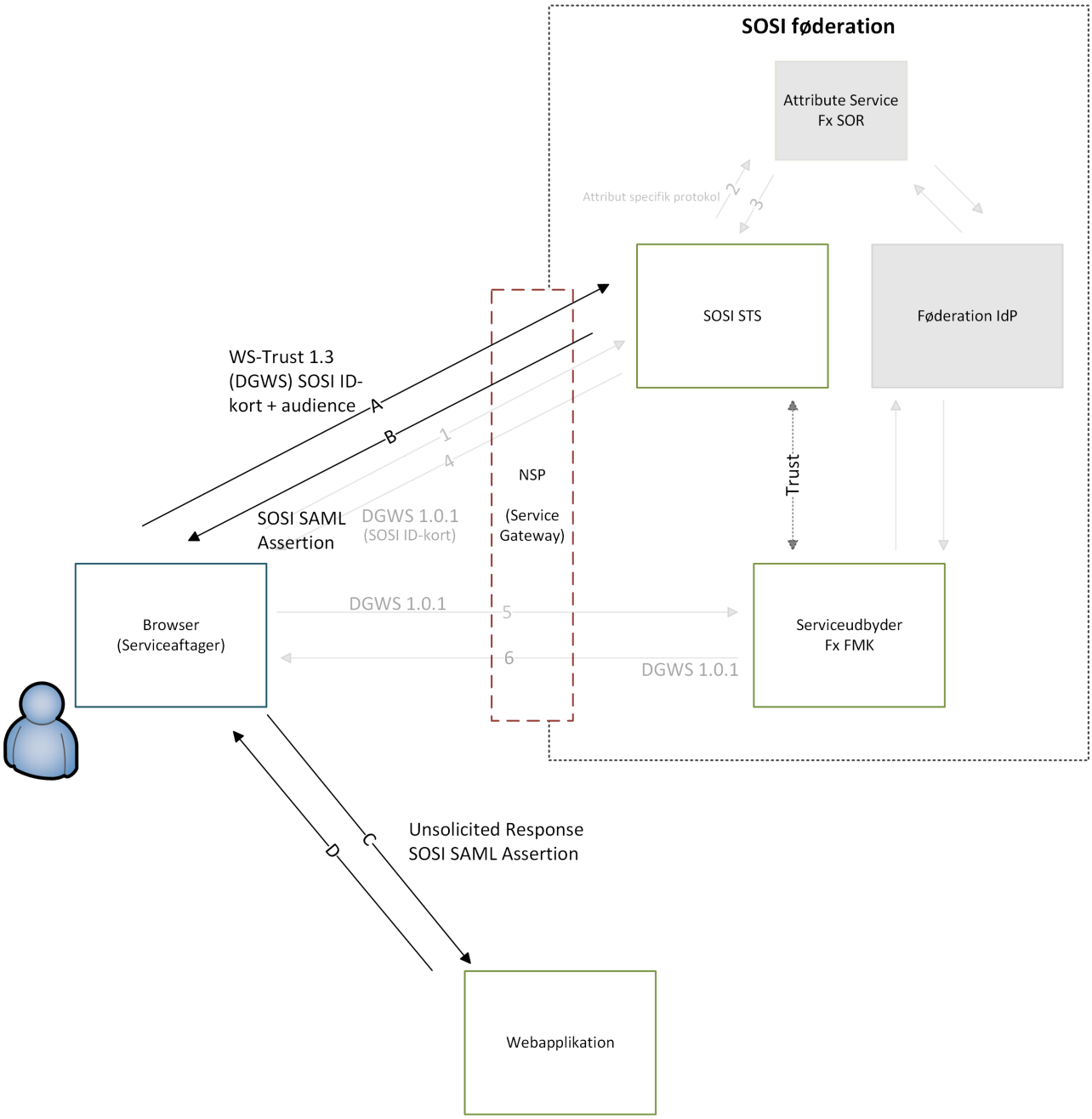
SOSI fra rig klient til web applikation

Et specielt scenarie for SOSI føderationen består i at skabe Single Sign-on mellem systemer, der tilgås via en "rig" klient og en web applikation, der tilgås via en browser. I denne situation skal den stærke autentifikation, der er etableret af brugeren i forbindelse med anvendelse af den "rige" klient, overføres til en browser session. Herved kan brugeren anvende den eksisterende autentifikation som 'log-in' i den webbaserede applikation, og skal ikke logge på igen.

Denne overførsel at autentifikation af brugeren benævnes "sikker browseropstart". Scenariet er illustreret i



Figur 9, hvor der bygges videre på forgående illustration af SOSI arkitekturen.



Figur 9 SOSI Sikker browseropstart

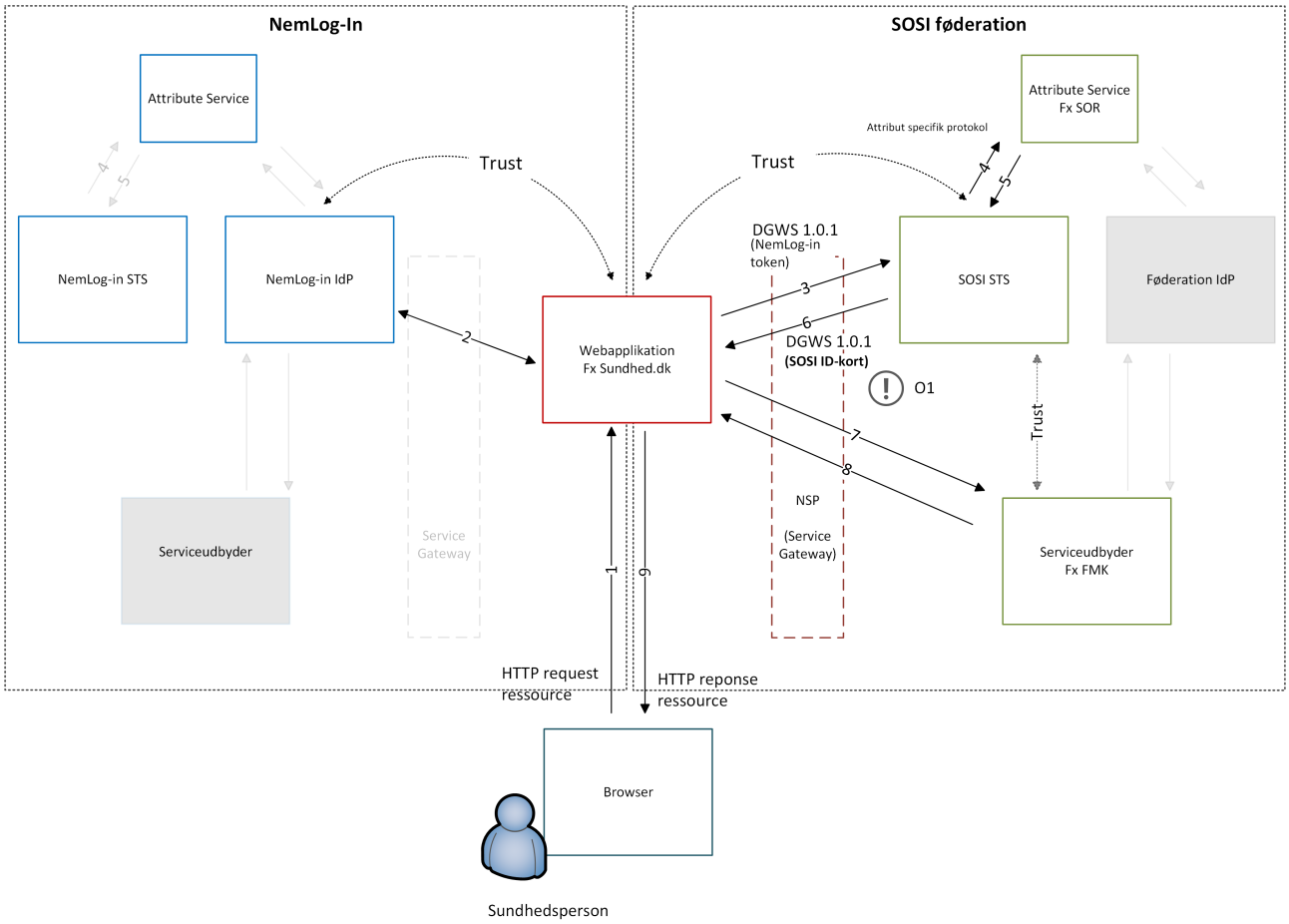
Scenariet vist i Figur 9 bygger videre på det almindelige SOSI scenarie vist i Figur 8, hvilket vil sige at serviceaftageren allerede har fået et SOSI ID-kort – dette er indikeret på Figur 9 vha. de gennemsigtige pile.

I skridt A og B følges Sikker browseropstart standarden idet SOSI STS'en anvendes til at veksle et eksisterende SOSI ID-kort til en SOSI SAML Assertion. Den nye SAML Assertion sendes i skridt C til webapplikationen, der implementerer OIOSAML2 standarden og derfor kan modtage "Unsolicited SAML Authentication Response" fra serviceaftageren i skridt D.

Fra web applikation til SOSI services

Hvis en sundhedsperson er logget ind i en webapplikation vha. sin medarbejdersignatur (f.eks. i NemLogin føderationen) og denne webapplikation skal kalde en service i SOSI føderationen på vegne af brugeren, er det nødvendigt at overføre oplysninger om brugerens autentifikation fra webapplikationen til SOSI servicen.

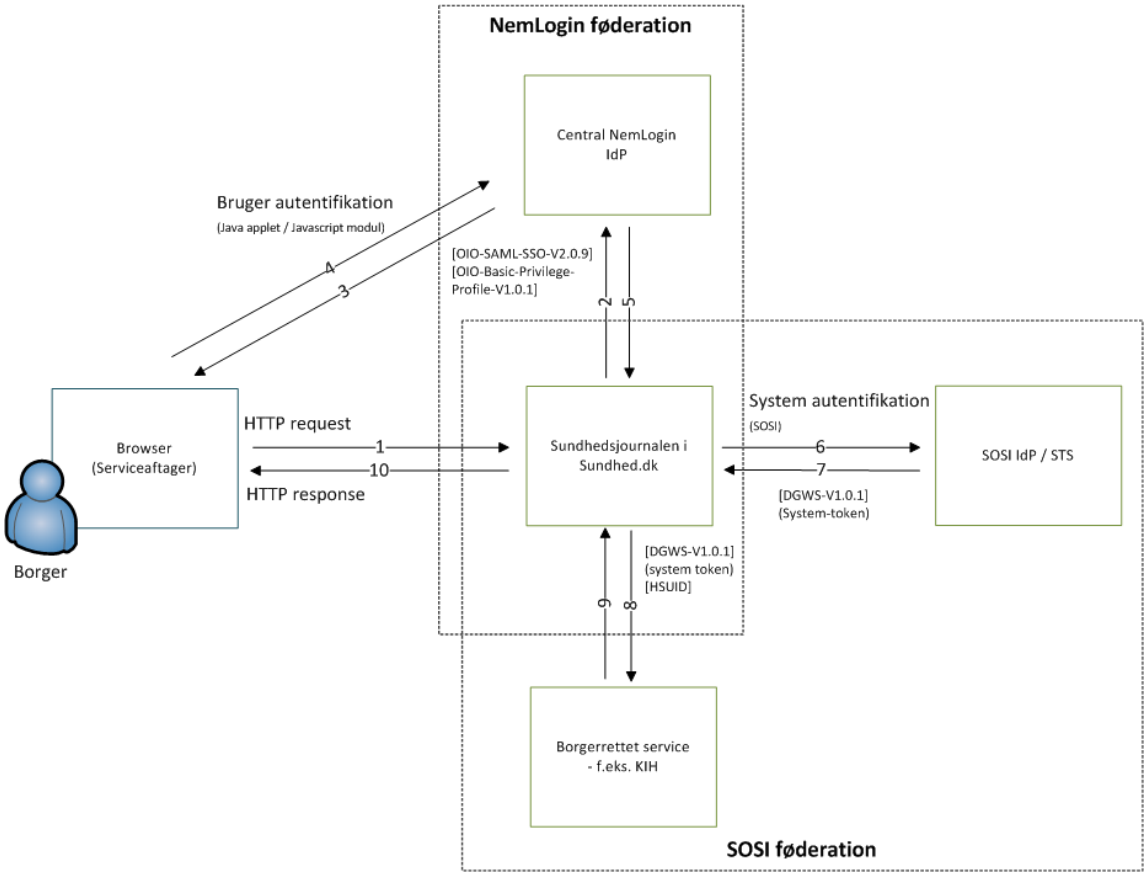
Scenariet er illustreret på Figur 10 nedenfor.



Figur 10: Kald fra webapplikation til SOSI service (sundhedsperson)

Webapplikationen agerer her serviceaftager i forhold til services, der er udbudt under SOSI føderationen idet webapplikationen kalder disse services på vegne af en sundhedsfaglig person. Brugeren er som på normal vis logget ind i webapplikationen via NemLog-in føderationen (skridt 1 og 2). Når webapplikationen skal kalde en serviceudbyder i SOSI føderationen, er denne nødt til at omveksle den sundhedsfaglige persons NemLog-in token til et SOSI ID-kort (skridt 3-6). Dette kan i dag ske vha. SOSI STS'en, der implementerer en snitflade til netop dette formål. Webapplikationen kalder herefter med SOSI ID-kortet serviceudbyderen i SOSI føderationen på vegne af den sundhedsfaglige person (skridt 7+8).

Hvis der er tale om en borger, der tilgår en webapplikation på Sundhed.dk, og denne ønsker at tilgå en SOSI service, kan dette ikke løses på samme måde som ovenfor (med omveksling mellem NemLogin-token og SOSI-ID kort). Dette skyldes, at der ikke findes et SOSI-ID-kort for borgere. I stedet sker der følgende (Figur 11):



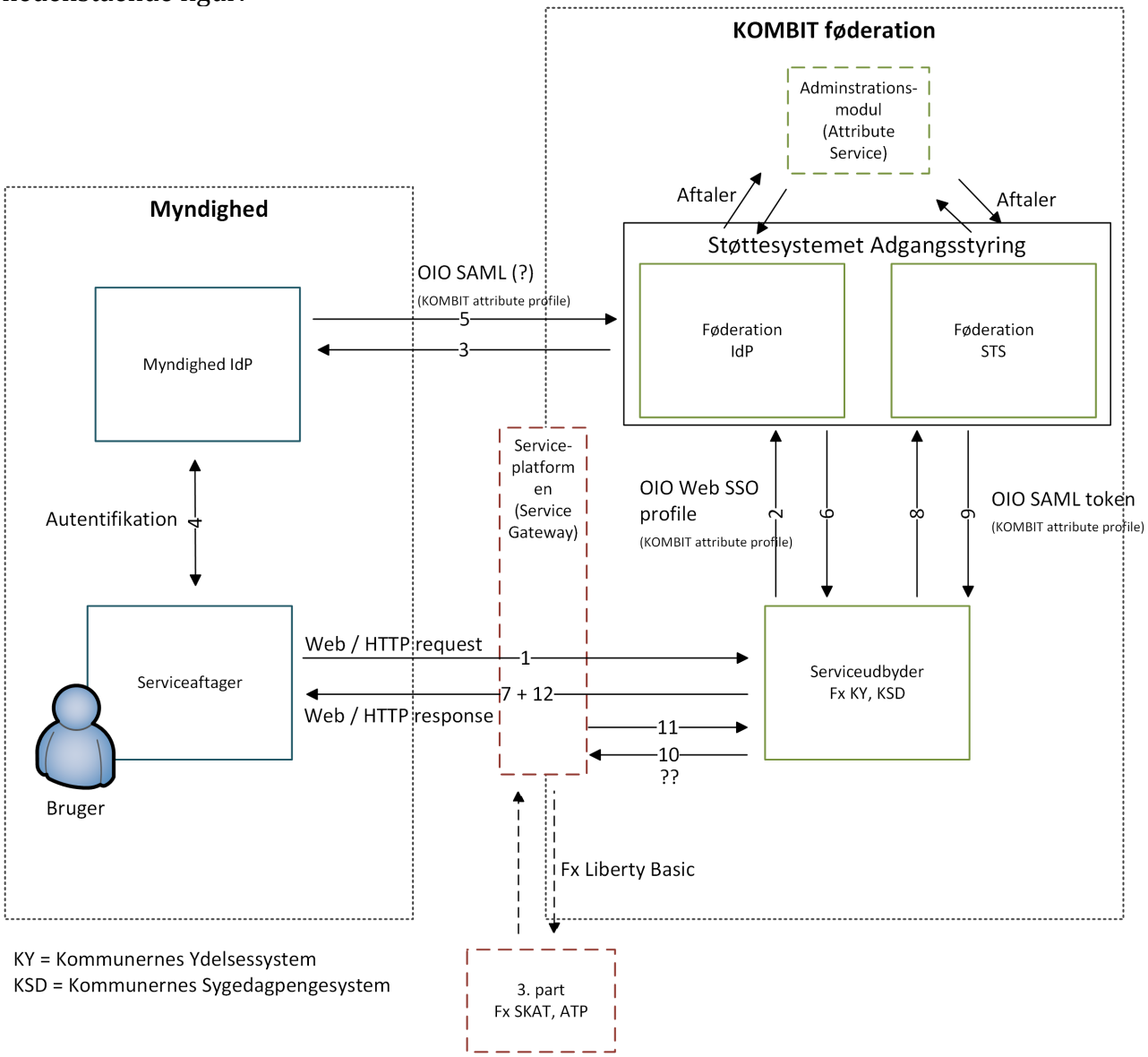
Figur 11 Kald fra webapplikation til SOSI service (borger)

Borgeren autentificeret sig overfor NemLogin IdP ved hjælp af et personligt OCES certifikat (POCES), og får et NemLogin security token som bevis herfor (1-5). Webapplikationen stoler på oplysningerne i dette security token og vil gerne videregive oplysningerne til SOSI serviceudbyder. For at serviceudbyder kan have tillid til, at oplysningerne rent faktisk kommer fra webapplikationen (som serviceudbyder har tillid til), autentificerer webapplikationen sig ud fra et funktions-OCES certifikat (FOCES) overfor SOSI-IdP/STS'en og modtager et SOSI system ID Kort som bevis herpå (6-7). Dette system ID-kort medsendes nu til serviceudbyder som bevis på webapplikationens identitet og de oplysninger om borgerens identitet som webapplikationen hentede fra Nemlogin security tokenet videresendes til serviceudbyder (8) som specificeret i Healthcare Service User Identification Header [HSUID].

KOMBIT-føderationen

KOMBIT-føderationen indeholder i både 'web'- og 'webservice'-scenarierne: Der udstilles flere nye fagsystemer til kommunale medarbejdere via webapplikationer, ligesom disse fagsystemer i høj grad gør brug af system-til-system integrationer med web services. KOMBIT-føderationen er bygget op omkring Den Fælleskommunale Rammearkitekturs [KL-RA] Støttesystem Adgangsstyring [KOMBIT-ADGANG], der binder autentifikation i de enkelte kommuner/myndigheder sammen med Single Sign-On, herunder autorisation, på tværs af systemer, der anvender Den Fælleskommunale Rammearkitektur.

Arkitekturen for KOMBIT-føderationens 'web'- og 'webservice'-scenarier er illustreret i nedenstående figur:



Figur 12 KOMBIT føderationens konkrete SSO løsning

Figur 12 viser hvordan den generiske arkitektur for både for 'web'-scenariet samt 'webservice'-scenariet er realiseret i parallel i KOMBIT føderationen. I KOMBIT føderationen er det eksempelvis KY og KSD, der er serviceudbyder. Serviceaftageren kan enten være en browser eller en klient på brugerens PC[10]. Den Fælleskommunale Rammearkitekturs støttesystem Adgangsstyring tager rollen som både IdP og STS, da støttesystemet anvendes ved brugerautentifikation såvel som token udstedelse/veksling.

I arkitekturen anvendes støttesystemet Adgangsstyring til først at sikre brugerens autenticitet (skridt 1-6) – det kunne være en sagsbehandler i et ydelsescenter. I KOMBITs realisering af den generiske arkitektur er IdP-rollen spredt ud over Adgangsstyring

[10] Der er i skrivende stund ikke fundet en leverandør til hverken KY eller KSD, hvorfor det ikke kan siges med sikkerhed, som systemerne tilgås via en webbrowser eller rige klienter.

støttesystemet, og kommunernes egne identity management systemer (IdM) (skridt 3-5). Når en bruger er logget ind igennem denne proces, returneres serviceudbyderens ressource til brugeren (skridt 7).

På et senere tidspunkt i løbet af en brugersession kan serviceudbyderen også anvende støttesystemet Adgangsstyring til at "trække" et token til brug for yderligere webservice kald, til andre serviceudbydere, på vegne af brugeren (skridt 8-12). Disse systemkald til andre 3. parts serviceudbydere kan gå igennem Serviceplatformen [KOMBIT-SP], som tager rollen som Service Gateway.

Danmarks Miljøportal

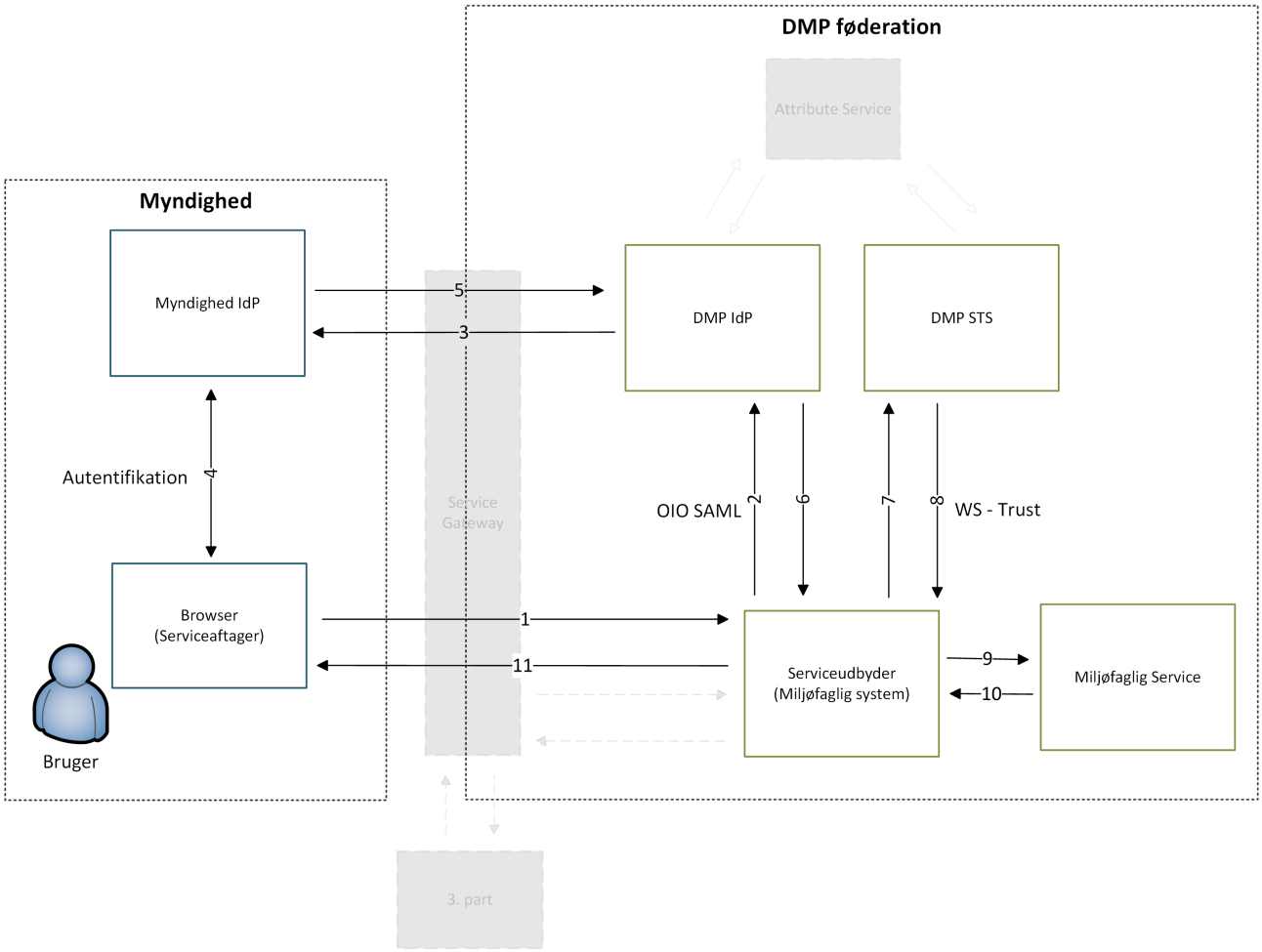
Danmarks Miljøportal indeholder en brugerstyringsløsning, der håndterer adgangen til applikationer og web services i Miljøportalen. Portalen er et partnerskab mellem kommunerne, Danske Regioner og Miljøministeriet.

Brugerstyringsløsningen i Miljøportalen realiserer en føderation mellem brugerorganisationer og serviceudbyderne. En brugerorganisation (partnerorganisation) kan tilslutte sig på to forskellige måder:

- Organisationen kan tilslutte en for afsenderorganisationen lokal Identity Provider, der kan autentificere egne brugere og medsende deres roller (vist på figuren nedenfor). En række kommuner anvender denne model ved at udstille deres lokale brugerkatalog (fx. Active Directory) gennem en føderationsserver (fx Active Directory Federation Services). Flere kommuner har endvidere tilsluttet sig via WAYF føderationen (se senere).
- For organisationer, der ikke har en lokal Identity Provider, kan man anvende en central brugeradministrationsløsning hos DMP. Denne består essentielt set af et hosted brugerkatalog med en web-baseret brugeradministrationsløsning, hvorpå der udstilles en autentifikationsservice via DMP's Identity Provider overfor applikationerne.

Endelig er det også muligt at logge på DMP via NemLog-in for de medarbejdere i brugerorganisationer, der har et OCES medarbejdercertifikat.

Miljøportalen rummer derudover en Security Token Service, der eksempelvis anvendes af rige klienter, der ønsker at tilgå web services udstillet gennem portalen.



Figur 13: Flowet gennem miljøportalen ved sammenhængende log-in kombineret med servicekald

Figur 13 ovenfor illustrerer forløbet for en myndighedsbruger, der tilgår en serviceudbyder i form af et web-baseret fagsystem i scenariet, hvor myndigheden er tilsluttet med sin egen Identity Provider. Pilene 1 – 5 viser, hvorledes fagsystemet anmoder DMP's Identity Provider om log-in via SAML protokollen, og hvor DMP's IdP herefter videresender forespørgslen om autentifikation til Myndighedens Identity Provider. Myndighedens IdP udsteder et token med brugerens roller på baggrund af en lokal autentifikation (trin 4), som eksempelvis kan være brugerens domæne log-in. Dette token omveksles herefter af DMP's IdP (trin 6) mod fagsystemet. Herefter har fagsystemet behov for at kalde en ekstern web service på vegne af brugeren. Til dette formål anmodes DMP's STS om et nyt token (trin 7-8), hvor brugerens oprindelige token (bootstrap token) medsendes for at bevise, at fagsystemet har en session med brugeren. Såfremt fagsystemet har lov til at kalde servicen på vegne af brugere, udsteder STS'en et nyt token til fagsystemet, som autoriserer kaldet. Med det nye token er fagsystemet i stand til at foretage et servicekald (trin 9-10) på vegne af brugeren (dvs. med brugerens autorisation i form af roller).

Samlet har brugerstyringen i Danmarks Miljøportal altså en arkitektur, der i høj grad minder om KOMBIT's Adgangsstyring. En væsentlig forskel er dog, at services i Miljøportalen kaldes i kontekst af en bruger (ActAs elementet fra WS-Trust), hvorimod services i den fælleskommunale rammearkitektur kaldes i kontekst af et anvendersystem og en myndighed

(fx systembruger autoriseret af kommune). Endvidere er der i DMP en række eksempler på kæder af services, der kalder hinanden på vegne af en bruger ("såkaldt ActAs i andet led").

Danmarks Miljøportal understøtter de fællesoffentlige standarder (OIOSAML og OIO IDWS), men kan samtidig også agere som protokol- og tokenveksler mod fagsystemer og services, der ikke understøtter de fællesoffentlige standarder (eksempelvis WS-Federation).

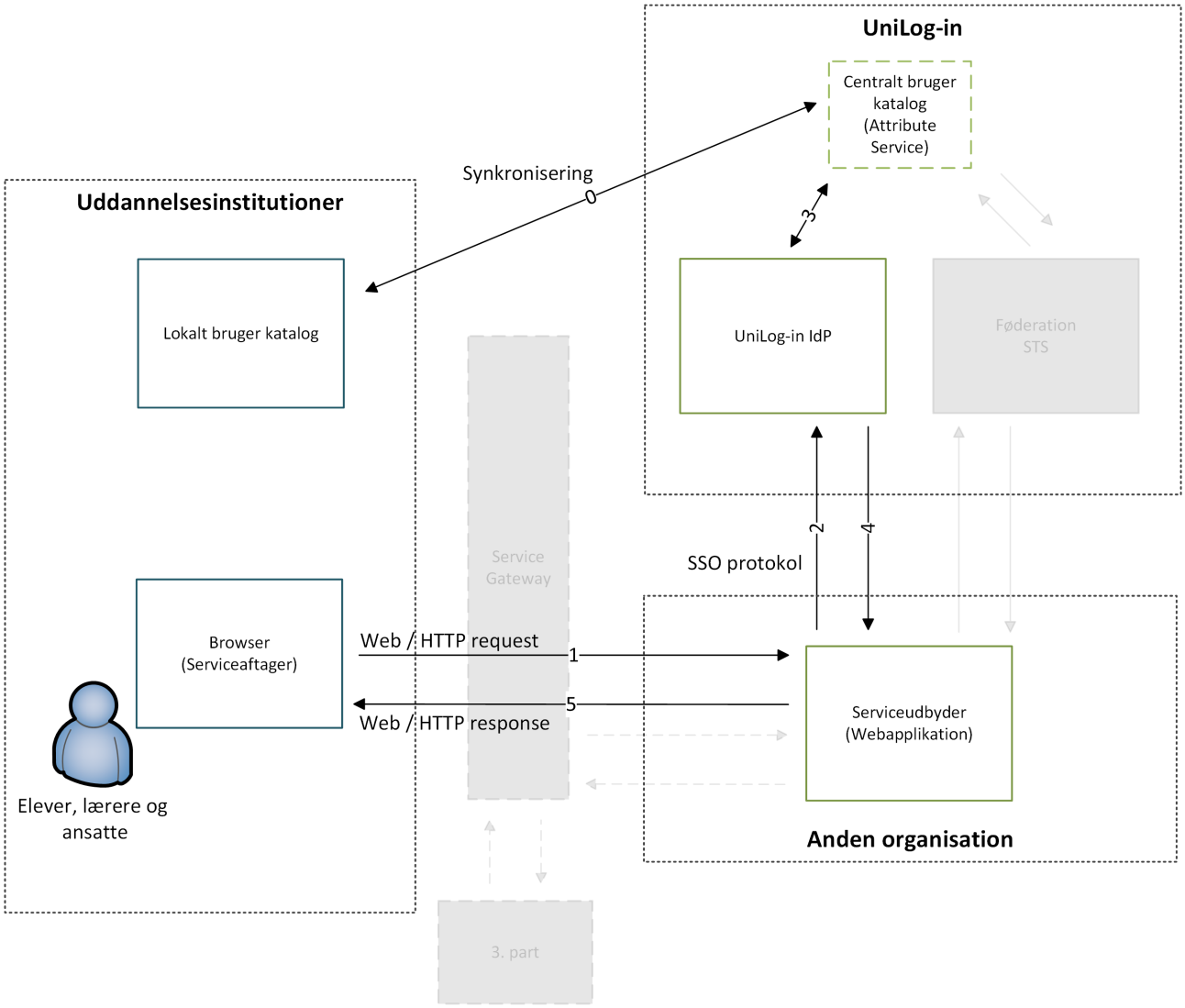
UNI•Login

UNI•Login er en tjeneste til adgangsstyring og brugeradministration for udbydere af net-baserede applikationer i uddannelsessektoren. Den drives af UNI•C, som er en styrelse under Undervisningsministeriet. Tjenesten etablerer en føderation mellem skoler og tjenester, og mere end en million elever, lærere og ansatte er registreret i UNI•Login-brugerbasen. UNI•Login er den eneste offentlige tjeneste, som udbyder en generel autentifikation af personer under 15 år.

Serviceudbyderne i føderationen kan både være private (fx forlag) og offentlige. Brugen er gratis for uddannelsesinstitutioner, mens serviceudbyderne betaler for adgangen.

Arkitekturmæssigt består UNI•Login af et centralt brugerkatalog, der ved synkronisering populeres fra lokale brugerkataloger eller administrative systemer hos uddannelsesinstitutioner. Synkroniseringen kan i visse tilfælde også ske den anden vej. Ovenpå brugerkataloget udstilles en Identity Provider service, som anvendes af serviceudbyderne til log-in, rollestyring og single sign-on. SSO-protokollen blev historisk designet før SAML-standarden, og er derfor proprietær, men efterfølgende er SAML 2 understøttelse tilføjet som en mulighed. I relation til autenticitetssikring anvendes autoritative kilder om elever og lærere på skoler, og brugerne udstyres med et statisk brugernavn og kodeord.

Det er endvidere muligt for brugerne at koble deres NemID til deres UNI•Login brugerkonto til brug i services, der kræver højere niveau af sikkerhed (autenticitetssikring) – eksempelvis for adgang til test- og eksamensapplikationer. Dette etableres ved, at man som bruger først logger ind med det almindelige UNI•Login brugernavn+kodeord og derefter med NemID. Herved kan den unikke brugerID i NemID (PID) kobles til UNI•Login brugerkontoen. Herefter har brugeren mulighed for at logge ind med NemID via UNI•Login til serviceudbydere.



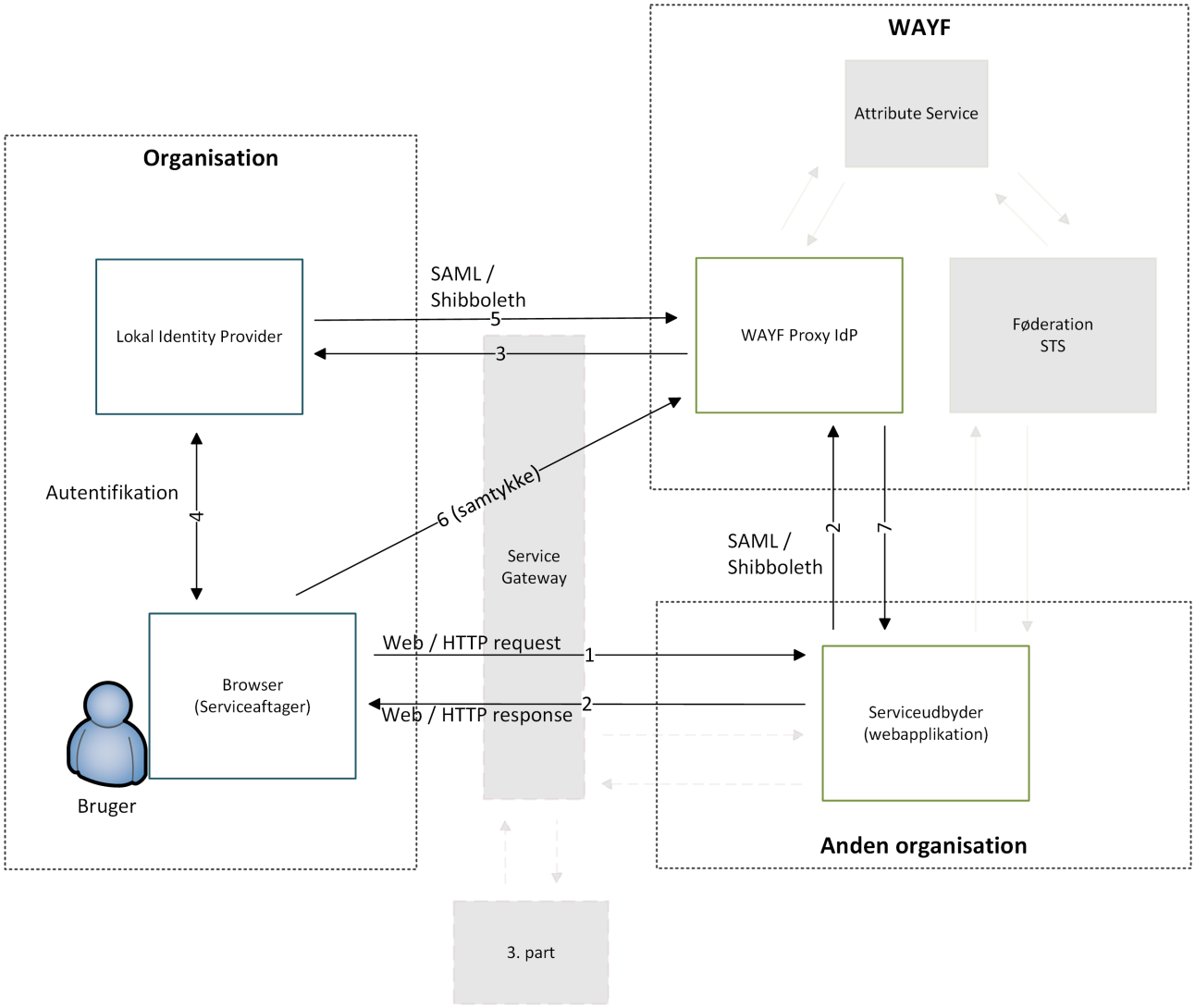
Figur 14: Flow gennem UniLogin ved adgang til web tjeneste

Figur 14 illustrerer forløbet, hvor en bruger tilgår en serviceudbyder i form af en webapplikation med det almindelige Uni•Login brugernavn og kodeord. Serviceudbyderen viderestiller brugeren til den centrale Uni•Login Identity Provider (trin 2), som prompter brugeren for brugernavn og kodeord (ikke vist på figuren). Disse matches mod den centrale brugerdatabase (trin 3), og hvis autentifikationen er succesfuld, udstedes et token med brugerens identitet og rolleoplysninger, som returneres til serviceudbyderen (trin 4). Herefter oprettes en session med brugeren på baggrund af oplysninger i det modtagne token.

WAYF (Where Are You From)

WAYF er en tjeneste, der formidler adgang mellem brugere i institutioner (fx universiteter, gymnasier og andre læreanstalter) og web-baserede tjenester (fx forlag, tidsskrifter, biblioteker, undervisningsmidler). WAYF har sit udspring indenfor forsknings- og uddannelsessektoren og hører i dag under DeIC, som er en enhed under Forsknings- og Innovationsstyrelsen. Opgaven med drift og udvikling af WAYF forestås af Danmarks Tekniske Universitet.

WAYF realiserer en såkaldt hub-and-spoke arkitektur ("fælles integrationspunkt"), hvor tjenesten agerer som IdP-broker, der kan veksle mellem forskellige protokoller og tokenformater, herunder SAML 2 og Shibboleth. Tjenesten har ikke sin egen selvstændige Identity Provider og leverer ikke brugerstyring mod web services. Den er tilsluttet NemLog-in via en OIO SAML integration, men denne anvendes i mindre grad, og er derfor ikke vist på figuren nedenfor.



Figur 15: Forløb ved adgang til tjeneste via WAYF

Figur 15 illustrerer forløbet ved adgang til en serviceudbyder tilsluttet WAYF. Brugeren navigerer til tjenesten (trin 1), som viderestiller til WAYF for autentifikation (trin 2). Hvis brugeren har anvendt WAYF før, kender denne evt. brugerens lokale Identity Provider – ellers bliver brugeren promptet for at vælge denne (ikke vist på figuren). Dette er WAYF 's såkaldte discovery tjeneste, som lader brugeren vælge (og huske) sin hjemorganisation, således at valget af (lokal) Identity Provider kun sker første gang. Herefter bliver brugeren viderestillet til den lokale Identity Provider for autentifikation (trin 3-5). Endelig prompter WAYF brugeren for samtykke til at videregive oplysningerne, og i fald dette er positivt, udsteder

WAYF et token til serviceudbyderen (trin 7). Den eksplicitte håndtering af samtykker til videregivelse af oplysninger er en af WAYF's særlige kendetegn. Bl.a. af den grund kan attributter indeholdende personoplysninger udleveres lovligt til private tjenesteudbydere – modsat NemLog-in, der af udbudsretlige grunde er forbeholdt tjenester udbudt på vegne af offentlige myndigheder.

Ved tilslutning af en web-tjeneste forhandler WAYF en såkaldt "attributkontrakt" med tjenesten, som definerer hvilke attributter, tjenesten må forespørge om. De udleveres som tidligere nævnt kun, hvis brugeren samtykker. Ved udformning af attributkontrakten tages bl.a. højde for tjenestens formål, således at der ikke udleveres flere data om brugerne end højst nødvendigt.

Prehospital Patientjournal (PPJ)

<TBD>

Nemhandel

<TBD>

MedCom-beskeder

<TBD>

Anvendte standarder

Ovenstående scenarier beskriver hovedparten af de løsninger, der kommunikerer på tværs af forskellige parter i dag. Scenarierne identificerer de profiler og sikkerhedsstandarder, der er i spil i denne kommunikation.

En hurtig analyse viser, at de anvendte profiler langt hen ad vejen baserer sig på (eller ligger tæt op ad) de samme grundlæggende standarder (SAML2, WS Trust mm.). Nedenstående opsummerer de mest anvendte profiler og sikkerhedsstandarder i fælles, offentligt etablerede sikkerhedsinfrastrukturer, og stiller dem op overfor hinanden, for at få et billede af, hvor stor mapningsproblematikken er, når der skal veksles fra et token til et andet (se også senere afsnit: Tokens).

Fra/til	NemLog-in	DMP	WAYF	Uni-login	DGWS	KOMBIT
NemLog-in OIO Web SSO 2.0.9		+ Web SSO 2.0.9 baseret *- Ingen STS-setup i NemLog-in*	+/- SAML2 vs. OIOSAML2 *- Ingen STS-setup i NemLog-in*	+/- SAML2 vs. OIOSAML2 - Propritær SSO vs. Web SSO	+/- SAML2 vs. OIOSAML2 *- Ingen STS-setup i NemLog-in* *- DGWS 1.0.1 ikke oplagt valg for NemLog-in token protokol*	+ OIO SAML2 baseret *- Ingen STS-setup i NemLog-in*
DMP OIO Web SSO 2.0.9 OIOIDWS WS-Federation (WS-Trust + WS-Sec)			+/- SAML2 vs. OIOSAML2 *Token protokol ukendt for Shibboleth/WAYF*	+/- SAML2 vs. OIOSAML2 - Proprietær SSO vs. Web SSO	+/- SAML2 vs. OIOSAML2 - IDWS/WS-Fed vs. DGWS	+ Web SSO 2.0.9 baseret + WS-Trust baseret - Attribut profiler
WAYF SAML 2.0 Shibboleth				+ SAML2.0 - Proprietær SSO vs. Shibboleth	+ SAML2 baseret - SAML profiler vs. DGWS	+/- SAML2 vs. OIOSAML2
Uni-Login Proprietær SSO SAML 2.0					+ SAML2 baseret - Proprietær SSO vs. DGWS	+/- SAML vs. OIOSAML2 - Proprietær SSO vs. OIOSAML2
DGWS DGWS 1.0.1 SAML 2.0						+/- SAML2 vs. OIOSAML2 - OIOSAML2/WS-Trust vs. DGWS
KOMBIT OIO Web SSO 2.0.9 OIO Identity tokens v1.0 WS-Trust KOMBIT Attribute Profile						

Teknisk målbillede

Med afsæt i den opstillede vision og de formulerede principper stræbes der i dette kapitel efter at beskrive en målarkitektur, som kan realiseres med minimale konsekvenser for de eksisterende føderationer og deres valg af standarder og teknologi (beskrevet i kapitlet: Teknisk beskrivelse af eksisterende løsninger). Målarkitekturen beskriver, hvorledes de eksisterende føderationer kan bringes til at hænge sammen og den beskriver en ramme som nye føderationer skal passes ind i for at disse bliver en del af en sammenhængende brugerstyring.

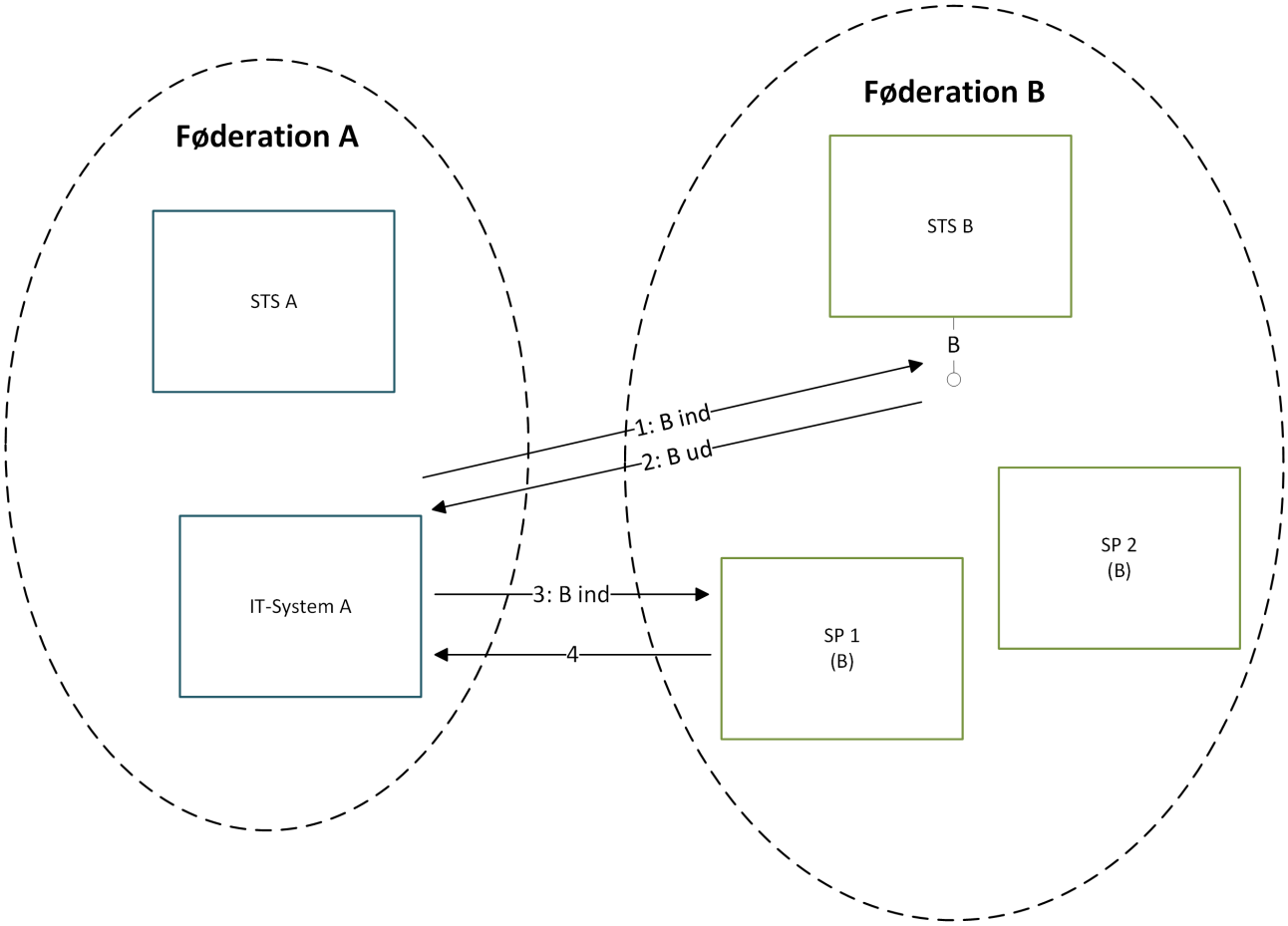
Målbillede for web services

Målarkitekturen skal løse problematikken for både 'web'-scenariet såvel som 'webservice'-scenariet. Dette kapitel vil først behandle problematikken generelt for 'webservice'-scenariet.

Udfordringer ved nuværende web service infrastruktur

System- og organisationslandskabet består i dag af en række føderationer, der alle er mere eller mindre forskellige konkrete realiseringer af arkitekturmønstrene, som beskrevet i forgående afsnit. Forskellene i føderationerne ligger i de anvendte kommunikationsprotokoller (standarder), definitioner af attributter - herunder roller - samt i fortolkning og anvendelse af disse attributter. F.eks. er sundhedsfaglig autorisationskode en del af SOSI-føderationens security tokens, mens security tokens i KOMBIT-føderationen indeholder kommunenr. og ikke autorisationskoder. Der er altså et mismatch mellem hvad tokens indeholder, og dermed et mismatch mellem hvad føderationernes IT-systemer forventer at modtage i forbindelse med et systemkald.

Med den nuværende situation er det nødvendigt for et IT-system, der ønsker at anvende en service i et sikkerhedsdomæne, at gøre brug af dette sikkerhedsdomænes sikkerhedskomponenter. Figur 16 nedenfor illustrerer denne situation.



Figur 16: AS-IS situation for integration på tværs af sikkerheds føderationer

På figuren ses det at et IT-system i føderation A er nødt til at autentificere sig op mod en IdP i føderation B for at få udstedt det security token (skridt 1+2), der skal til for at kalde en serviceudbyder i føderation B (her SP 1) (skridt 3+4).

Autentifikationen kræver at STS B har kendskab til it-system A. Faktisk skal alle IT-systemer, der skal anvende en SP i føderation B, være kendt af STS B. Det skaber med andre ord tætte koblinger mellem systemer på tværs af føderationer.

Hvis serviceudbyderen kræver sikkerhed for brugerens identitet (og altså ikke blot serviceaftagersystemets identitet) kommer brugeren til at autentificere sig en ekstra gang. Først autentificerer brugeren sig overfor IdP A for at få adgang til serviceaftagersystemet og dernæst skal brugeren autentificere sig overfor IdP B for at få adgang til servicen ved SP B.

Konkret målbillede – løst koblede føderationer

For at løse problematikken beskrevet i forgående afsnit, er der behov for en målarkitektur der kan sikre Single Sign-On på tværs af føderationer. Dette tænkes realiseret ved at skabe tillid til udstedte security tokens føderationerne imellem[11]. Et allerede udstedt security token kan således benyttes til at få udstedt et nyt security token, som skal bruges til at få adgang til en service i en anden føderation. Denne "omveksling" af security tokens kan ske af en STS i

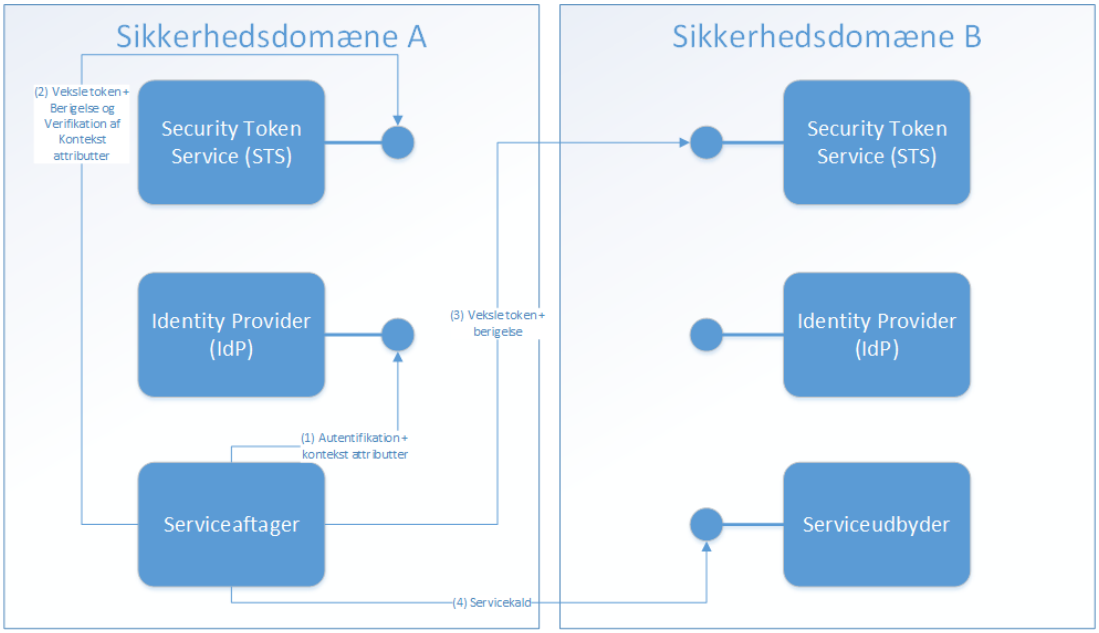
[11] Hvad der danner grundlaget for denne tillid behandles i næste kapitel: Trust framework

serviceaftagerens egen føderation, i serviceudbyderens føderation, i en omliggende føderation eller i kombination af flere af disse.

STS'en i serviceaftagerens domæne vil ofte kunne verificere attributter om brugerens tilknytning til organisationen, herunder om den arbejdsfunktion, brugeren hævder at indgå i. STS'ens i serviceudbyderens domæne kan derimod ofte berige tokenet med yderligere information, som er relevant for serviceudbyderen. I sundhedssektoren kunne det f.eks. være at slå en brugers sundhedsfaglige autorisation op på baggrund af et medsendt CPR nummer i tokenet og berige det hermed. Det er således ofte meningsfyldt, at det ikke bare veksles hos serviceaftagerens egen STS, men også hos serviceudbyderens.

På figuren nedenfor er der etableret en føderation mellem to sikkerhedsdomæner A og B, hvor de to STS'er har et tillidsforhold til hinanden. Det har den umiddelbare fordel er, at det nedbringer antallet af tillidsforhold mellem systemer, da IdP'en i sikkerhedsdomæne B nu ikke behøver at have et tillidsforhold til STS'en i domæne A og vice versa.

Til gengæld betyder det også at serviceaftageren altid skal veksle sit bootstrap token hos egen STS inden det kan veksles hos en fremmed STS. Det giver en ekstra veksling, men denne veksling ofte nødvendig alligevel.

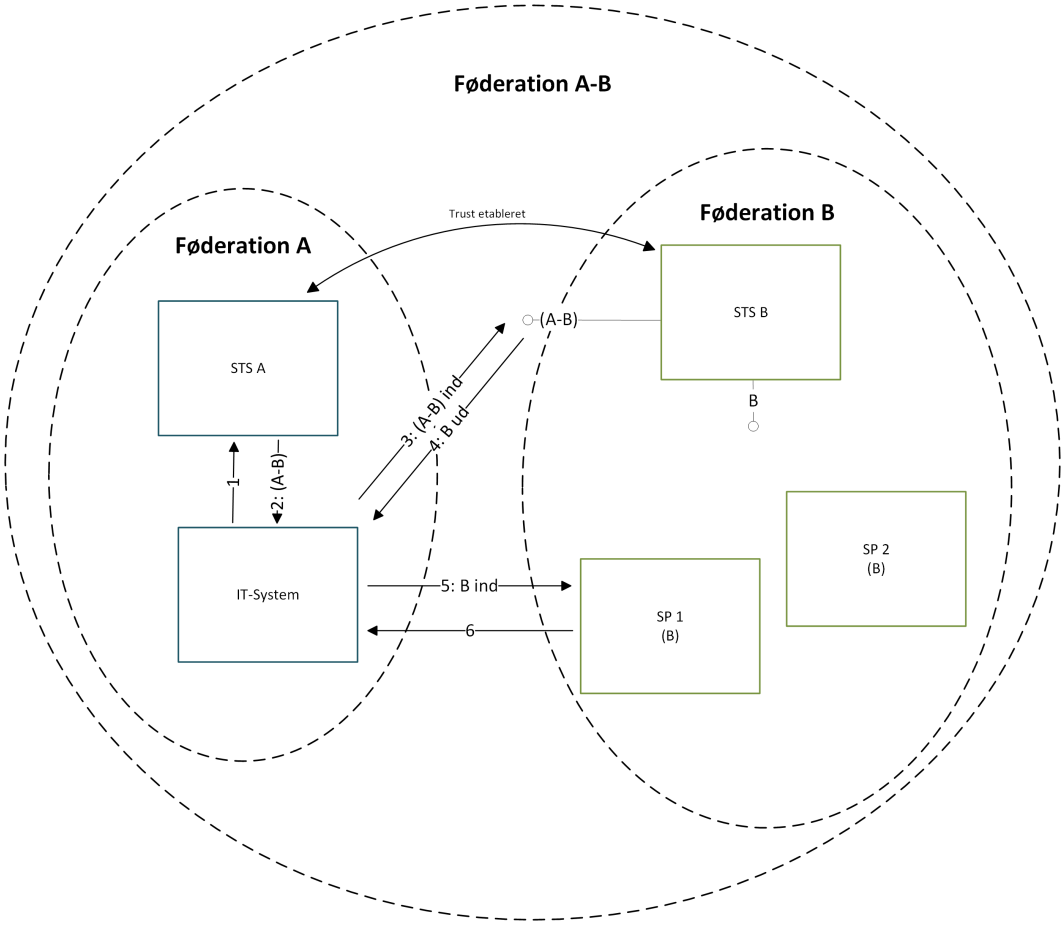


Figur 17: Tokenveksling mellem sikkerhedsdomæner

Det anbefales at lave en dybere analyse af, hvornår hvilke STS'er skal involveres i tokenveksling, samt beskrive retningslinjer herfor. Der bør desuden udarbejdes mønstre for tokenveksling, med angivelse af relevans, udfordringer og løsninger, samt eksempler.

Konkret målbillede – standardisering af token protokoller og formater

I målbilledet introduceres endvidere konceptet om en fælles forståelse af eksterne kommunikationsprotokoller og tokens. En sådan fælles forståelse vil løsne den tætte kobling mellem IT-systemer i én føderation til sikkerhedskomponenter i en anden føderation, som beskrevet ovenfor. Ved at begge de involverede føderationer adapterer en fælles forståelse af protokoller og tokens ligger koblingen i denne forståelse, og ikke ved specifikke sikkerhedskomponenter. Figur 18 illustrerer dette:



Figur 18: Kobling af 2 føderationer

På figuren vises føderationerne A og B, med hver deres sæt af protokoller og tokens. Den fælles forståelse, der etableres mellem disse føderationer udgør i sig selv en føderation (af føderationer), og betegnes derfor på figuren som føderation A-B.

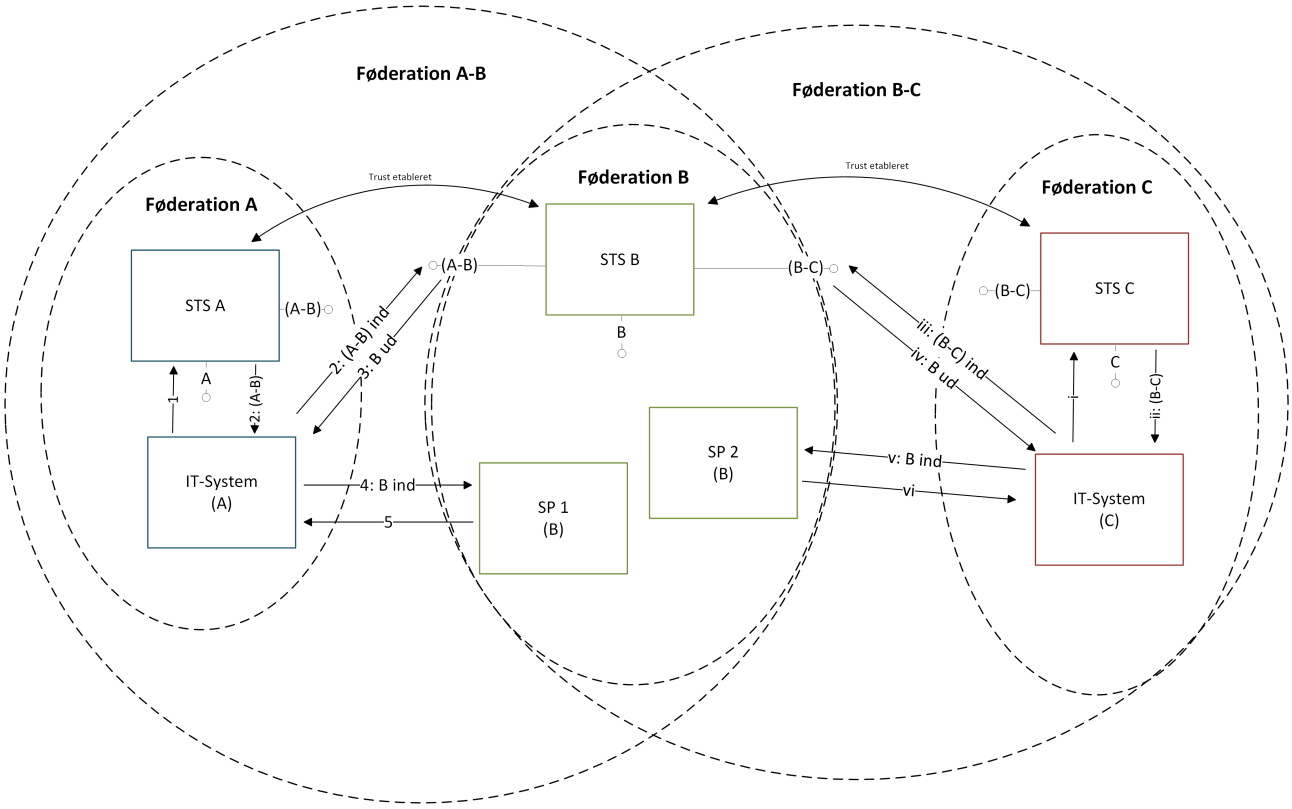
Med den fælles enighed der ligger i A-B omkring protokoller og tokens, skal sikkerhedskomponenterne i hhv. føderation A og B nu implementere denne fælles forståelse, for at gøre den fælles føderation operationel i praksis. Dette medfører at eksempelvis STS B i føderation B, implementerer en snitflade, der overholder den fælles forståelse. Bemærk at STS B bibeholder sin eksisterende snitflade B, til kommunikation med de eksisterende systemer i føderation B.

Snitfladen der realiserer den fælles forståelse af protokoller og tokens, føderation A-B, kan anses som en "**ekstern snitflade**" for føderation B, hvor den eksisterende snitflade (B) der anvendes af alle føderations B systemer kan anses som en "**intern snitflade**". Vice versa for føderation A (ikke illustreret).

Flowet for kommunikation mellem et IT-system i føderation A og SP 1 i føderation B ved brug af målarkitekturen, er vist i Figur 18: IT-systemet benytter først STS A til at blive autentificeret og få udstedt et A-B token (1+2). Dette token kan derefter veksles til et B token (3+4), som kan anvendes i systemkald til SP 1 (5+6).

Udvides scope og ser på tre føderationer (A, B og C) kobles sammen med to forskellige sæt af protokoller og tokens, ser billedet ud som vist på Figur 19 nedenfor. Casen hvor tre føderationer kobles sammen med en fælles forståelse vil være identisk med Figur 18, hvor der blot er en tredje boble identisk med føderation A, kaldet føderation C.

Figur 19 vises de tre føderationer (A, B og C), med to forskellige sæt af protokoller og tokens (A-B og B-C). Boblen med føderation C er en spejling af føderation A, som beskrevet tidligere. Føderation Bs STS har derimod fået endnu en ekstern snitflade, nemlig snitfladen der realiserer B-Cs fælles forståelse af protokoller og tokens.



Figur 19: Kobling af 3 føderationer

Med dette målbillede er det muligt at skabe en kobling mellem to eller flere forskellige føderationer og tillade systemintegrationer på tværs af disse. Konceptet om en fælles forståelse af kommunikationsprotokoller og attributter skaber en løs kobling mellem de forskellige føderationer, samtidig med at den enkelte føderation fortsat kan have et sæt af interne protokoller og attributter.

Det anbefales, at der defineres fælles kommunikationsprotokoller og tokenformater, der kan benyttes, når tokenindhold skal kommunikeres på tværs af føderationer..

Det er vigtigt at bemærke at de fælles protokoller og tokenformater gælder for den **eksterne** del af føderationen. Anbefalingen udtaler sig ikke om den interne del af føderationen. For en føderation, der dækker en konkret branche, er der således mulighed for at lægge sig op ad de protokoller og formater, der er markedsdominerende indenfor branchen. Omkostningen ved omvekslingen af protokoller og formater i en føderations STS vil her opvejes af ikke at skulle ændre væsentligt på de serviceudbyder- og serviceaftager systemer, der kan købes på markedet. Samtidig åbner dette mulighed for at etablere service gateways inden for en føderation, som yderligere kan optimere mulighederne for afkobling mellem de enkelte føderationers teknologiske, indholdsmæssige og sikkerhedsmæssige valg.

Tilsvarende er der mulighed for at tage løsninger i brug, der bygger på nye tokenbaserede teknologier, når blot der fortsat kan ske en omveksling mellem de eksterne og de interne tokens. Innovationskraften tages således ikke ud af de enkelte føderationer. Faktisk er det de enkelte føderationer, der driver innovationen. De fælles (eksterne) protokoller og formater er konservative i den forstand, at de lægger sig op ad de teknologier og standarder som flest anvender. Derved reduceres kompleksiteten i den samlede omveksling. Det betyder også, at hvis flere og flere går over til de samme nye teknologier og standarder, da vil det på et tidspunkt være hensigtsmæssigt at understøtte disse af fælles protokoller og formater – igen for at reducere kompleksiteten i de samlede omvekslinger. Og efterhånden som "gamle" protokoller og formater ikke længere benyttes lokalt (internt i de enkelte føderationer), kan de udfases som fælles (eksterne) standarder.

Omvendt, hvis fælles standarder er tilstrækkelige til at basere intern kommunikation på, og der ikke er væsentlige markedsmæssige eller innovative grunde til at vælge andre protokoller og formater, da bør man også internt lægge sig op ad de eksterne standarder, da man derved undgår ekstra kompleksitet i forbindelse med omveksling.

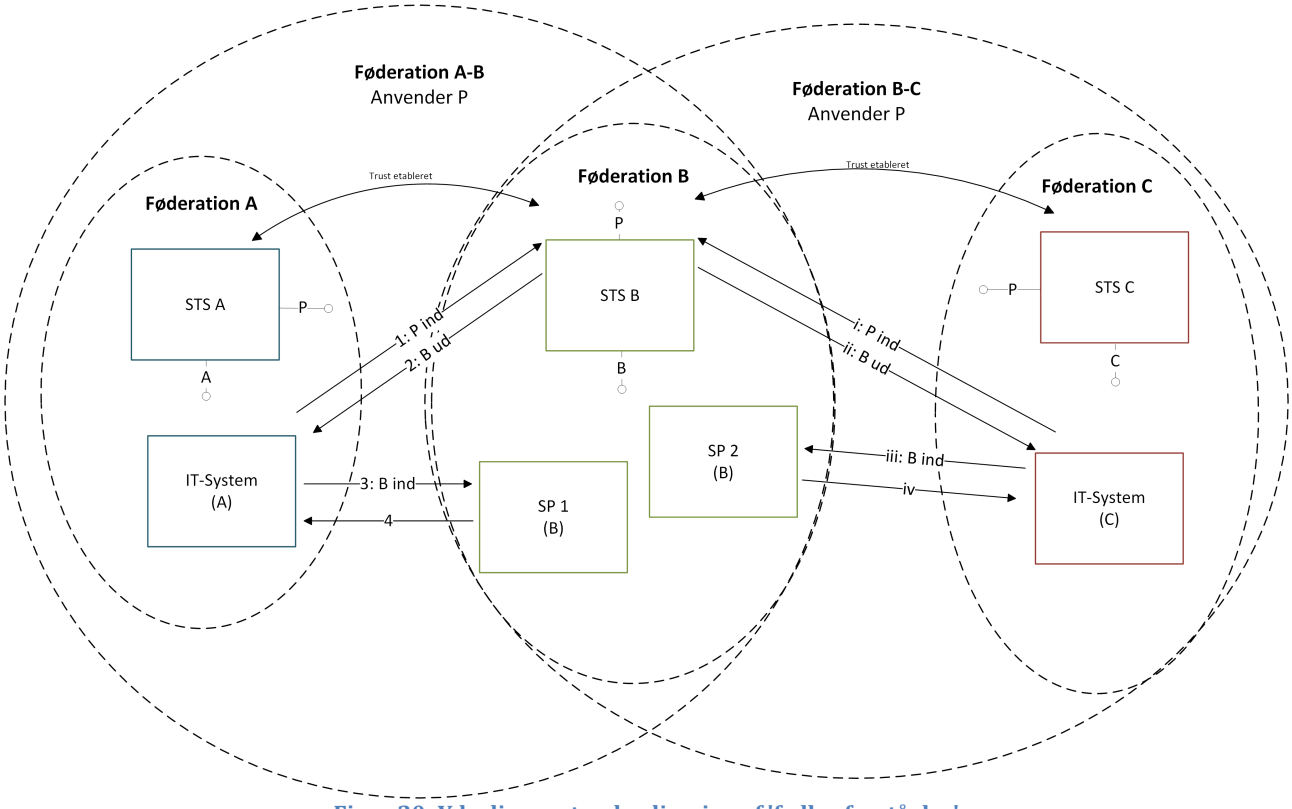
Endelig skal det bemærkes, at eksistensen af fælles (eksterne) protokoller og formater ikke forhindrer direkte kommunikation (uden omveksling til og fra fælles standarder), der hvor der kan være gode grunde til en sådan. Det kan eksempelvis være, hvis kommunikation alene sker mellem to løsninger og disse langt hen ad vejen følger samme standarder (forskellig fra de eksterne standarder) og/eller hvis der er tale om meget tidskritiske systemer, og omvekslingen til og fra fælles standarder ikke kan ske tilstrækkeligt driftseffektivt.

Konkret målbillede – standardisering af token indhold

Protokoller og token-formater definerer *hvordan* sikkerhedskomponenter og IT-systemer taler sammen teknisk. Disse elementer kan generaliseres og anvendes i alle koblinger af føderationer. Token-indhold er tæt bundet til forretningen i de føderationer, der kobles sammen og definerer *hvad* der kommunikeres. Her er tale om information som jobroller (almen praktiserende læge, kommunal sagsbehandler indenfor børnehandicap området, osv.)

og andre attributter (sundhedsfaglig autorisation, kommunenummer, osv.). Denne information kan typisk ikke generaliseres grundet den forretningsspecifikke forståelse og kontekst, der er behov for i systemintegrationerne.

Figur 20 illustrerer hvordan målbilledet vil se ud, med en yderligere standardisering: Føderationerne A-B og B-C anvender begge en fælles forståelse af protokol og token-format, kaldet 'P' på figuren. Føderationerne kan være enige om denne "globale" fælles forståelse uden tab af forretningsmæssig kontekst eller informationsgranularitet. Der er stadigvæk behov en fælles forståelse af token-indhold i A-B føderationen, såvel som B-C føderation, som beskrevet i ovenfor på Figur 19.



Figur 20: Yderligere standardisering af 'fælles forståelse'

Som illustreret på figuren skal alle STS'er i alle føderationerne (A, B og C) kun realisere én ny ekstern snitflade (P) ud over den eksisterende interne snitflade (hhv. A, B og C). Tokens der er kommunikeret over P snitfladerne, efter de protokoller og formater som P definerer, vil skulle indeholde domænernes (A-B og B-C) fælles forståelse af token-indehold. SP'er vil fortsat udstille deres services på interne snitflader, sådan at den fælles forståelse P kun tillader indhentning / veksling af tokens, uden at påvirke den eksisterende føderation og dennes interne brug af protokoller og formater.

Denne "globale" fælles forståelse er i de ovenstående beskrivelser et generelt koncept. Placeret i en konkret kontekst, som eksempelvis det systemlandskab vi ser i Danmark i dag, vil denne "globale" fælles forståelse kunne anses om en nationalt defineret fælles forståelse.

Med en sådan nationalt defineret fælles forståelse er det muligt at opnå et domæneuafhængigt målbillede. Retningslinjer for protokol og token-format til kobling af føderationer vil gøre det

muligt at koble nye føderationer, der allerede realiserer protokoller og token-format, med minimalt overhead. For nye føderationer, der skal kobles til en eller flere føderationer, vil et sæt af nationalt definerede retningslinjer skabe klarhed omkring hvilke krav, der er for at opnå interoperabilitet på tværs af føderationer. Ydermere skal en ny føderation kun realisere én ny ekstern snitflade, for at kunne koble sig til alle andre eksisterende føderationer.

*Det anbefales, at undersøge, om der skal ske justeringer af OIO IDWS og OIO SAML for at disse kan benyttes som standarder for **eksterne** kommunikationsprotokoller og token-formater.*

Tokens

De analyserede føderationer bygger alle på en model, hvor identitetsoplysninger udveksles vha. et token. Tokenet rummer information, der anvendes af serviceudbydere til at afgøre, om et it-system og/eller en bruger må få adgang til at anvende en udbudt service.

Bootstrap Tokens

Nogle føderationer f.eks. NemLogin og KOMBIT udsteder et såkaldt bootstrap token i forbindelse med autentifikationen hos en IdP. Bootstrap tokenet udtrykker, at IdP'en har autentificeret et subjekt via et sæt akkreditiver.

Når en serviceaftager senere skal have adgang til en ressource hos en serviceudbyder benyttes bootstrap tokenet til at få udstedt et security token fra føderationens STS. Dette security token er specifikt målrettet en eller flere serviceudbydere. Bootstrap tokenet rummer således typisk heller ikke ret meget information om serviceaftageren, men nok til at en STS kan verificere identiteten og danne det mere rige security token.

Security tokens

Et security token rummer et sæt af påstande fremsat af en STS. Tokenet er i reglen målrettet et begrænset sæt af serviceudbydere, som er identificeret i tokenet selv og det anvendes til at give en serviceaftager adgang til ressourcer hos en serviceudbyder.

Tokenet kan eksempelvis rumme følgende typer af information:

Kontekst *Hvem modtageren af security tokenet er, f.eks. en specifik service*
Metadata *Information om tokenet selv, herunder om udsteder, levetid, etc.*
Subjekt *Information om den kommunikerede identitet, samt hvordan subjektet autentificerede sig overfor udstederen*
Attributter *Information, som relaterer sig til subjektet, f.eks. adresse, email, jobfunktion.*

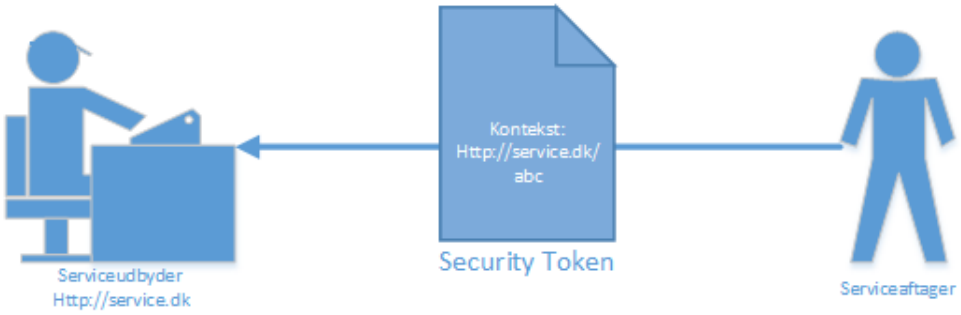
De analyserede tokens rummer alle ovennævnte typer af information, men anvender dels forskellig syntaks og dels forskellig semantik for indholdet. For at kunne veksle tokens på tværs af sikkerhedsdomæner er det nødvendigt at oversætte både syntaks (format) og semantik (indhold) og analysen nedenfor undersøger derfor de muligheder og udfordringer denne veksling giver med primært fokus på det semantiske aspekt, idet mapning mellem syntaks anses for værende mindre kompliceret.

Målbilledet identificerer behovet for et fælles tokenformat og fælles kommunikationsprotokoller og diskussionen i de følgende afsnit går i detalje med udfordringerne ved en sådan veksling fra et token i én føderation til det fælles format. Et token indeholder 4 hovedelementer, som analysen går i detaljer med: Kontekst, metadata, subjekt og attributter.

Kontekst

Konteksten for et token begrænser dets anvendelse til et specifikt domæne, organisation eller service. Modtageren af et token vil altid selv skulle verificere, at et token er acceptabelt, herunder om det er tiltænkt modtageren. Det er derfor væsentligt, at anvenderen af tokenet og modtageren har en fælles forståelse af, hvordan kontekst kommunikeres.

I eksemplet nedenfor illustrerer hvordan et security token, medsendt i et servicekald fra serviceaftageren til serviceudbyderen kan angive en kontekst, via servicens URL, i dette tilfælde http://service.dk/abc:



Figur 21: Kommunikation af kontekst

Ud fra målbilledet, hvor der defineres et fælles tokenformat, er det således nødvendigt at definere en model for at kommunikere kontekst på tværs af sikkerhedsdomæner. Hvis et sikkerhedsdomæne allerede har sit eget format at kommunikere konteksten på, betyder det, at der skal oversættes mellem det lokale format og det fælles format.

KOMBIT og NemLogin føderationerne anvender en URI til at angive konteksten i form af et <AudienceRestriction> element i tokenet. Tokens i SOSI føderationen rummer ikke kontekstinformation. Det er derfor oplagt at adoptere URI syntaksen og samtidig forlange at enhver URI er unik, dannet ud fra f.eks. URL'en på den service, der modtager tokenet, som i eksemplet ovenfor.

Det anbefales, at der defineres et format for angivelse af et tokens kontekst. De enkelte føderationer kan så enten adaptere dette format eller der kan defineres en mapning fra lokal navngivning til det fælles format. Formatet bør baseres på URI og følge SAML specifikationens definition af <AudienceRestriction> elementet. (se [SAML Core] 2.5.1.4)

Meta information

For at en serviceudbyder kan validere et token er det nødt til at rumme et sæt af information om selve tokenet. Et security token rummer sædvanligvis følgende meta information:

Issuer:	*Hvem har udstedt dette token.*
Signatur:	*En digital signatur, der beskytter selve tokenet mod manipulation og samtidig giver mulighed for autentifikation af udstederen (message authentication)*
Assurance Level:	*Det niveau af autenticitetssikring, som dette token har jævnfør diskussionen af dette under afsnittet om trust frameworks.*
SpecVer:	*Versionen af den profil (Den Gode Webservice, OIO-IDWS, etc.), som dette token er underlagt.*
Timestamp:	*Det tidsrum indenfor hvilket dette token er validt, samt hvornår det er udstedt.*

De analyserede føderationer rummer alle stort set hele sættet af meta information ovenfor, men har forskellige formater for informationen og det er ikke alle elementer der er med for alle. SOSI føderationen har f.eks. ikke en audience restriction.

> *Det anbefales, at der defineres et fælles sæt af meta information, som en serviceaftager altid kan regne med vil være til stede i et fælles security token. Det fælles sæt kan med fordel baseres på de obligatoriske attributter i OIO SAML standarden. De enkelte føderationer kan så enten udvide eget token format eller oversætte fra eget format til det fælles.*

Subjekt

Et security token kommunikerer ofte information om et subjekt, typisk en person eller et IT-system. Subjekter kan identificeres ved forskellige typer af information, f.eks. et CPR nummer, en MAC adresse, et CVR nummer koblet med et unikt certifikat-løbenummer (f.eks. CVR-RID), et brugernavn, en digital signatur, etc.

Uanset hvordan subjektet identificeres er det nødvendigt, at den serviceudbyder, der skal benytte tokenet til at afgøre adgang til egne ressourcer, forstår og kan tolke identiteten. Dermed bliver der behov for profiler for hvordan et subjekt identificeres, som er fælles på tværs af føderationer. OIO Web SSO profilen [OIO-SAML] som anvendes i NemLogin føderationen definerer f.eks. en OCES attributprofil, der udtaler sig om, hvordan et subjekt beskrives, når autentifikationen er foregået via et MOCES certifikat.

> *Det anbefales at definere et sæt af fælles profiler for angivelse af identitet, som en serviceaftager skal kunne tolke.*

Attributter

Centralt for tokens er muligheden for at rumme påstande om dets subjekt i form af attributter. Attributter identificeres ved en nøgle, som har en tilknyttet værdi. Figuren nedenfor viser eksempler på simple attributter, der kan medsendes i et token:

Nøgle	Værdi
Email	somebody@somewhere.dk
Fornavn	Some
Efternavn	Body

Arbejdsfunktion	Hjemmehjælper

Attributter medsendes i et token med forskelligt formål: Nogle attributter kan anvendes til præsentation eller logning, f.eks. personens navn, mens andre kan anvendes af serviceudbyderen til autorisation, f.eks. en arbejdsfunktion.
Der er mange aspekter af anvendelse af attributter og disse diskuteres i det følgende.

Generelle og domænespecifikke attributter

I målbilledet defineres en fælles forståelse af tokenformat på tværs af sikkerhedsdomæner, som hvert domæne kan mappe til eller implementere evt. som en delmængde af egne informationer. Centralt for det fælles tokenformat er attributterne.

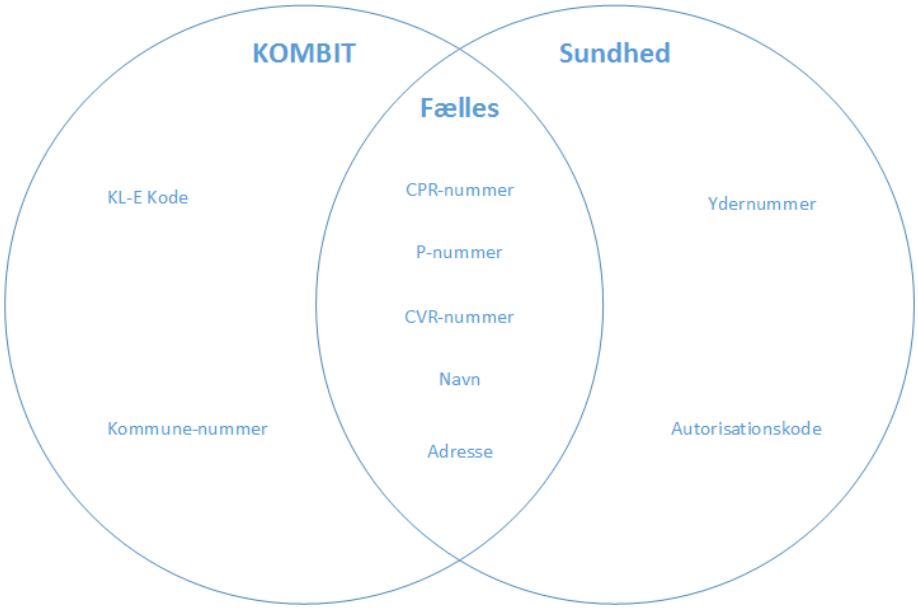
Indenfor et sikkerhedsdomæne vil alle parter automatisk benytte samme sæt af attributter, da den lokale IdP/STS standardiserer dette og dermed have konsensus på format og semantik af attributterne. Denne antagelse holder ikke automatisk imellem sikkerhedsdomæner eller føderationer.

Attributter falder i to kategorier:

- **Generelle attributter**: Attributter hvis værdisæt er generelt kendt og ofte kan tilvejebringes for udenforstående. Navne, adresser, etc. falder i denne kategori. Generelle attributter er værdisæt, der er konsensus på mellem flere parter f.eks. fordi de er velkendte i en kulturel kontekst. Man kan derfor næppe regne med at alle generelle attributter, der f.eks. vil være forståelige af alle i dansk kontekst også vil være det i udenlandsk.
- **Domænespecifikke attributter**: Attributter hvis værdisæt er specifikt for domænet og måske slet ikke meningsfyldt udenfor. Ydernumre, kommunekode, SOR værdier, KL-E numre etc. falder i denne kategori

For de generelle attributter giver det mening at standardisere en fælles kerne, der giver et sprog på tværs af domæner, mens det samme ikke er meningsfyldt for domænespecifikke attributter.

Figuren nedenfor viser attributter, der er lokale for to føderationer, KOMBIT og Sundhedssektoren, samt attributter hvor semantikken er veldefineret på tværs af de to parter.



Figur 22: Attributter, der er specifikke og fælles for to føderationer

En fælles kerne af attributter er allerede defineret af Digitaliseringsstyrelsen [Kerneattributter], der har sin rod i internetstandarden "RFC 2798 - Definition of the inetOrgPerson LDAP Object Class" [InetOrgPerson]. Det fælles sprog anvendes af KOMBIT og NemLogin, samt til dels WAYF [WAYF Attr.], mens SOSI definerer sin egen kerne (der dog er stærkt inspireret af OIOSAML).

Skemaet nedenfor opsummerer de 6 føderationer, der er genstand for analysen i denne rapport, lister hvorfra generelle attributter stammer, samt hvilket domæne resterende attributter hører til.

	Generelle	**Domænespecifikke**
WAYF	inetOrgPerson	Schac: Schema for Academia [Schac]
KOMBIT	OIOSAML	Fælleskommunale attributter (f.eks. KombitSpecVer)
SOSI	Ligner OIOSAML	DGWS attributter
NemLogin	OIOSAML	Ingen
UniLogin	Ligner OIOSAML	UNI-Login specifikke attributter [UNILogin Attr.]
DMP	*Ikke analyseret*	Miljøspecifikke attributter (f.eks. arealinformation)

Det anbefales at definere et sæt af fælles kerneattributter, der kan veksles til fra alle føderationer. Kerneattributterne kan oplagt defineres ud fra Digitaliseringsstyrelsens eksisterende arbejde med [Kerneattributter]. Disse bør kvalificeres ud fra hver føderation, og det bør nøje overvejes for hver attribut om den er relevant at medtage i en fælles kerne.

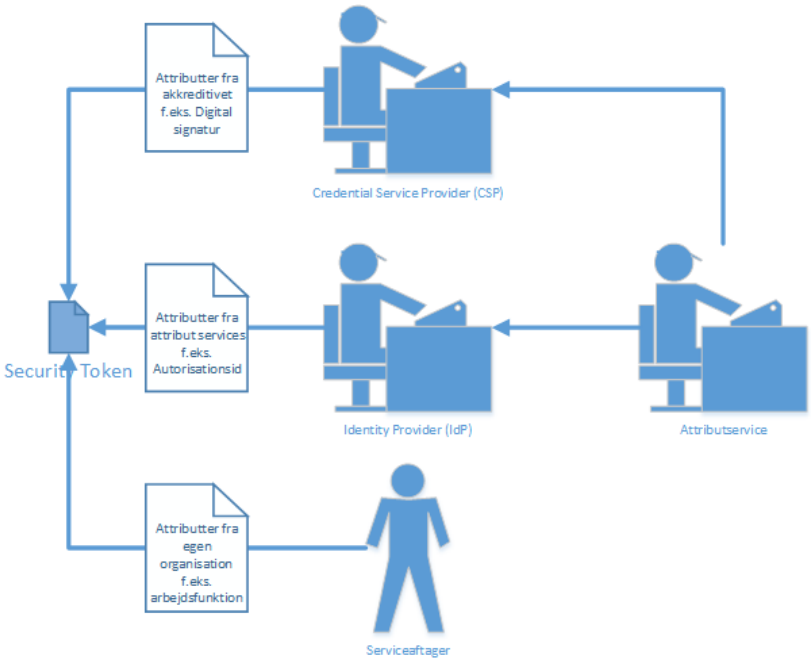
Kilder til token information

Påstande om et subjekt kan stamme fra 5 kilder:

1) Fra **Credential Service Provideren (CSP)**, der for nogle akkreditivers vedkommende vil levere yderligere information. Det gælder f.eks. når akkreditivet er et digitalt certifikat, som typisk har oplysninger om personen, navn, organisatorisk tilhørsforhold, mm. indlejret
2) Fra **Serviceaftageren** og være medsendt til IdP'en under autentifikationsprocessen, f.eks. oplysninger om en bestemt arbejdsfunktion, som subjektet aktuelt udfører jævnfør diskussionen af dette nedenfor
3) Fra **IdP'en,** der via viden om subjektet kan berige tokenet med yderligere information
4) Fra **STS'en i serviceaftagerens sikkerhedsdomæne**, der via viden om subjektet kan berige tokenet med yderligere information, som kun kendes i serviceaftagerens sikkerhedsdomæne
5) Fra **STS'en i serviceudbyderens sikkerhedsdomæne**, der via viden om subjektet kan berige tokenet med yderligere information, som kun kendes i serviceudbyderens sikkerhedsdomæne.

En STS vil i nogle tilfælde kunne kontakte en autoritativ kilde, en attributservice, for at hente eller verificere attributter om et subjekt. Det kunne f.eks. være et sundhedsfagligt autorisations-id eller et CPR nummer. Dermed kan STS'en altså både berige et token med yderligere information om subjektet, men også potentielt verificere attributter der måtte være medsendt i tokenet.

Figuren nedenfor illustrerer de kilder, der kan levere attributter til et security token:



Figur 23: Kilder til attributter i et Security Token

Verifikation af token information

I nogle tilfælde er det muligt for en STS at kontrollere validiteten af attributter ved at kontakte en attributservice. For at dette check har nogen værdi er det afgørende, at attributservicen er autoritativ kilde eller en betroet kopi af et autoritativt register. I dansk kontekst tilbyder

Nets/DanID f.eks. en service til at slå et CPR nummer op på baggrund af værdien af attributten Subject Serial Number i MOCES X.509 certifikater og Sundhedsstyrelsens autorisationsregister tilbyder en service til at slå sundhedsfagliges autorisations-id(er) og uddannelseskode(r) op på baggrund af et CPR nummer.

Når en person arbejder med et IT-system, foregår det f.eks. altid i kontekst af en konkret arbejdsfunktion, som personen varetager. Det er derfor alene på serviceaftagersiden, at denne viden kan findes. Da arbejdsfunktionen ofte vil være adgangsgivende til ressourcer hos en serviceudbyder, kan det være nødvendigt at serviceaftager medsender informationen i forbindelse med sin autentifikation mod IdP'en og STS'en.

Hvis IdP/STS har viden om hvilke arbejdsfunktioner, subjektet generelt må varetage (via en attributservice), kan den verificere at den arbejdsfunktion som serviceaftager påstår subjektet har også er på listen over tilladte arbejdsfunktioner for subjektet. En sådan verifikation kan være med til at løfte kvaliteten af attributten, da serviceudbyder nu har større sikkerhed for at subjektet vitterlig er autoriseret (af en tredjepart) til arbejdsfunktionen i det medsendte token og at dette forhold aktivt er verificeret af IdP/STS. Tilsvarende betragtninger gør sig gældende for andre attributter.

For at serviceaftager faktisk kan vurdere kvaliteten af en attribut, skal tokenet tilknyttes yderligere information. Dette er analogt til diskussionen om niveauer af autenticitet, hvor tokenet tilknyttes en værdi for, hvor stor tillid serviceaftager kan have til kvaliteten af det akkreditiv, subjektet benyttede ved autentifikation på en skala fra 1 til 4.

Der findes ikke aktuelt nogen normativ standard for angivelse af kvalitetsinformation om attributter, så en sådan vil skulle defineres. Et forslag til angivelse af kvalitetsinformation findes i [OIOSAML Att. Context], hvor ekstra information om attributter i et SAML token angives ved at tilføje flere attributter med samme navn, men tilføjet suffikset ":context". Kvalitetsinformationen angives så i en URI, f.eks. http://somedomain.org/onlinevalidated. Semantikken af URI'erne skal følgelig også defineres.

En attribut med navnet "dk:gov:saml:attribute:someattribute" vil altså få en søsterattribut med navnet "dk:gov:saml:attribute:someattribute:context", der refererer en URI, som angiver attributtens kvalitet.

Det anbefales at definere en standard for hvordan kvaliteten af en attribut kan angives i et token og at tage udgangspunkt i det arbejde, der er lavet i [OIOSAML Att. Context].

Principper for tokenindhold

Når en serviceaftager skal kommunikere med en serviceudbyder er der en række principper der skal overholdes for det token, der medsendes i kaldet:

1) Der skal medsendes tilstrækkelig metainformation, som serviceudbyder har brug for til at vurdere om tokenet er anvendeligt (udsteder, levetid, etc.)
2) Der skal være tilstrækkelig information om subjektet, som serviceudbyder har brug for til at foretage adgangskontrol, logning etc.

3) Der skal medsendes de attributter, som serviceudbyder har brug for til at kunne foretage adgangskontrol (arbejdsfunktion, samtykke, etc.)
4) Syntaksen af attributterne, meta data, subjektet, mm., dvs. formatet af nøgler og værdier, skal være som serviceudbyder forventer det
5) Serviceaftager og serviceudbyder skal være enige om semantikken af meta data, identitet, attributter, så en arbejdsfunktion f.eks. har samme "betydning" hos begge parter og dermed bidrager til den intenderede adgangskontrol. Dette gælder indenfor et sikkerhedsdomæne eller en føderation.
6) Der skal medsendes så lidt information i tokenet som nødvendigt for at beskytte brugerens data mod misbrug. Omvendt er det også vigtigt at antallet af token vekslinger holdes lavt, hvilket kan sikres ved at gøre tokens tilpas brede til at kunne bruges af flere modtagere.

Princip nummer 6 rummer to modsatrettede hensyn nemlig behovet for beskyttelse af tokeninformation imod behovet for robusthed. Hvis et token kommunikerer information om en ansat er behovet for beskyttelse af informationen oftest lavere end hvis det kommunikerer information om en borger. Udfordringen er at finde balancen i de to hensyn.

Målbillede for webapplikationer

De konkrete målbilleder gennemgået ovenfor behandler hvordan kommunikation på tværs af føderationer kan etableres når der er tale om kommunikation og veksling af identitets- og security tokens. Et andet scenarie for Single Sign-on er for brugervendte webapplikationer, hvor brugeren er private borgere såvel som offentlig ansatte. NemLog-in, som er beskrevet i afsnittet "NemLog-in føderationen", er et kendt eksempel på dette.

Et konkret målbillede for dette scenarie vil kræve en arkitektur med nogle andre egenskaber, end i de hidtil beskrevne konkrete målbilleder. Dette behov opstår da der er et ekstra element i etablering af SSO på tværs af føderationer for dette scenarie, nemlig behovet for at identificerer i hvilken (om noget) føderation en bruger har en aktiv browsersession i gang, dvs. allerede er logget ind – der er behov for at introducere en "discovery"-funktionalitet af aktive sessioner på tværs af føderationer. Problematikker omkring token format og indhold gør sig stadigvæk gældende i dette scenarie.

Med andre ord kan de nøgle punkter, der er analyseret og diskuteret i denne rapport genbruges anvendes i formuleringen af et konkret målbillede for SSO i brugervendte webapplikationer. Dog er der herudover behov for yderligere analyse af hvordan de ekstra behov kan opfyldes i et konkret målbillede.

Det anbefales, at der gennemføres yderligere analyse af konkret målbillede for SSO i scenariet for brugervendte webapplikationer, på tværs af føderationer. Herunder at der defineres et fælles sæt af kommunikationsprotokoller og tokens indhold samt format.

Behov for nye standarder

<TBD>

Trust framework

Når ansvaret for autentifikation uddelegeres til en IdP introduceres et element af tillid. En serviceudbyder er nødt til at stole på at IdP'ens processer for identifikation og autorisation af serviceaftagere – på det tidspunkt hvor en serviceaftager indgår en aftale med IdP'en – er velfungerende, og at IdP'en selv er pålidelig og sikrer at opbevaret identitets- og aftale-information ikke kan ændres af en ondsindet 3. part. Samtidig har serviceudbyderen behov for at vurdere om de modtagne tokens teknisk set er tilstrækkeligt robuste til at man kan stole på informationen, når der autentificeres, eller når identiteten fastslås. Dvs. at service udbyderen har høj nok grad af sikkerhed for, at den modtagne information ikke er forfalsket. Endelig skal IdP'en stole på at CSP'ens procedurer for udstedelse af akkreditiver er sikre og serviceudbyder stoler dermed også indirekte på CSP'ens procedurer.

I en føderation, der involverer flere sikkerhedsdomæner, udvides tilliden, som det enkelte sikkerhedsdomæne skal have, desuden til at omfatte komponenter som IdP'er og STS'er fra alle andre involverede sikkerhedsdomæner.

For at alle parter kan have tillid til hinanden bliver det en fordel at eksplicitere, harmonisere og standardisere forskellige aspekter af sikkerhed, herunder politikker, sikkerhedsmæssige tiltag og fælles sprog. Dette sker ved udarbejdelse af et såkaldt trust framework. Harmonisering og standardisering er teoretisk set ikke en nødvendighed, men konsekvensen ved ikke at harmonisere og standardisere er, at kompleksiteten af kommunikationen mellem sikkerhedsdomæner bliver meget høj. Der skal indgås individuelle aftaler mellem parterne og disse skal kende til hinandens politikker og arbejdsgange m.m. Et trust framework er med til at reducere denne kompleksitet.

Dette afsnit beskriver rammerne for et sådant trust framework, der tillader at tokens indeholdende identitetsinformation og andre attributter, herunder roller, kan sendes fra serviceaftager i ét domæne, til en serviceudbyder i et andet domæne, samt at den serviceudbyder der modtager dette token, kan tillade serviceaftager adgang til ressourcer. Frameworket beskrevet her bygger primært på STORK projektet, der har til formål at modellere en føderation af services på tværs af landegrænser, samt af NISTs niveauer af autenticitetssikring [NIST].

Principper for evaluering af sikkerhedsegenskaber

Tillid er ikke noget absolut. Man kan operere med grader af tillid (levels of assurance). NIST [NIST] opererer med fire niveauer:

Niveau 1: Lille eller ingen grad af tillid
Niveau 2: Nogen grad af tillid
Niveau 3: Høj grad af tillid
Niveau 4: Meget høj grad af tillid

I det efterfølgende fokuseres der på graden af tillid til at man har kunnet verificere identiteten af en bruger eller et system, men der kan opereres med grader af tillid til andre påstande (eksempelvis omkring sundhedsfaglig autorisation eller organisatorisk rolle).

Et af nøgleelementerne i et trust framework er et eller flere sæt af sikkerhedsegenskaber, som man anvender til at kategorisere og vurdere deltagende komponenter og/eller organisationer. To overordnede principper er styrende for evalueringen disse sikkerhedsegenskaber:

- **Maksimumsprincippet (risiko)**: Det største krav eller den risiko med de største konsekvenser afgør den totale risiko
- **Minimumsprincippet (total sikkerhed)**: De dårligste modtræk til et givet angreb afgør den totale sikkerhed, der kan opnås.

Kvalitetsniveauer

Før en serviceaftager kan autoriseres til at anvende en ressource, skal serviceudbyderen først autentificere serviceaftageren via dennes akkreditiv. Akkreditiver findes i mange forskellige kvaliteter gående fra i den mindre sikre ende brugernavn/password til i den stærkere ende flere-faktor akkreditiver. Sidstnævnte kendetegnes ved at blande noget brugeren har (f.eks. hard tokens) med noget brugeren ved (f.eks. et password) eller noget brugeren er (f.eks. et fingeraftryk).

Bemærk at et akkreditiv ikke nødvendigvis kommunikerer en identitet. Det kan være tilstrækkeligt at vide, om en person er myndig eller at brugeren er tildelt en bestemt rolle. Omvendt vil identitet oftest være nødvendig på sundhedsområdet for at kunne leve op til krav om logning.

Akkreditivets kvalitet er dog langt fra alene afgjort af hvor mange faktorer, der anvendes, men afhænger i lige så høj grad af hvordan det er udstedt. Skemaet nedenfor beskriver 5 kvalitative egenskaber, som et akkreditiv og dermed den samlede elektroniske identitet vurderes ud fra:

Krav til registreringfasen (RP)	Kvaliteten af identifikationsproceduren	*Den fysiske tilstedeværelse af serviceaftageren for så vidt denne er en person, samt kvaliteten af beviserne for dennes identitet*
	Kvaliteten af identitets-udstedelsesproceduren	*Måden hvorpå akkreditiver dannes og leveres til serviceaftageren*
	Kvaliteten af myndigheden, der udsteder akkreditiver	*Er myndigheden underlagt pålidelig kontrol?*
Krav til autentifikations-fasen (EA)	Typen og robustheden af akkreditiverne	*Spænder fra brugernavn/password til "hårde" certifikater, fra enkelt til flere faktorer*
	Sikkerheden af autentifikationsmekanismen	*Den beskyttelse, et givet akkreditiv tilbyder mod angreb*

Når en elektronisk identitet vurderes ud fra skemaet tilskrives det et af 4 kvalitetsniveauer for henholdsvis registreringsfasen (RP) og autentifikationsfasen (EA), hvor 1 er laveste kvalitet. RP og EA niveauerne vurderes ud fra minimumsprincippet, så det laveste kvalitetsniveau afgør den totale kvalitet.

Vurderingen af de 5 kriterier for en given elektronisk identitet er ikke beskrevet i detalje her. Dette arbejde er dog i nogen grad allerede udført i STORK projektet og i større grad i Kantara projektet [Kantara]. Samtidig har IT- og Telestyrelsen i 2005-2006 udarbejdet en vejledning vedrørende niveauer af autenticitetssikring [OIO-AUTSIK], der kan danne udgangspunktet for arbejdet med en vurdering.

Anbefaling: Det anbefales af udarbejde vurderingskriterier for de 5 kvalitative egenskaber baseret på [OIO-AUTSIK], samt arbejdet i STORK og Kantara projekterne.

Autenticitetsniveau

For at operationalisere den kvalitet, en serviceudbyder kan regne med for en identitet, beregnes autenticitetsniveauet nu ud fra RP og EA niveauerne vurderet efter minimumsprincippet, som angivet i skemaet nedenfor. En elektronisk identitet med RP2 og EA3 vil f.eks. have Niveau 2 som autenticitetsniveau:

		Niveauer for autentifikationsfasen			
		EA1	**EA2**	**EA3**	**EA4**
Niveauer for registreringsfasen	**RP1**	Niveau 1	Niveau 1	Niveau 1	Niveau 1
	RP2	Niveau 1	Niveau 2	Niveau 2	Niveau 2
	RP3	Niveau 1	Niveau 2	Niveau 3	Niveau 3
	RP4	Niveau 1	Niveau 2	Niveau 3	Niveau 4

Autentifikationsniveauerne giver dermed en entydig skala på tværs af akkreditivtyper og på tværs af IdP'er, der muliggør at en afhængig part kan vurdere om der kan gives autorisation til en ressource. Forudsætningen er selvfølgelig, at IdP'erne er enige om hvordan autenticitetsniveauerne beregnes og evalueres.

Akkreditering

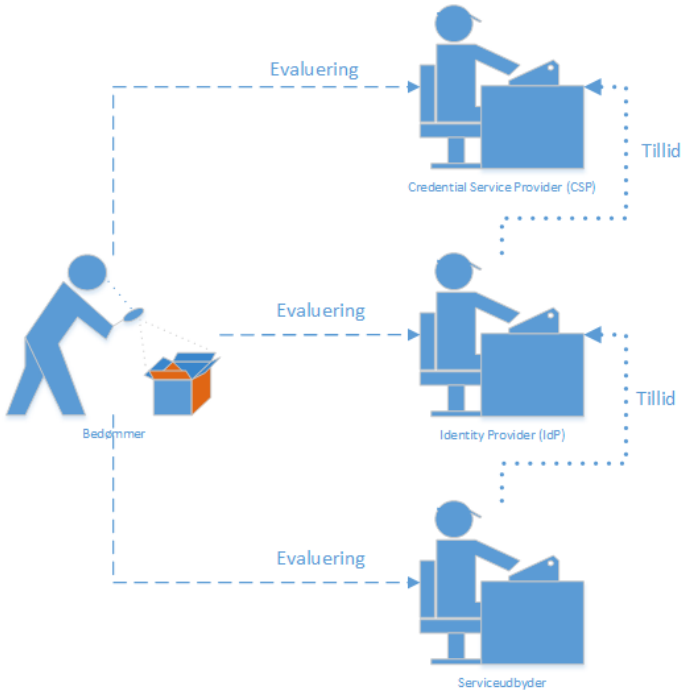
For at sikre en ensartethed i hvordan niveauer for autenticitet beregnes på tværs af parter i en føderation, er der behov for en uafhængig part, en "bedømmer" (engelsk, "Assessor"), der via et sæt af procedurer og retningslinjer kan evaluere CSP, IdP, STS og Serviceudbydere.

En sådan bedømmer skal f.eks. vurdere hvordan en CSPs procedurer for registrering (RP) matcher en fælles model og give point ud fra en fælles skala. Tilsvarende for EA.

Derudover skal en bedømmer tage stilling til en række forskellige organisatoriske og juridiske spørgsmål, herunder bl.a. men ikke udtømmende:

- Hvem er ansvarlig for at udstede og nedlægge identiteter?
- Hvem er ansvarlig hvis der sker fejl?
- Hvem kan garantere at et akkreditiv er mappet korrekt til autenticitetsniveauer for en given myndighed / domæne?
- Hvordan vedligeholdes mappingen mellem akkreditiver og autenticitetsniveauer når sikkerheden opgraderes / reevalueres? Dette er særligt relevant fordi der hele tiden kommer nye sikkerhedstiltag og angrebstyper?
- Hvordan og hvornår kontrolleres føderationernes overholdelse af specifikationer?

Figuren nedenfor illustrerer hvordan kæden af tillid fra serviceudbyder over IdP og CSP holder fordi en uafhængig 3. part foretager en upartisk evaluering og rangerer parterne ud fra en fælles, konsensusbåren model.



Figur 24: En bedømmer evaluerer føderationsparter

Organisationen bag Kantara [Kantara] tilbyder at indtræde i rollen som bedømmer og definerer samtidig et omfattende sæt af procedurer og retningslinjer for at evaluere de enkelte parter i en føderation. Kantaras forståelse af niveauer af autenticitet er anvendt som udgangspunkt for den her skitserede model og man kunne derfor anvende Kantara organisationen som bedømmer. Imidlertid er det forbundet med omkostninger per part at få gennemført en sådan bedømmelse og da offentlige myndigheder i dansk kontekst allerede i dag skal udføre en årlig IT-revision er det oplagt at undersøge om bedømmelsen ikke kan ske i samme revision.

Det anbefales at introducere en bedømmer. Opgaven med at vurdere om en given part lever op til føderationens aftaler og politikker kan varetages i forbindelse med den årlige IT-revision. Dette gælder for en dansk national føderation og det anbefales at undersøge hvad IT-revisionen skal udvides med, samt hvordan denne akkreditering kan foregå i praksis.

Vurdering af risici og autenticitetsniveau

En serviceudbyder skal per ressource, som denne udbyder, afgøre hvilke sikkerhedskrav en serviceaftager skal leve op til for at få adgang. Denne vurdering beror på en analyse af de risici, der vil være hvis uautoriserede serviceaftagere skaffer sig adgang og risikovurderingen definerer så hvilken kvalitet akkreditiver nødvendigvis mindst må have. Bemærk at dette alene relaterer sig til styrken af akkreditiver, ikke til aktiv adgangskontrol, hvor en serviceudbyder kontrollerer at serviceaftager har den fornødne autorisation til at tilgå ressourcen.

For at vurdere sårbarheden, dvs. den konsekvens der kan være ved fejl i forbindelse med autenticitetssikring kan en afhængig part benytte nedenstående skema, hvor "-" angiver at det angivne niveau slet ikke kan anvendes i forbindelse med den angivne risiko:

Risiko ifht. niveauer af autenticitet				
Kategorier af konsekvenser ved fejl i forbindelse med autenticitetssikring	**1**	**2**	**3**	**4**
Ulempe, kval eller tab af anseelse	Lille	Moderat	Moderat	Stor
Økonomisk tab eller ansvarspådragelse	Lille	Moderat	Moderat	Stor
Skade på myndighedsaktiviteter eller andre offentlige interesser	-	Lille	Moderat	Stor
Ikke-autoriseret frigivelse af sensitiv information	-	Lille	Moderat	Stor
Fysisk personskade	-	-	Lille	Stor
Mulighed for at begå/modvirke opklaring af ulovligheder	-	Lille	Moderat	Stor

Autenticitetsniveauet for en ressource beregnes ud fra maksimumsprincippet over de identificerede risici. En ressource, hvor der f.eks. er lille risiko for ulempe, kval eller tab af anseelse og en lille risiko for fysisk personskade skal således kræve autenticitetsniveau 3.

Foruden at sikre sig, at der anvendes det mindste nødvendige niveau for autentifikation, skal en serviceudbyder også forholde sig til relevante sikkerhedsforanstaltninger for udbudte ressourcer. Disse falder i to kategorier, men den samlede informationssikkerhed udgøres af summen af foranstaltninger:

- **Tekniske**, hvor der fokuseres på krav til styrken af autenticiteten, hærdning af maskinel, anvendelse af krypteringsmekanismer til sikring af konfidentialitet, integritet, mm.

- **Organisatoriske**, hvor der fokuseres på procedurer og retningslinjer, revision og kontrol, mm.

En diskussion af emnet findes i [ReferenceSikkerhed] s. 43ff og arbejdet her kan bruges som udgangspunkt for en egentlig fastlæggelse af hvilke sikkerhedsforanstaltninger der er nødvendige i forskellige situationer sammen med anbefalingerne i [NIST], som beskrevet ovenfor.

Det anbefales, at defineres modeller for vurdering af risici og nødvendig informationssikkerhed i forbindelse med beskyttelse af ressourcer. Arbejdet bør tage udgangspunkt i [NIST] og [ReferenceSikkerhed].

Et trust framework

Et trust framework rummer således et sæt af retningslinjer og procedurer m.v., som parterne, der anvender trust frameworket kan acceptere at overholde, så der kan etableres gensidig tillid.

Trust frameworket skal fastsætte egenskaber som kvaliteten af udstedelsesprocessen af digitale identiteter, herunder hvilke autorisationer en person får; der skal være krav til sikkerheden omkring opbevaring og transmission af identiteter, samt krav til selve autentifikationsfasen hos den enkelte IdP. Derudover skal der være enighed om mere forretningsorienterede elementer, så som krav til at opnå et bestemt autenticitetsniveau. Trust frameworket skal stille redskaber til rådighed for parterne til at fastsætte hvilket autenticitetsniveau en type service eller ressource skal kræve.

For at trust frameworket har en værdi er det essentielt med bedømmelse og kontrol af de enkelte parters overholdelse af fremsatte retningslinjer og specifikationer. Dette kræver en organisation omkring trust frameworket.

Det anbefales, at der udarbejdes et nationalt trust framework baseret på eksisterende arbejde i STORK og Kantara projekterne, tilpasset danske forhold. Det anbefales desuden, at trust frameworket eksplicit erklæres i udstedte tokens (fx via en URI), så man automatisk kan bruge denne viden i adgangsbeslutninger / håndhævelse hos modtageren.

Analyse af de nuværende standarder i sundhedsdomænet

Den nuværende anbefalede standard for web service kommunikation i sundhedsvæsenet er "Den Gode Web Service" (DGWS) version 1.0.1. Den mest udbredte anvendelse af standarden ses gennem Fælles Medicinkort, hvor samtlige EPJ systemer, samtlige Lægepraksissystemer (LPS) og en række andre systemer er WSC'er mod den centrale FMK løsning. Standarden blev udarbejdet af MedCom i 2006-2007 som en profilering af en række ledende internationale Web Service standarder, og har medvirket til at konsolidere sikkerhedsløsninger for især nationale web services. Derudover har DGWS også dannet rammen omkring indførelse af "stærk autentifikation" ved anvendelse digitale medarbejder- og virksomhedscertifikater i relation til system-til-system integration.

Uhensigtsmæssigheder i den nuværende standard

DGWS er ikke blevet opgraderet i takt med at de internationale standarder og løsninger har udviklet sig siden DGWS blev skabt. Det gør blandt andet at DGWS i dag ikke uden besvær kan sameksistere med nogle af de mest markedsunderstøttede standarder, og inviterer dermed ikke internationale spillere ind på det danske marked.

Også lovgivningen i Danmark har flyttet sig, ligesom borgeres og tilsynsførende myndigheders fokus har ændret sig i den mellemliggende periode. F.eks. er der mere fokus på borgerens indsigt og medvirken i 'beskyttelse' af helbredsdata her i 2014, end der var i 2006. F.eks. kan samtykkeinformationer (og en række andre vigtige sikkerhedsinformationer) ikke kommunikeres med den nuværende udgave af DGWS.

Ud over disse mere overordnede uhensigtsmæssigheder, har den konkrete anvendelse af DGWS i f.eks. FMK vist sig at have nogle mere tekniske uhensigtsmæssigheder eller mangler. Nogle af disse er meget tekniske (detaljer kan findes i Appendiks 4: Uhensigtsmæssigheder og begrænsninger ved DGWS), men hovedobservationerne listes nedenfor.

Uhensigtsmæssigheder i selve DGWS specifikationen

Selve standarden har nogle uhensigtsmæssigheder, der dels hidrører fra nogle mindre heldige beslutninger, der blev taget da den blev udfærdiget 2006, og dels er opstået som følge af, at de standarder, som DGWS benytter sig af, har udviklet sig uden af DGWS har fulgt med. En af de væsentligste uhensigtsmæssigheder er, at DGWS blander forskellige sikkerhedsaspekter sammen. DGWS 1.0.1 opererer med 5 sikkerhedsniveauer, der ikke alene beskriver autentifikationsniveau, men også inkluderer aspekter som forskellige subjekt typer og uafviselighed. Det gør det svært at øge eller reducere kravene i én sikkerhedsdimension (f.eks. autentifikationsstyrke) uden at det får konsekvenser i andre sikkerhedsdimensioner (f.eks. uafviselighed), hvilket er meget uhensigtsmæssigt. På den sikkerhedsmæssige side, benytter DGWS en sikkerhedsfunktion, som eksperter fraråder at anvende i fremtidige løsninger, da forskere har fundet svagheder i sikkerhedsfunktionen. I listeform er der afdækket flg. uhensigtsmæssigheder med DGWS specifikationen:

- Autentifikationsniveau svarer ikke til gængse klassifikationer
- Manglende overholdelse af SAML2 standarden på tre punkter (SAML2 standarden er grundstenen i DGWS og NemLogin)

- Understøtter ikke den nyere SOAP 1.2 standard
- DGWS anvender en sikkerhedsfunktion, der af eksperter frarådes pga. kendte svagheder.
- Der er kendte fejl specifikationen, som ikke er blevet rettet
- DGWS specificerer ikke protokol eller beskedindhold i relation til udstedelse af tokens (hos STS-servicen)
- DGWS specificerer ikke relationen til nyere standarder for web service beskeder, der indeholder større (binære) datamængder (f.eks. billeder).

Uhensigtsmæssigheder som følge af begrænsninger

At udarbejde en god standard er en svær balancegang mellem på den ene side at indsnævre mulighederne (og fejlfortolkningsmulighederne), så der opnås interoperabilitet, og på den anden side at åbne for at standarden også kan bruges i de tilfælde, hvor enkeltprojekter eller 'snævre' anvendelser har brug for at kommunikere særlige dataelementer ved anvendelse af standarden, men uden at standarden skal ændres. Da DGWS blev udfærdiget var man ikke opmærksom på dette, og standarden endte med at blive for rigid. Det har blandt andet afstedkommet, at man i flere projekter (herunder FMK) har set sig nødsaget til at lægge ekstra sikkerhedsinformationer 'ved siden af' det token, som DGWS specificerer. Andre projekter har gjort noget tilsvarende. På listeform er flg. uhensigtsmæssigheder blevet identificeret, som kan henledes til begrænsninger:

- Sammenblanding af identifikationsinformationer og kontekstinformationer, hvilket giver udfordringer i forhold til behov for genudstedelse af tokens ved kontekstskifte. I praksis har projekterne valgt ikke at kræve genudstedelse, men blot at undlade at bruge disse dele af tokenet og lade tokenet være 'misvisende' når brugeren ændrer kontekst.
- Mangelende udvidelsesmuligheder for attributter, som beskrevet ovenfor.
- Relationsbegrebet er ikke understøttet i DGWS, dvs. sikkerhedsinformationer som samtykke og behandlingsrelation kan ikke kommunikeres med DGWS.
- Manglende sondring mellem system og medarbejder tokens.
- DGWS understøtter alene system og medarbejder tokens, men ikke tokens for borgere/patienter.
- DGWS understøtter ikke muligheden for at kommunikere flere tokens, f.eks. ét token vedrørende brugeren og ét vedrørende systemet (eller en mellemliggende service gateway).
- DGWS giver ikke mulighed for at angive om, hvorledes og hvornår dataelementer er blevet verificeret mod autoritative kilder.
- DGWS indeholder pt. ikke muligheder for at angive unikke id'er for hvilke klassifikationer der ligger til grund for attributværdierne.
- DGWS indeholder ikke specifikationer om udstedelse eller veksling af tokens.

Uhensigtsmæssigheder i relation til sikkerhed

Allerede tilbage i pilotafprøvningen af DGWS (SOSI projektet) blev det påpeget, at én af svaghederne ved DGWS var manglen på såkaldt *message integrity,* dvs. en systemmæssig binding af det token, der sendes med i web service beskeden til netop denne besked. Manglen på *message integrity* gør det muligt at foretage identitetstyveri, ved at 'løfte' sikkerhedstokenet ud af en opsnappet besked og putte denne på en anden opsnappet besked. Risikoen for denne type angreb vurderes ret lille, idet alle beskeder i dag sendes via

sundhedsdatanettet, men netop denne forudsætning gør det svært at bruge standarden i andre sammenhænge, f.eks. i forhold til borgere (telemedicin) eller private virksomheder. På listeform er flg. uhensigtsmæssigheder blevet identificeret, som kan henledes til uhensigtsmæssigheder ift. sikkerhed:

- Mangel på *message integrity,* som beskrevet ovenfor
- Sundhedsdatanettet (eller tilsvarende) er en forudsætning for sikkerheden
- Ingen mulighed for at tilegne tokens til en bestemt service, serviceudbyder eller subdomæne.
- DGWS understøtter ikke krypterede tokens
- Mangel på sessionsstyring, herunder styring og koordinering af single log-out.

Øvrige praktiske uhensigtsmæssigheder

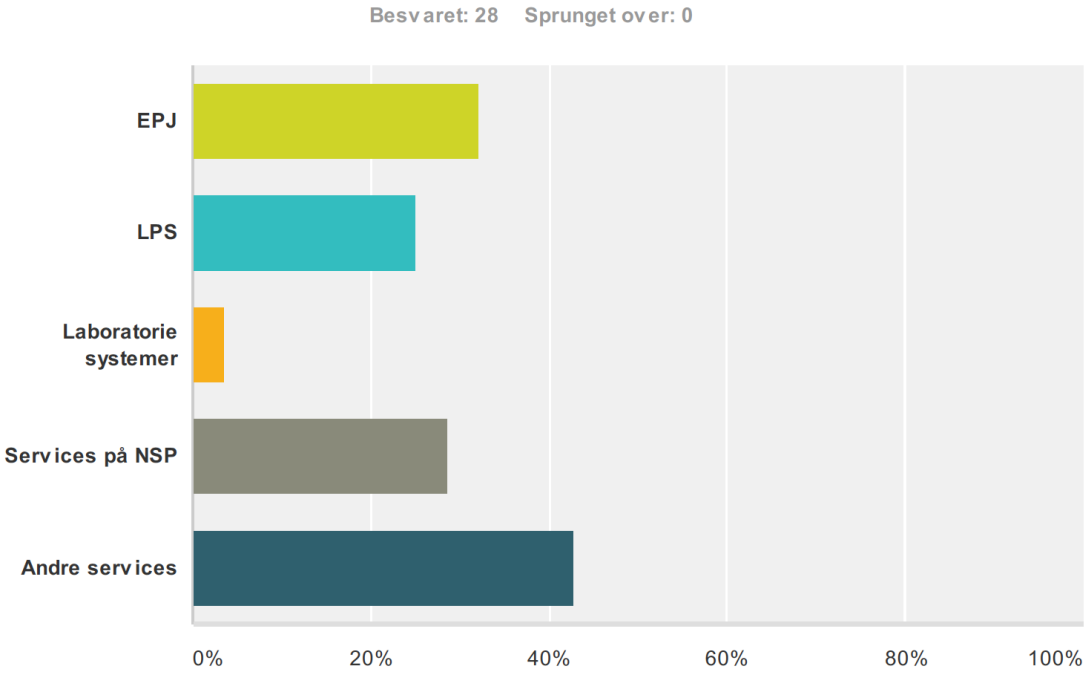
I udarbejdelsen af DGWS indarbejdede Medcom nogle af de samme krav som til øvrige beskedstandarder, herunder krav om genforsendelse af svar, dvs. serviceudbydere skal genfremsende præcist det samme svar, hvis man modtager den samme forespørgsel igen. Dette krav er meget svært at leve op til, idet det potentielt kræver at samtlige tidligere afgivne svar skal opbevares eller skal kunne genproduceres, selv om datagrundlaget har ændret sig. Øvrige praktiske uhensigtsmæssigheder på listeform:

- Krav om genforsendelse af svar, som beskrevet ovenfor
- DGWS har nogle uhensigtsmæssige krav til rækkefølgen af de XML elementer, der sendes i web service beskeden
- Snæver standardisering af fejlbeskeder
- Manglende understøttelse for andet end request/response kommunikationsmønstret (f.eks. mangel på mulighed for envejs kommunikation)
- Standarden findes kun på dansk.

Leverandørernes opfattelse af den nuværende standard - spørgeskema

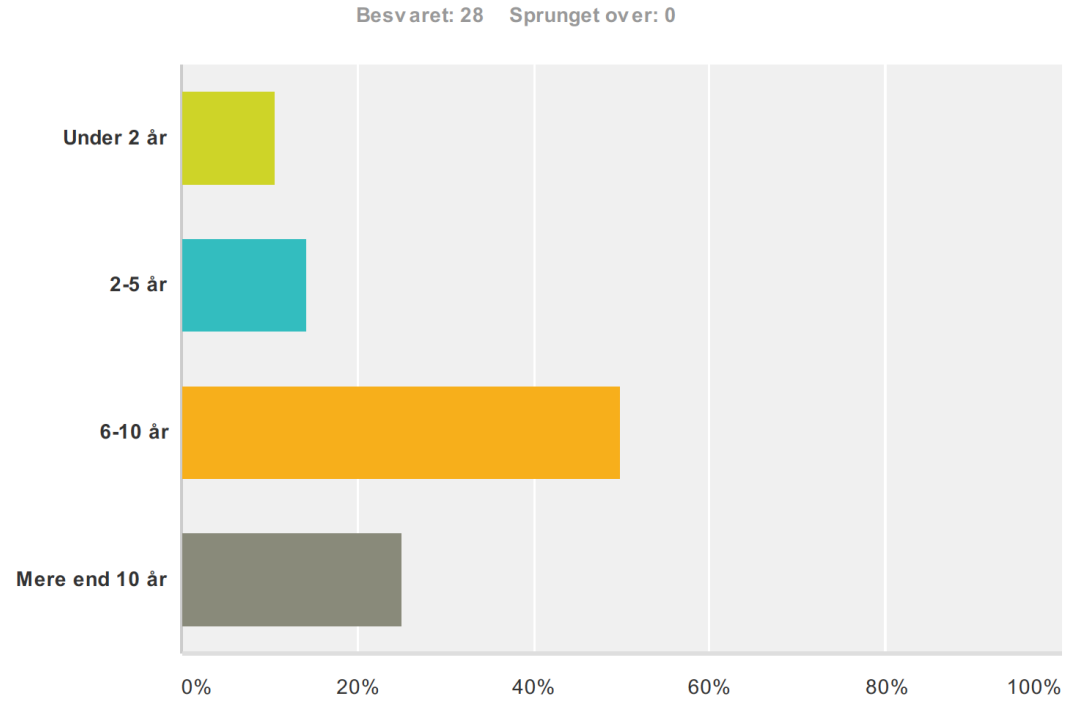
Som ovenfor nævnt, blev der i forbindelse med denne analyse dels afholdt møder med leverandører, dels udsendt spørgeskemaer til samme. Især spørgeskemaerne gav mulighed for at evaluere på den nuværende standard. I alt 58 parter har modtaget spørgeskemaet, hvoraf 27 (46%) har fundet tid til at svare på undersøgelsen. Modtagerne var primært leverandører af sundheds-it systemer. Efterfølgende er enkelte respondenter – der eksplicit har givet tilladelse til dette i undersøgelsen – blevet kontaktet for uddybning på enkelte tekniske punkter. Undersøgelsens spørgsmål og de opsummerede svar kan ses i Appendiks 5: Spørgeskema til leverandører – opsummering af svar.

Besvarelserne afspejler en bred anvenderskare fra EPJ over EOJ til LPS-leverandører, speciale-løsninger samt service- og integrationsleverandører:



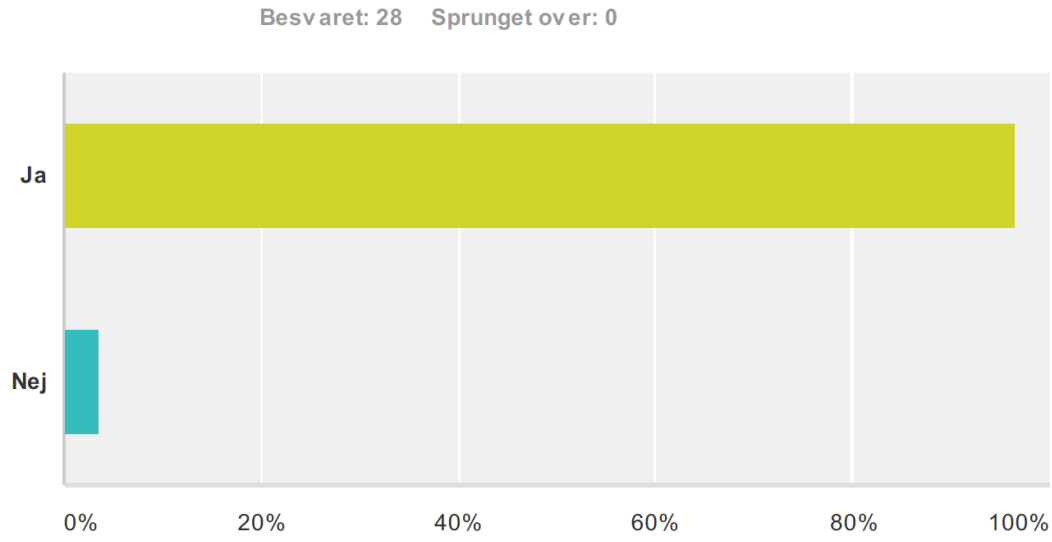
Figur 25: Hvilke type løsninger leverer I?

Respondenterne afspejler ligeledes en bred og relativ lang erfaring med at udvikle og implementere web services løsninger på området for sundheds-it:



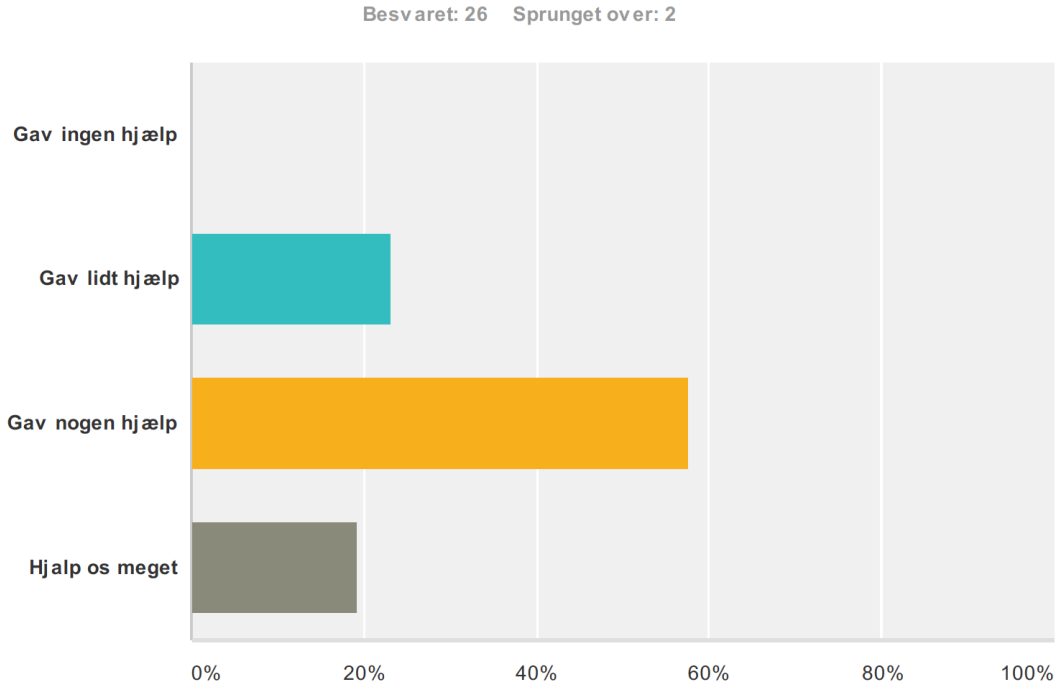
Figur 26: Hvor længe har virksomheden arbejdet med web services indenfor sundhedsområdet?

68% af respondenterne har et højt eller et meget højt vidensniveau om DGWS.



Figur 27: Har I haft behov for at læse specifikationen til DGWS (Den Gode Web Service)?

På trods af biblioteksunderstøttelse og "indpakning" indikerer 96% af de adspurgte, at de alligevel har haft behov for at læse og konsultere specifikationen for DGWS. Alle respondenter har fundet støtte i at læse specifikationen. Dog i varierende omfang. 77% har fundet *meget* eller *nogen hjælp* i specifikationen.



Figur 28: [Opfølgende til ovenstående spørgsmål] Hvis ja. Hvor meget hjalp den jer?

De tungestvejende begrundelser for at anvende standarder handler om konsolidering af kompetencer og løsninger. Dernæst angiver respondenterne at de ser fordele i at få adgang til frameworks/biblioteker- og fælles vidensressourcer.

Svarvalg	Besvarelser	
Brug af standarder gør det muligt for os at genbruge og konsolidere kompetencer	80,77%	21
Brug af standarder gør det muligt for os at minimere antallet af forskellige sikkerhedsløsninger	65,38%	17
Brug af standarder gør det muligt for os adgang til fælles vidensressourcer (communities etc.)	50%	13
Brug af standarder gør det muligt for os at anvende nationale og internationale frameworks	53,85%	14
Brug af standarder gør det muligt for os at imødekomme krav fra aftagerne af vores løsninger	23,08%	6
Brug af standarder giver os reelt ingen fordele (Forklar i tekstboxen nedenfor)	3,85%	1
Respondenter i alt: 26		

Figur 29: Hvilke gevinster ser I generelt ved standardiserede sikkerhedsløsninger?

Respondenterne angiver generelt at det er vigtigt med understøttende aktiviteter i forhold til adoption af standarder. Gode specifikationer, vejledninger og direkte udviklingsstøtte i form af kode-eksempler og udviklingssupport vægtes højest. Erfa-grupper, kurser og fora bliver ikke umiddelbart tillagtsamme betydning.

	Ingen indvirkning	Lille indvirkning	Nogen indvirkning	Stor indvirkning	Meget stor indvirkning	I alt
Utilstrækkelige standardspecifikationer	0% 0	8,33% 2	16,67% 4	45,83% 11	29,17% 7	24
Utilstrækkelige vejledninger og dokumentation	0% 0	4,17% 1	20,83% 5	33,33% 8	41,67% 10	24
Ingen eller utilstrækkelige eksempler på kommunikation (XML)	0% 0	4,35% 1	39,13% 9	30,43% 7	26,09% 6	23
Ingen eller utilstrækkelige kodeeksempler i 'moderne' udviklingsrammeværk	0% 0	8,33% 2	41,67% 10	29,17% 7	20,83% 5	24
Udfordringer med opbygning af nye skillsets ifm. kommende nye standarder	0% 0	26,09% 6	47,83% 11	21,74% 5	4,35% 1	23
Dårlig adgang til vidensressourcer (erfaringer fra andre, vidensfora, FAQ, kurser etc.)	4,17% 1	20,83% 5	33,33% 8	29,17% 7	12,50% 3	24
Dårlig adgang til vidensopbygning (kurser, code camps mv.)	20,83% 5	20,83% 5	37,50% 9	16,67% 4	4,17% 1	24
Dårlig adgang til udviklingssupport (en person, der kan ringes til)	4,17% 1	20,83% 5	45,83% 11	20,83% 5	8,33% 2	24

Figur 30: I hvor høj grad vil følgende udfordringer påvirke jeres arbejde med sikkerhedsstandarder?

Spørgeskemaet har også forsøgt at afdække, hvilke dele af de nuværende hjælpeværktøjer (eksempler, biblioteker etc.) der har leveret mest værdi for leverandørerne, og om det vil være muligt at erstatte nogle af disse elementer:

Svarvalg	Besvarelser	
Det vil være en kardinalbrøler!	4,17%	1
Det vil være usmart	12,50%	3
Det vil give nogenlunde samme muligheder og hjælp som nu	50%	12
Det vil give os bedre hjælp	12,50%	3
Det ville være super!	20,83%	5
I alt		24

Figur 31 - I hvor høj grad vil det påvirke støtten til jeres udvikling, hvis man i fremtiden vælger at afløse SEAL bibliotekerne med nogle eksempler/referenceimplementationer baseret på moderne rammeværk kombineret med nogle test-muligheder?

Analysen viser, at hvis man understøtter standarden med eksempler/referenceimplementationer og nogle muligheder for at validere sin anvendelse af standarden, vil 83% af leverandørerne føle at de enten får samme eller bedre hjælp end i dag.

Afdækningen viser at der som sådan ikke er de store forskelle mellem Java og .NET-repræsentanter i vurderingen af barrierer i forhold til implementering af sikkerhedsstandarder. Det er de anvendere, som anvender at andet programmeringsmiljø (delphi, 4D) som – naurligt nok – har haft det sværest med at anvende Seal.Net. Når man ser bort fra disse er der ikke den store forskel mellem hvor svært det har været for respondenterne at anvende hhv. Seal.Java eller Seal.Net.

I forhold til kvaliteten af specifikationen, reference-implementationer og udviklingssupport har repræsentanterne for henholdsvis Java og .Net svaret nogenlunde ens. Til gengæld vurderes vigtigheden af testklienter, biblioteksunderstøttelse samt kurser, erfa-grupper og code-camps generelt højere i Java.

Resultatet af øvrig leverandørinvolvering

Den 21/2-2014 blev nuværende standarder, hjælpeværktøjer og øvrige understøttende elementer diskuteret på et møde med udvalgte leverandører (se referat fra mødet i Appendiks 6: Opsamling fra leverandørmøde). Hovedparten af de inputs, der kom fra leverandørerne omhandlede styring af standarder og standardiseringsprocesser. Nedenfor ses de samlede konklusioner fra mødet.

- ✓ **Værdien af standarder**
  - Standarder medvirker til at indsnævre spannet af løsningsmuligheder. Standarderne inkorporerer "best practice" i forhold til løsning af opgaven (f.eks. HL7's anvendelse af OID'er).
  - Standarder er i sig selv en gevinst, men den kan optimeres med en række hjælpemidler:
    1. Vejledninger
    2. Kodeeksempler
    3. Kørende kodeeksempler (testklienter)
    4. Biblioteker (primært for komplekse standarder som f.eks. sikkerhedsstandarder)

- Det bliver først 'nemt' (og dermed forretningsmæssigt fordelagtigt), når standarderne understøttes langt ned i ovenstående liste (3-4). Gevinsten ved standardiseringen vil være afhængig af dette.
- Ved uoverensstemmelse mellem to parters design, kan en standard være nyttig til at fastslå, hvad der er gældende (autoritativ tolkning)
- En god profilering af standarder kan være med til at reducere opgaven med at sætte sig ind i bagvedliggende standarder.

✓ **Om standardiseringsprocessen og governance**

- **Brug interessenterne aktivt**
  Valg af nye standarder skal ske ved inddragelse af de væsentligste interessenter (serviceudbydere, serviceanvendere, leverandører) i en anerkendelse af, at interessenternes behov (og behov for støtte) er *overordentligt* forskelligt. Der skal opdyrkes et *aktivt* og *modereret* community omkring profiler.
- **Pilotafprøvninger**
  Implementering af nye eller ændrede standarder skal ske gennem pilotafprøvninger. Pilotafprøvningerne skal ske med inddragelse af en stor del af kompetencespektret og gerne med inddragelse af flere domæner (især hvis standardens virkefelt ser ud til at være påvirket af opgaveglidning mellem domæner). **Bemærk:** Pilotafprøvning er en afprøvning af en operationel løsning (i drift) men i mindre skala. Det er *ikke* proof of concept.
- **Løbende evaluering og opfølgning**
  Sørg for at der sker løbende læring omkring anvendelsen af standarderne ved at foretage objektiv evaluering og synliggørelse af brugen. Dette skal også bruges til at identificere "lignende brug" af f.eks. attributter, så der på bagkant kan ske standardisering af dette.
- **Hold profilerne "levende":**
  Sørg for at standarder/profiler udvikler sig med forretningsbehov, jura, teknologi, opdaterede standarder, som profilerne benytter sig af etc.
- **Fokus på reel fornyelse og forandring**
  Sørg for stram styring af standardernes implementering, udbredelse og udfasning (lifecycle) og sørg for at afdække muligheder for (mere eller mindre 'automatisk') at forny eksisterende snitflader, så de udadtil ser ud som om de er renoverede. Dette vil nedbringe byrden ift. midlertidige løsninger.
- **Der skal være nogen, som 'bekymrer' sig om standarden**
  Erfaringen viser at man generelt godt ved, hvor man skal henvende sig ift. DGWS og SEAL, og det betragtes som meget værdifuldt.
- **'Nogen' skal have ansvaret og overblikket**
  Det er vigtigt, at standarder ikke bare introduceres "tilfældigt". Kandidater skal som udgangspunkt vælges ud fra en række principper og kriterier (CAMMS) og 'nogen' skal have myndigheden til og ansvaret for at foretage fornøden analyse inden pilotafprøvning. Disse 'Nogen' skal også være kontaktpunkt for spørgsmål eller ideer, der går på tværs af profiler eller ligger på kanten af profilerne.
- **Sørg for løbende at udvide specifikationer**
  Observationer om behov for standardisering skal relativt hurtigt ind i specifikationerne.

- **Der skal være nogen, som man kan kontakte**
  Kompetencespændet er enormt blandt sundhedsvæsenets leverandører, og derfor er det svært at specificere på en måde, så alle føler det nemt at anvende, men hvis/når der opstår problemer med fortolkning eller formulering, så skal der være nogen som man kan rette henvendelse til.
- **Det er en kunst at lave gode vejledninger**
  Der er brug for erfaringsopsamling og kvalitetssikring af vejledninger. Brug leverandørerne aktivt.

✓ **Om standardernes beskaffenhed**

- **Hold det simpelt**
  Som udgangspunkt skal de valgte standarder være "tynde" profileringer af internationale standarder/profiler. Det vil gøre profilerne mere kompatible med udviklingsværktøjer og –rammeværk, samt gøre det muligt at hente hjælp fra andre anvendelser i andre sammenhænge/lande.
- **Hold standarderne 'åbne'**
  Sørg for OID'er og/eller URI'er på alle attributter, så man kan finde frem til den entydige autoritative fortolkning (og udsteder). Det gør det også muligt at tilføje eller ændre i klassifikationer til allerede eksisterende attributter med minimal ændring til specifikationer og implementeringer.
- **Sørg for god sondring mellem obligatoriske, anbefalede og valgfrie informationer**
  Parterne efterspørger gode og solide beskrivelser af, hvad der **skal** anvendes, hvad der **bør** anvendes og hvad der **kan** anvendes.
- **Man skal kunne komme hurtigere i gang**
  Det skal være muligt at komme i gang med anvendelse af en ny standard i løbet af en halv dag. Kørende eksempler, testkode, testklienter og gode vejledninger. Man skal helst kunne komme i gang på egen hånd og i eget miljø (uden anvendelse af eksterne systemer og testmiljøer). NIAB (eget milø) -> Test0 (uden bureaukrati) -> Test 1 etc.).
- **Hjælpemidler skal understøtte hovedparten af anvenderne**
  Som udbyder af en standard skal man anerkende at man ikke kan hjælpe alle. Hvis man kan hjælpe 60%, så har man formodentligt fundet et passende niveau.

Konklusioner og anbefaling i relation til nuværende standard:

- **Den nuværende standard er utilstrækkelig**.
  Den nuværende standard på sundhedsområdet har brug for en overhaling. Der er flere forhold, der gør at standarden er blevet for rigid og på visse punkter er forældet. Hvis disse forhold ikke adresseres, kan det i værste fald give anledning til brud på sikkerheden.
- **Leverandørerne efterspørger solide specifikationer og gode eksempler**
  Af spørgeskemaundersøgelsen fremgik det, at det er vigtigt med gode specifikationer, idet specifikationerne bliver brugt. Foruden specifikationerne har leverandørerne dog brug for nogle gode vejledninger, eksempler og testværktøjer, for at kunne implementere standarderne.
- **Leverandørerne efterspørger bedre styring og som minimum samme støtte.**
  Leverandørerne efterspørger bedre styring og mere dynamik i specifikationerne, så erfaringer og nye behov hurtigere understøttes af standarden. Desuden efterspørger leverandørerne bedre communities. Disse skal modereres af nogle, der 'følger' standarden.
- **Leverandørerne efterspørger bedre samspil med internationale markedsunderstøttede standarder**
  Den nuværende standard er for svær at anvende med øvrige internationale standarder (især IHE og HL7). Det anbefales at kommende standarder forholder sig aktivt til sameksistensen med internationale markedsunderstøttede standarder.

Forslag til fremtidige web service standarder for sundhedsvæsenet

Nærværende kapitel fremlægger forslag til nye/forbedrede standarder for system-til-system kommunikation inden for sundhedsdomænet og imellem sundhedsdomænet og andre domæner. Når der ikke fokuseres på standarder for web applikationer er det fordi de fagsystemer, som sundhedspersoner anvender, ofte baseres på klient serverløsninger med såkaldte "rige" klienter og fordi, at de web applikationer, der benyttes indenfor sundhedsdomænet, langt hen ad vejen baseres på samme standarder som indenfor andre domæner.

Analysen har fokuseret indsatsen på web service teknologien, da dette i dag er den absolut mest udbredte teknologi til system-til-system integration i sundhedssektoren. Det skal dog bemærkes, at flere parter har påpeget, at andre teknologier ('letvægtsprotokoller' som f.eks. JSON / REST) trænger sig på, og i nær fremtid vil kræve standardisering. Denne standardisering bør tværoffentligt tage sit udspring i Digitaliseringsstyrelsens arbejde (og på sundhedsområdet også det internationale arbejde med HL7 FIHR[12]).

Kommissoriet for nærværende analyse efterspørger svar på, om der vil være gevinster forbundet med at anvende fællesoffentlige standarder. På web service området er det OIOIDWS, der er den fællesoffentlige standard, og analysen skal derfor omfatte denne standard.

Men spørgsmålet i kommissoriet bør også sammenholdes med de øvrige forretningsmæssige og teknologiske drivere og tendenser der er på sundhedsområdet. Her efterspørges flere internationale spillere og mere fokus på anvendelse af internationale standarder (jf. også kapitlet: Strategiske overvejelser).

Et af de initiativer, som i stigende grad tiltrækker opmærksomhed fra internationale parter, er IHE[13],[14]. IHE leverer sjældent egne standarder, men specificerer hvorledes man på sundhedsområdet skal anvende en række andre standardiseringsorganisationers standarder (IHE profilerer standarder). IHE baserer deres profilering på meget høj grad af åbenhed, idet standardiseringsprocesserne (eller profileringsprocesserne om man vil) er velkendte og offentliggjorte, alle kan melde sig ind og deltage i profileringerne, præliminære resultater og beslutninger bliver offentliggjort etc. Derudover udvikler og driver IHE en række støtteværktøjer, blandt andet i form af referenceimplementationer og såkaldte 'connectathons', hvor leverandører kan vise, at deres produkter kan interoperere med andre leverandørers produkter. Især det sidstnævnte instrument differentierer IHE, og har medvirket til at IHE ikke blot udarbejder 'standarderne' men også at de reelt bliver implementeret med henblik på interoperabilitet og klinisk værdiskabelse.

---

[12] Se http://wiki.hl7.org/index.php?title=FHIR

[13] Integrating i Healthcare Enterprise. Formålet er beskrevet på deres hjemmeside: "IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively."

[14] EpSOS projektet (www.epsos.eu) valgte også at anvende IHE standarder til kommunikationen af helbredsinformationer på tværs af medlemsstater i EU.

Skal man se på mulige afløsere til den nuværende DGWS standard, er der således umiddelbart tre muligheder:

1. Beholde den nuværende domænespecifikke standard (DGWS), men modernisere den så uhensigtsmæssighederne i ovenstående kapitel imødegås. Denne mulighed omtales i det følgende som "DGWS version 1.1"
2. Erstatte den nuværende domænespecifikke standard (DGWS), med de fællesoffentlige standard (OIOIDWS). I praksis vil det være nødvendigt at subprofilere OIOIDWS, men dette kan ske som en meget "tynd" subprofil, der ikke kræver megen vedligeholdelse og support.
3. Erstatte den nuværende domænespecifikke standard (DGWS), med de tilsvarende internationale IHE standarder (IHE XUA mfl.). I praksis vil det sandsynligvis også være nødvendigt at subprofilere standarderne, så de særlige danske forhold indfanges af standarden (CPR numre, samtykke, behandlingsrelation, værdispring mv.). Igen bør dette ske som en meget "tynd" subprofil, der ikke kræver megen vedligeholdelse og support.

Overordnet set vil der være nogle fordele og ulemper ved hver af disse valg:

Mulighed	Fordele	Ulemper
DGWS 1.1	Sundhedsområdet vil med denne standard have friheden til at sammensætte standarden helt efter egne behov. Kun de nødvendige ændringer vil skulle indarbejdes (ikke en helt ny standard), hvilket kan medføre at biblioteker, eksempler og vejledninger i et vist omfang kan genanvendes.	Danmark vil fortsætte med at have en proprietær standard på sundhedsområdet. Fordele ved at samarbejde på tværs af fagdomæner i og uden for Danmark tabes. Leverandører, der leverer løsninger i flere fagdomæner eller som kræver integration på tværs af fagdomæner, skal opretholde flere kompetenceområder. Internationale leverandører har stadig dårlige muligheder for at komme ind på det danske marked og de danske løsninger vil ikke få det lettere ift. at komme ud på de internationale markeder.
OIOIDWS	Mulighed for synergi og fælles investeringer på tværs af fagdomæner inden for Danmark. Mulighed for dansk profilering af fagdomænefælles dataelementer.	Kræver subprofilering på sundhedsområdet. Nogle af støtteværktøjerne vil både skulle etableres på fællesoffentligt plan og tilpasses til sundhedsvæsenet, hvilket vil medføre parallelle udgifter.
IHE XUA	Stor synergi med internationale initiativer. Genanvendelse af IHE støtteværktøjer (referenceimplementationer, connectathons). Danske leverandører opnår bedre muligheder for at penetrere på	Standarden vil ikke kunne bruges på tværs af fagdomæner. IHE profilerne er ofte relativt 'defensivt' formuleret, og interoperabilitet/fortolkningssikkerhed opnås derfor først efter gennemførelse af connectathon.

	internationale markeder. Udenlandske leverandører får bedre adgang til det danske marked.

At komme nærmere en anbefaling af en specifik standard, kræver en dybere analyse af kandidaterne. I 2010 blev der i regi af organisationen Digital Sundhed gennemført en analyse og sammenligning af DGWS og OIOIDWS. Da analysen ligger 3-4 år tilbage, er det nødvendigt at foretage en fornyet vurdering. Digital Sundheds vurdering tog udgangspunkt i en opstillet model til vurdering af modenhed og egnetheden af standarder på sundheds-it området [SDSD model], mens nærværende analyse tager udgangspunkt i EU's CAMSS metode ("Common Assessment Model for Standards and Specifications"). CAMSS analysen vurderer og sammenligner forskellige standarder inden for flg. 7 kriterieområder:

1. **Applicability,** vurderer i hvilket omfang standarderne retter sig mod og skaber merværdi i det konkrete forretningsområde, og hvor godt standarderne understøtter 'tvær domæne' forretningsgange.
2. **Maturity,** vurderer modenheden af standarderne blandt andet i relation til kvaliteten og stabiliteten af standarderne.
3. **Openness,** vurderer i hvor høj grad standardiseringsprocesserne, som har udfærdiget standarderne har været åbne/offentlige, i hvor høj grad de væsentlige interessenter er blevet inddraget, hørt og har haft indsigelsesmuligheder
4. **Intellectual Property Rights**, vurderer licensforhold og andre juridiske forhold omkring standarderne
5. **Market Support,** vurderer markedsunderstøttelsen til/af standarderne, herunder hvor udbredt standarderne er, om der er proprietære forhold omkring standarderne etc.
6. **Potential,** vurderer standardernes potentiale ift. effekt, risiko og fremtidig vedligeholdelse og styring (standard governance) og endelig
7. **Coherence,** der vurderer standardernes sammenhæng til øvrige relaterede standarder (på EU plan) og om der er medlemsstater, der anbefaler eller kræver anvendelse af de pågældende standarder.

Mange af disse kriterier er overensstemmende med den oprindelige analyse fra Digital Sundhed [SDSD vurdering], og resultatet af vurderingen af modenhed og egnetheden af OIOIDWS og DGWS er da også konsistente med nedenstående resultater.

CAMSS vurderingen består af ja/nej svar på 51 spørgsmål inden for de ovennævnte 7 kriterieområder. Omfanget af afgivne svar afgør "styrken" af vurderingen. I [Bilag XX – CAMSS] findes de specifikke analysedata[15]. Den væsentligste værdi i CAMMS analysen består i at standarderne vurderes efter en række opstillede kriterier. Ved at besvare spørgsmålene kommer man godt omkring de forskellige aspekter ved standarderne. Da der kun er mulighed for at svare "ja", "nej" eller ikke at besvare, kan de enkelte svar virke lidt forsimplede (i en

[15] Det skal bemærkes, at kommissoriet til nærværende analyse, hvor der efterspørges analyse af specifikke standarder (nuværende standarder op mod danske fællesoffentlige standarder) medfører at de første procestrin i CAMSS modellen ikke er blevet gennemgået (proposal og consideration)

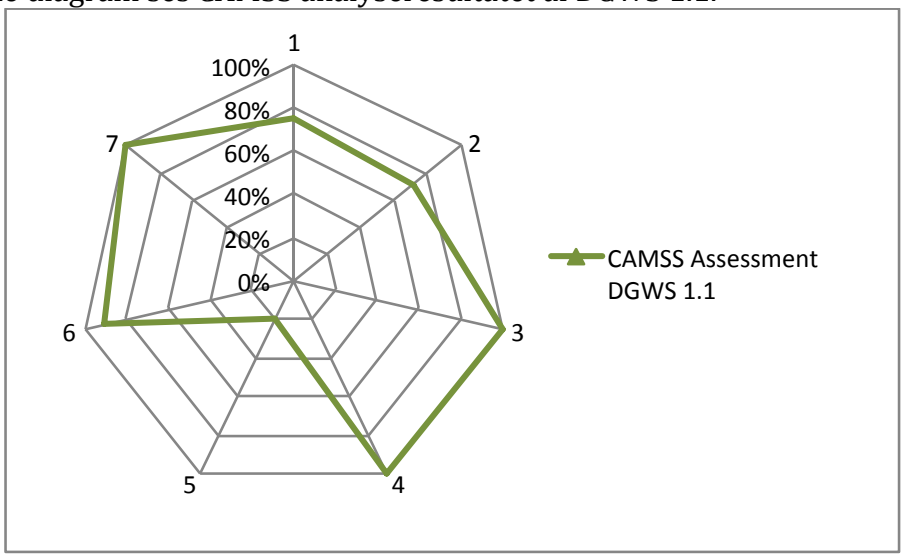
fremtidig anvendelse af metoden kunne man overveje at give mulighed for at graduere svarene). Man skal derfor ikke hænge sig alt for meget i de enkelte scoringer nedenfor.

En anden erfaring med at anvende CAMMS er, at det er nødvendigt at konkretisere de enkelte spørgsmål, herunder hvad det er for et perspektiv der anlægges og hvordan dette passer til den ønskede scoring. F.eks. vil et spørgsmål som A.1.: "Does the technical specification or standard address and facilitate interoperability between public administrations?" kunne besvares på to måder afhængig af, om der tænkes på interoperabilitet indenfor sundhedsdomænet eller mellem forskellige domæner.

Med disse forbehold opridses hovedobservationerne i CAMSS analysen i nedenstående afsnit. En uddybning af spørgsmål og svar er at finde i Bilag 1: CAMMS vurdering af DGWS, OIO IDWS og IHE.

CAMMS analyse af DGWS 1.1

I nedenstående diagram ses CAMSS analyseresultatet af DGWS 1.1.



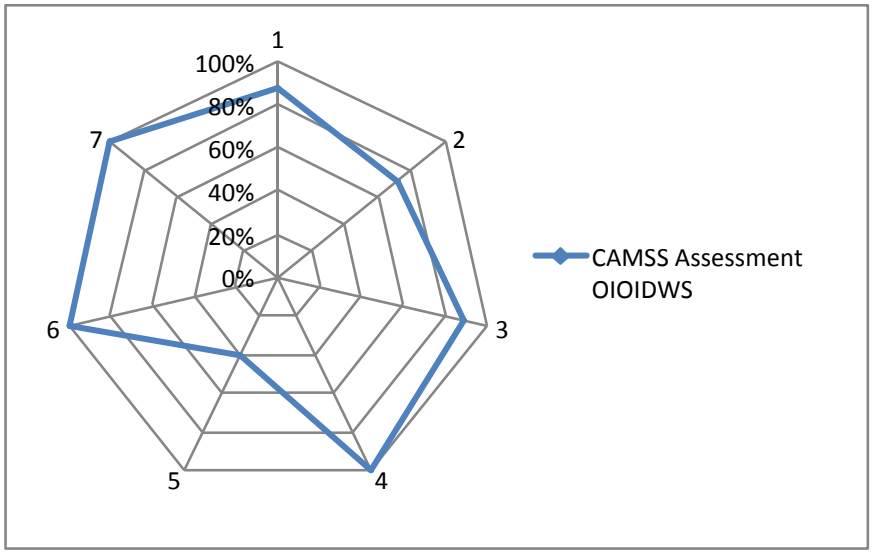
Figur 32 - CAMSS analyseresultat af DGWS 1.1 kandidaten.

Kriterieområderne 1 (applicability), 2 (Maturity) og især 5 (Market Support) er svage for denne kandidat. *Applicability* er relativt svag da den ikke forventes at kunne anvendes i andre fagdomæner og da den ikke vurderes til at levere merværdi ift. andre alternativer / profiler. *Maturity* er naturligt nok relativt svag, da der er tale om en uafprøvet standard, mens *Market Support* er svag da det er en proprietær dansk sundhedsstandard. **Den samlede score er 80%**.

Analysen er relativ sikker, idet det for denne standard har været muligt at finde svar på 97% af de relevante CAMSS spørgsmål.

CAMMS analyse af OIOIDWS (subprofileret til sundhedsområdet)

I nedenstående diagram ses CAMSS analyseresultatet af en kommende subprofil af OIOIDWS til sundhedsområdet.



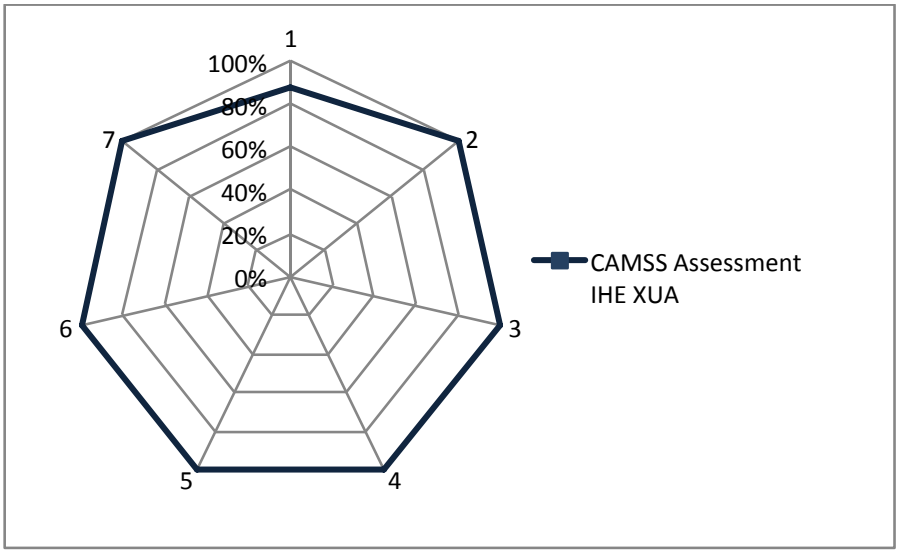
Figur 33 - CAMSS analyseresultat af OIOIDWS kandidaten. OIOIDWS er svag på markedssupport (5), idet der ikke findes ret mange realiseringer af denne standard endnu.

Kriterieområderne 2 (Maturity) og 5 (Market Support) er svage for denne standard. *Maturity* er svag, da der ikke findes ret mange realiseringer af standarden endnu og fordi der ikke findes mekanismer til at afgøre om løsningerne lever op til standarden. *Market Support* er meget svag, da standarden endnu ikke er blevet anvendt i forskellige fagdomæner, ikke har en væsentlig markedsandel og da der ikke findes aktive fora/interessegrupper omkring standarden. **Den samlede score er 87%.**

Analysen er relativ sikker, idet det for denne standard har været muligt at finde svar på 97% af de relevante CAMSS spørgsmål.

CAMMS analyse af IHE (subprofileret til sundhedsområdet)

I nedenstående diagram ses CAMSS analyseresultatet af en kommende subprofil af IHE XUA.



Figur 34 - CAMSS analyseresultat af IHE kandidaten.

IHE XUA scorer væsentligt højere end de to andre kandidater på kriterieområderne, hvilket primært skal tilskrives IHE organisationens åbenhed ift. standardiseringsprocesserne, og den store markedsmæssige udbredelse (internationalt). IHE XUA scorer ikke perfekt ift. *applicability*, hvilket er pga. bindingen til sundheds-fagdomænet.

Analysen er relativ sikker, idet det har været muligt at finde svar på 97% af de relevante CAMSS spørgsmål.

Det ville være naturligt at pege på IHE XUA standarden som den foretrukne og dermed anbefalede standard for fremtidens web service kommunikation på sundhedsområdet, men det ville efterlade sundhedsområdet på en standardiseringsmæssig "ø", idet disse standarder ikke umiddelbart kan anvendes til kommunikation imellem domænerne. Samtidig skal det bemærkes, at IHE profilerne forholder sig meget åbent i forhold til hvordan brugerne bliver autentificeret og hvordan tokens skaffes og evt. veksles. Vælger man at anvende IHE profiler skal man således stadig udarbejde profiler til hhv. autentifikation (og dermed profilere bootstrap tokens) og evt. vekslingsprotokoller.

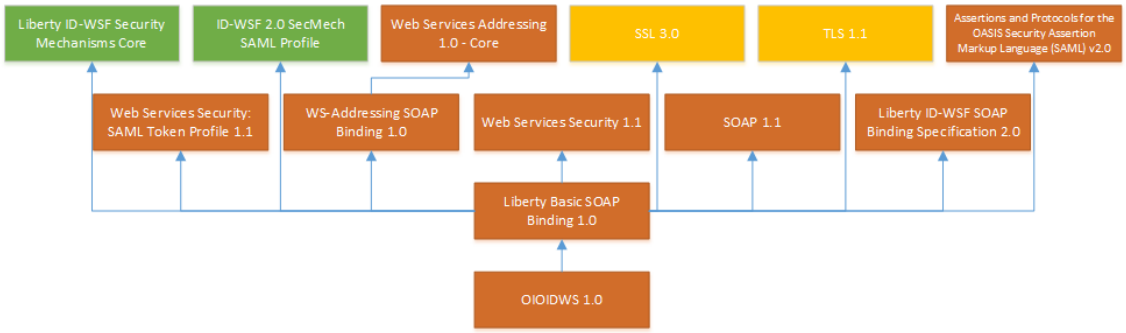
I relation til token veksling og format af bootstrap token har OIOIDWS allerede udarbejdet profiler, hvilket har ledt analyseprojektet til at undersøge, om det vil være muligt at kombinere OIOIDWS med IHE standarderne, og hvad der evt. skal ændres i OIOIDWS standarden for disse standarder kan sameksistere.

Sameksistens mellem IHE og OIOIDWS?

De to specifikationer bygger begge på en række eksisterende web service standarder, som enten profileres eller inkorporeres i specifikationerne.

Figurerne nedenfor giver et overblik over de relevante specifikationer, hvor

- **Rød** angiver at en specifikation er obligatorisk,
- **Gul** angiver at et eller flere elementer kan bringes i anvendelse og
- **Grøn** at specifikationen er informativ af karakter ifht. profilen.

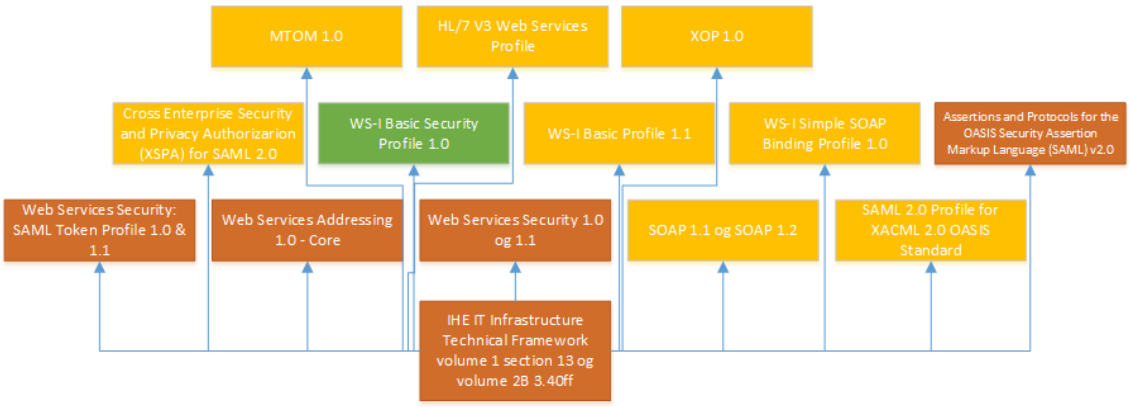


Figur 35: OIOIDWS Profilen og direkte afhængigheder

Afhængighederne i OIOIDWS er vist på figuren ovenfor og er som følger:

- **Liberty ID-WSF Security Mechanisms Core**: OIOIDWS er kompatibel med Liberty profilerne, men subprofilerer ikke disse direkte
- **ID-WSF 2.0 SechMech SAML Profile**: OIOIDWS er kompatibel med Liberty profilerne, men subprofilerer ikke disse direkte

- **WS-Addressing SOAP Binding 1.0**: Subprofileres og det specificeres hvordan addressing skal anvendes
- **Web Services Addressing 1.0 Core**: Subprofileres og det specificeres hvordan addressing skal anvendes
- **SSL 3.0**: Hvis konfidentialitet er nødvendig kan SSL 3.0 anvendes
- **TLS 1.1**: Hvis konfidentialitet er nødvendig kan TLS 1.0 anvendes
- **Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0**: Subprofileres
- **Web Services Security 1.1**: Subprofileres
- **Web Services Security: SAML Token Profile 1.1**: Subprofileres
- **SOAP 1.1**: OIOIDWS understøtter alene SOAP 1.1 og ikke SOAP 1.2
- **Liberty ID-WSF SOAP Binding Specification 2.0**: OIOIDWS er kompatibel med Liberty profilerne, men subprofilerer ikke disse direkte. Til gengæld forlanger profilen, at et enkelt element (Framework header) fra Liberty ID-WSF SOAP Binding Specification 2.0 medtages
- **Liberty Basic SOAP Binding 1.0**: Dette er reelt selve OIO-IDWS specifikationen for SOAP binding.



Figur 36: IHE XUA profilen og direkte afhængigheder

Afhængighederne i IHE XUA er vist på figuren ovenfor og er som følger:

- **Web Services Security: SAML Token Profile 1.0 og 1.1**: Anvendes direkte
- **Web Services Addressing 1.0 Core**: Subprofileres og det specificeres hvordan addressing skal anvendes, samt hvordan addressing information bindes i SOAP beskeden
- **Web Services Security 1.0 og 1.1**: Anvendes direkte
- **SOAP 1.1 og SOAP 1.2**: Når IHE XUA anvendes til andet end IHE XDS og HL/7 beskeder er det tilladt (men ikke anbefalet) at bruge SOAP 1.1. Ellers er SOAP 1.2 påkrævet.
- **SAML 2.0 Profile for XACML 2.0 OASIS Standard**: Når visse valgfri attributter bringes i anvendelse i SAML tokenet, anvendes XACML navngivning
- **Cross Enterprise Security and Privacy Authorizarion (XSPA) for SAML 2.0**: Når visse valgfri attributter bringes i anvendelse i SAML tokenet, anvendes XSPA navngivning
- **WS-I Basic Security Profile 1.0**: Refereres som en standard der kan anvendes efter behov

- **WS-I Basic Profile 1.1**: Anvendes meget løst (guidelines)
- **WS-I Simple SOAP Binding Profile 1.0**: Anvendes meget løst (guidelines)
- **Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0**: Subprofileres
- **MTOM 1.0**: Anvendes når der transmitteres IHE XDS beskeder
- **HL/7 V3 Web Services Profile**: Anvendes alene når der transmitteres HL/7 beskeder. Anvendes ikke ellers
- **XOP 1.0**: Anvendes når der transmitteres IHE XDS beskeder.

Som ovenfor nævnt er tokenudstedelse og tokenomveksling udenfor scope i IHE XUA standarden, men det anbefales at anvende SAML protokoller og WS-Trust. IHE anbefaler, at hvis der anvendes WS-Trust, så bør det være WS-Trust 1.3. OIO-IDWS profilerer WS-Trust 1.3 til tokenomveksling. Der er således ingen udfordringer i at lade disse dele af standarderne sameksistere.

IHE XUA baserer sig på XSPA-SAMLv1.0 OASIS Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of the Security Assertion Markup Language (SAML) for Healthcare v1.0". I nedenstående tabel ses en sammenligning mellem de elementer, som IHE XUA hhv. OIOIDWS benytter.

Emne	IHE XUA	OIO-IDWS
Profilering af SAML token format	IHE IT Infrastructure Technical Framework Volume 2b (ITI TF-2b) Section 3.40	OIO SAML Profile for Identity Tokens 1.0
Element /saml:Subject	Obligatorisk	Obligatorisk
Element /saml:SubjectConfirmation	bearer, holder-of-key	holder-of-key
Element /saml:Conditions	NotBefore, AudienceRestriction er obligatoriske	NotBefrore, AudienceRestriction er obligatoriske
Element /saml:Conditions	NotOnOrAfter er ikke angivet	NotOnOrAfter er obligatorisk
Element /saml:AuthnStatement	Obligatorisk	Valgfri
SAML Version	2.0	2.0

Som det ses, er de to profiler kompatible hvad angår de elementer, der indgår i tokenet. Det skal dog bemærkes, at IHE XUA's muligheder for at sende tokens, hvor SubjectConfirmation er "bearer" ikke vil være muligt[16] i Danmark.

IHE XUA specificerer hvordan attributter fra XSPA encodes, hvis de anvendes. XSPA definerer en række obligatoriske attributter hvorimod der i XUA skrives at 'When Local Policy requires that the following attributes are carried in the SAML assertion then they should be encoded as

[16] Alternativt skal OIOIDWS profilen udvides til også at tillade "bearer".

follows'. Nedenfor opsummeres derfor XSPA attributterne, hvor "M" angiver "Mandatory" og "O" "Optional":

Identifier	Obligatorisk
urn:oasis:names:tc:xacml:1.0:subject:subject-id	M
urn:oasis:names:tc:xspa:1.0:subject:organization-id	M
urn:oasis:names:tc:xspa:1.0:organization	M
urn:ihe:iti:xca:2010:homeCommunityId	M
urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	O
urn:oasis:names:tc:xacml:2.0:subject:role	M
Urn:oasis:names:tc:xspa:1.0:subject:functional-role	O
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	M
urn:oasis:names:tc:xacml:1.0:resource:resource-id	M
urn:oasis:names:tc:xacml:1.0:action:action-id	O
urn:oasis:names:tc:xspa:1.0:resource:hl7:type	O
urn:oasis:names:tc:xspa:1.0:environment:locality	M
urn:oasis:names:tc:xspa:2.0:subject:npi	O
urn:oasis:names:tc:xacml:2.0:subject:role	O
urn:ihe:iti:bppc:2007:docid	O
urn:ihe:iti:xua:2012:acp	O
urn:oasis:names:tc:xacml:2.0:resource:resource-id	O
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	O

OIO-IDWS definerer ikke nogen attributter, og der er således heller ingen problemer i at få de to profiler til at sameksistere på dette område. Desuden skal det nævnes, at IHE profilen ligesom OIOIDWS tillader, at der medsendes yderligere attributter end de der er defineret ovenfor. Profilerne har derfor ikke de samme uhensigtsmæssigheder som DGWS.

IHE XUAs profilering af SOAP er specificeret i "IHE IT Infrastructure Technical Framework Volume 2x (ITI TF-2x) Appendix V Web Services for IHE Transactions", mens OIO-IDWS anvender "Liberty Basic SOAP Binding 1.0".
Skemaet nedenfor afdækker forskellene på de to profileringer:

Emne	IHE XUA	OIO-IDWS
Profilering af SOAP binding	IHE IT InfrastructureTechnical Framework Volume 2x (ITI TF-2x) Appendix V Web Services for IHE Transactions	Liberty Basic SOAP Binding 1.0
SOAP Protokol	SOAP 1.2 (og SOAP 1.1)	SOAP 1.1
WS-Addressing (wsa)	Web Services Addressing 1.0 - Core W3C Recommendation 9 May 2006	Web Services Addressing 1.0 - Core W3C Recommendation 9 May 2006
Element /wsa:To	Obligatorisk	Obligatorisk

Element /wsa:ReplyTo	Obligatorisk	Valgfri
Element /wsa:MessageID	Obligatorisk (indirekte fordi ReplyTo er obligatorisk jævnfør ws-addressing)	Obligatorisk
Element /wsa:RelatesTo	Obligatorisk på svar	Obligatorisk på svar
Element /wsa:Action	Obligatorisk	Obligatorisk
Sikkerhed	Web Services Security: SOAP Message Security 1.0 og 1.1	Web Services Security: SOAP Message Security 1.1
/wsse:Security	Obligatorisk	Obligatorisk
/sbf:Framework	Ikke angivet	Obligatorisk
MTOM og XOP	Anvendes når der udveksles IHE XDS beskeder og her forlanges SOAP versionen samtidig at være 1.2	Kan indlejres, idet MTOM og XOP kan eksistere i SOAP 1.1

IHE XUA er her lidt mere stringent i bindingen til SOAP, idet der i nogle IHE profiler (f.eks. IHE XDS, som anvendes til deling af dokumenter og billeder) kræver SOAP version 1.2. For at de to standarder kan sameksistere, vil det derfor være nødvendigt at udvide OIOIDWS profilen til også at understøtte SOAP 1.2.

Konklusioner i relation til sameksistens mellem OIOIDWS og IHE profiler:

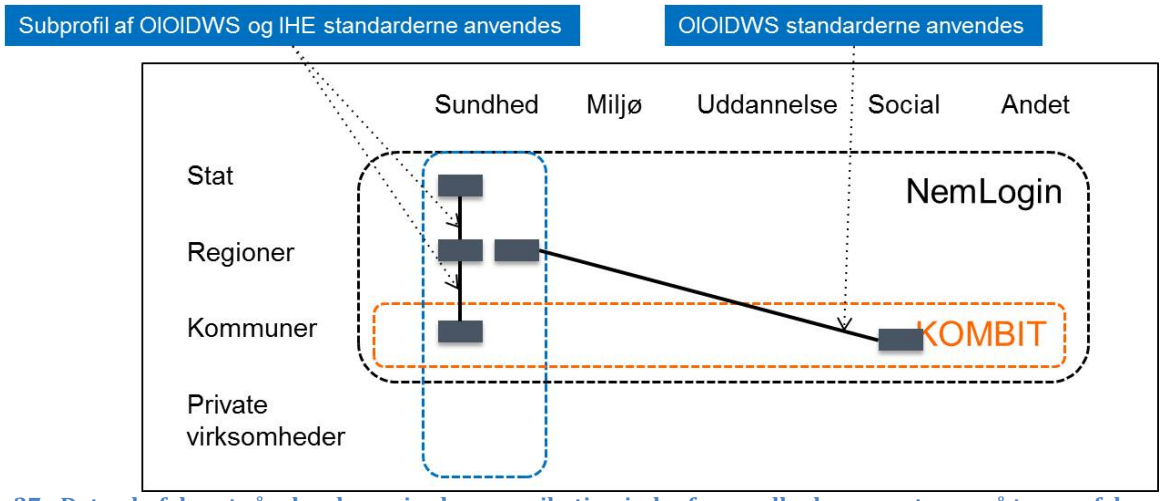
Det vil være muligt at bringe OIOIDWS og IHE XUA til at sameksistere. Umiddelbart er der ganske små forskelle, som skal håndteres:

- **SOAP version**. OIOIDWS skal udvides til også at tillade SOAP 1.2 binding
- **Bearer/Holder-of-Key.** Det bør overejes at udvide OIOIDWS til også at understøtte "bearer" subjectconfimation.

Derudover er der ingen sameksistensproblemer.

Sammenholdt med CAMSS analysen *anbefales der derfor, at sundhedsvæsenet i fremtiden anvender en tilpasser udgave af OIOIDWS (der samtidig bliver en subprofil af IHE XUA) som grundlag for kommunikationen* ***inden for sundhedsvæsenet****. Det anbefales at anvende OIOIDWS (ikke subprofileret), i relation til tjenester* ***uden for sundhedsdomænet.***

Anbefalingerne kan illustreres således:



Figur 37 - Det anbefales at såvel web service kommunikation indenfor sundhedsvæsenet som på tværs af domæner baseres på en revideret udgave af OIOIDWS standarden for så vidt angår sikkerhedstokens mv. Inden for sundhedsdomænet anbefales det at anvende IHE som indholdsstandard.

Figuren illustrerer, at systemer indenfor sundhedsområdet kan anvende en subprofil af OIO-IDWS og IHE-standarderne til at kommunikere med hinanden på tværs af kommuner, regioner og Stat. Omvendt behøver eksempelvis kommunale systemer, der benyttes indenfor andre områder end sundhedsområdet, ikke at anvende sundhedsområdets sub-profil til at kommunikere med services på sundhedsområdet, men kan i stedet benytte den fællesoffentlige OIO-IDWS standard rent.

Når subprofilen af OIOIDWS udarbejdes for sundhedsdomænet, skal denne kunne dække alle nuværende specialløsninger, der er opstået som følge af rigiditeten af DGWS, herunder:

- FMK programmets ekstra sikkerhedsattributter [FMK dokumentation][FMK Services]
- NPI projektets header attributter, herunder samtykke, behandlingsrelation og værdispring [HSUID], der også benyttes i forbindelse med Sundhedsjournalens integration til KIH-databasen (klinisk integreret hjemmemonitorering).
- Sundhed.dk's kontekstoverførsel i relation til "Sikker Browseropstart" [SundJournalAttrib]
  Den "Healthcare Context Token Profile" der blev udarbejdet i forbindelse med billetomvekslingsprojektet [NSI-context-token]

Endvidere bør sub-profileringsarbejdet orientere sig mod tidligere arbejde med at standardisere[17] sikkerheds- og kontekstattributter på sundhedsområdet:

- Den "Sign-on" profil som blev udarbejdet i regi af det nationale Sign-on projekt [SDSD-Sign-on-profile]
- De brugerstyringsattributter, der blev defineret i regi af Digital Sundhed som opfølgning på projektet sammenhængende brugeradministration [SDSD-bs-attrib-intro] [SDSD-bs-attrib-indhold] [SDSD-bs-attrib-politik] [SDSD-bs-attrib-ræsson]

[17] Alle specifikationer herunder er behandlet af arkitekturrådet i regi af Digital Sundhed og optaget i kataloget over standarder på sundhedsområdet [NSI-standardkatalog]

- Den subprofil, som blev lagt til grund for den tidligere sammenligning mellem OIO IDWS og DGWS [SDSD-IDWS-H-identity-token] (se også [SDSD-IDWS-H-overview] og [SDSD-IDWS-H-aut-token])

Skulle der mod forventning vise sig udfordringer ved at få samordnet IHE og OIOIDWS profilerne, vil sundhedsvæsenets prioritet være at standardisere via IHE profilerne. Den primære årsag til dette er, at langt de fleste kommunikationstransaktioner foregår inden for sundhedsdomænet, og den standardisering indenfor sundhedsområdet derfor vejer højere end tvær-domæne standardisering.

Sammenholdes ovennævnte analyseresultater med aktørernes tilbagemeldinger om ønsker og behov til standardisering, giver det anledning til følgende yderligere anbefalinger:

Øvrige konklusioner og anbefalinger i relation til kommende standarder:

- Det anbefales at der såvel på fællesoffentligt plan som i sundhedsdomænet etableres en række hjælpemidler og supportelementer for standarderne:
    - Udførlige programmeringsvejledninger som minimum i programmeringssprogene Java og .NET
    - Referenceimplementationer som minimum i programmeringssprogene Java og .NET
    - Etablering af test- og valideringsmuligheder, hvor udviklere kan få kontrolleret validiteten af de genererede web service beskeder.
    - Der skal oprettes "kom i gang" kodeprojekter, hvor udviklere meget hurtigt kan komme i gang med udviklingen i OIOIDWS standarden. På sundhedsområdet skal disse muligheder også omfatte muligheden for at komme hurtigt i gang på de fælles testmiljøer (uden bureaukratiske arbejdsgange).
    - Der etableres vedligeholdelsesorganer (Change Advisory Boards, CAB'er) på sundhedsområdet og på tværs af domæner til behandling af ændringer i løsninger og hjælpeværktøjer.
    - Etablering af nogle modererede fora, hvor udviklere og arkitekter kan udveksle erfaringer, tips og tricks

- Det anbefales at etablere governance organisationer på såvel fællesoffentlig som sundhedssammenhæng, mhp. at styre standardiseringen af OIOIDWS (hhv. subprofilerne) samt iværksætte nødvendige moderniseringstiltag i takt med udviklingen på international og markedsmæssig plan.

Anbefalingerne afspejler udviklingen af udviklingsværktøjer, hvor man for 8 år siden (da DGWS blev skabt) ikke havde samme muligheder for understøttelse i gængse rammeværk, hvorfor det dengang var meget fornuftigt at understøtte DGWS med et relativt komplet programmeringsbibliotek. I dag skal der være mere fokus på, at den værktøjsunderstøttelse, der skal ledsage en profil på sundhedsområdet, kan integreres i gængse rammeværk. Leverandørernes ønsker uddybes mere i næste kapitel.

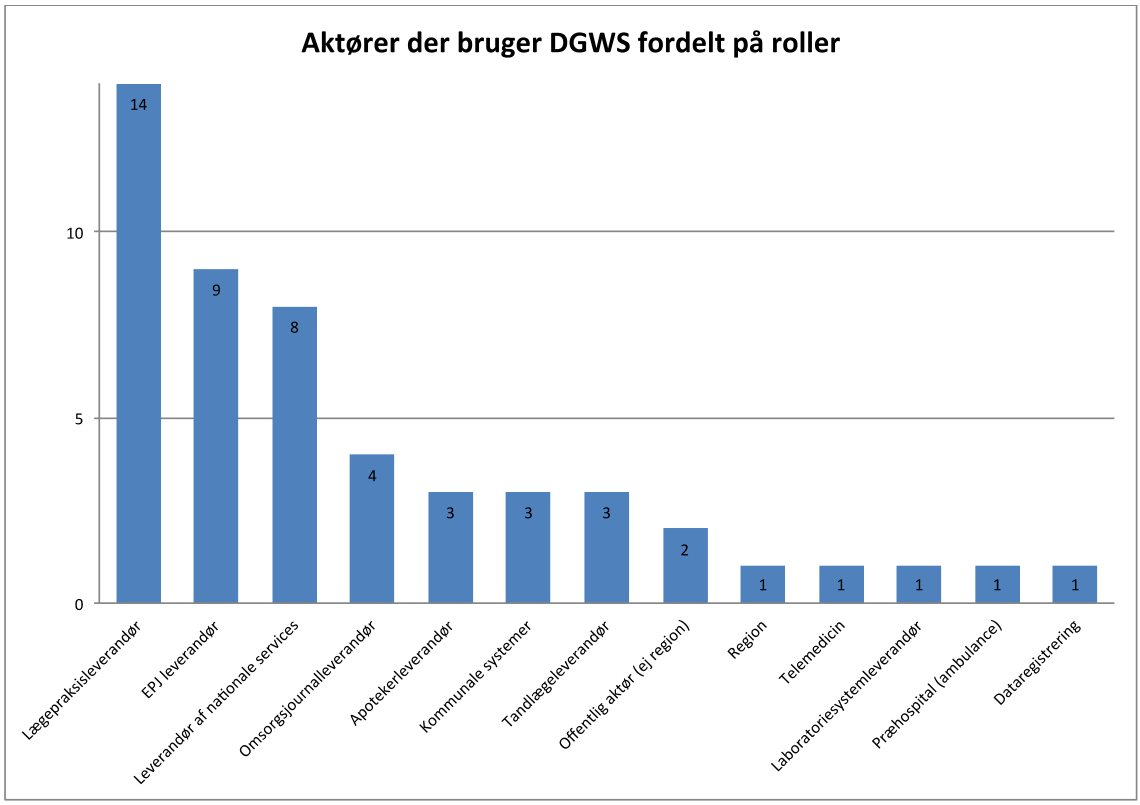
Migreringsovervejelser

Siden 2006 har Den Gode Web Service (DGWS) været anvendt som standard for identitetsbaserede webservices i det danske sundhedsvæsen. Gennem årene er standarden blevet relativt bredt udbredt, ikke mindst som følge af implementeringen af Det Fælles Medicinkort (FMK). Præcis hvor bred udbredelse der er af den nuværende standard, analyseres i dette kapitel, med henblik på at estimere hvor stor migreringsopgaven fra nuværende til ovenstående anbefalede standarder vil være, og hvilken migreringsstrategi, der bør lægges til grund.

Udbredelsen af den nuværende standard baserer sig på analyse af logudtræk fra NSP platformen, interviews af nøglepersoner, samt en spørgeskemaundersøgelse[18]. For en mere præcis gennemgang af afdækningsmetoden henvises til Appendiks 3: Metode for afdækning af udbredelse af nuværende standard.

Aktører der bruger den nuværende standard?

Der er i analysen identificeret ca. 50 aktører, som anvender de omtalte standarder på sundhedsområdet. Langt hovedparten af disse aktører er private virksomheder, som er leverandører til stat, regioner og kommuner. I Figur 38 nedenfor ses en kategorisering af aktørerne fordelt på forskellige leverandør/aktør typer.

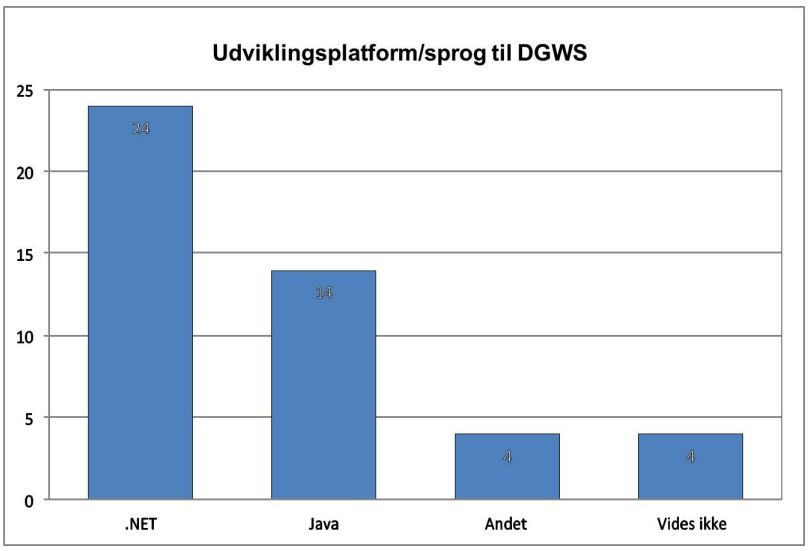


Figur 38 – Aktører fordelt på roller/leverandørtyper[19].

[18] Ikke den føromtalte spørgeskemaundersøgelse, men en spørgeskemaundersøgelse skræddersyet til netop afdækning af nuværende standard.

[19] Enkelte af ovenstående aktører er leverandør af flere typer systemer. I diagrammet er disse opført for hver af deres

Aktørerne bruger forskellige udviklingsplatforme, programmeringssprog og hjælpemidler. I nedenstående diagrammer ses fordelingen af disse.



Figur 39 – Udviklingsplatform og –sprog som anvendes til fortolkning af DGWS.

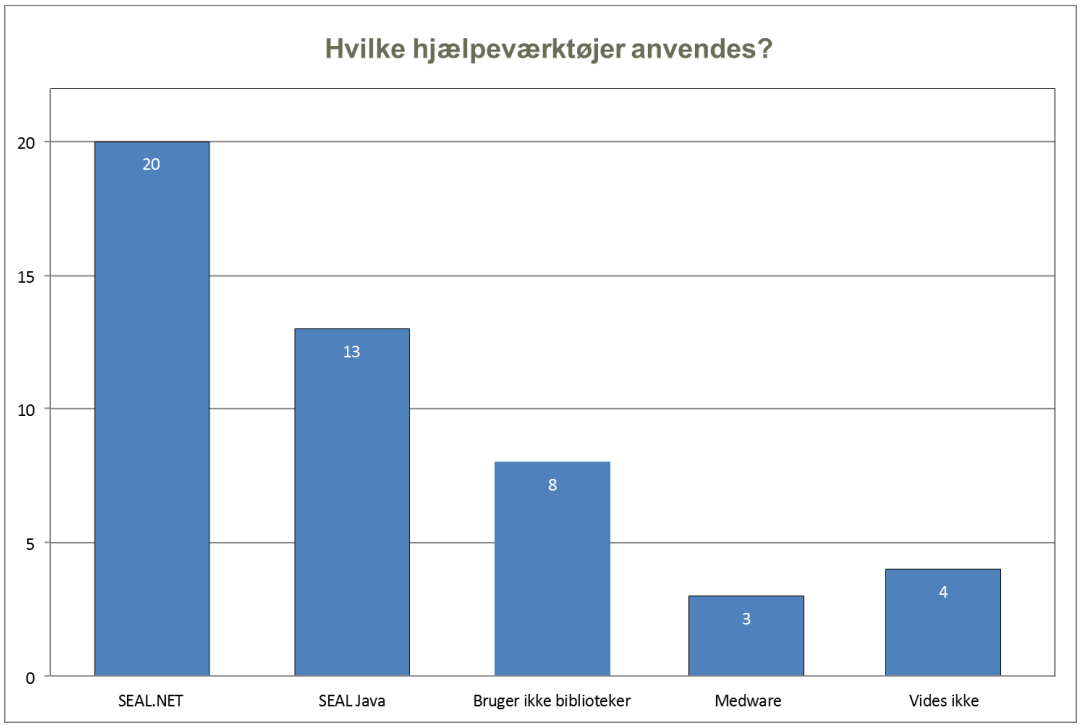
Som det ses, udvikler langt de fleste leverandører pt. deres DGWS anvendelser i enten .NET eller Java. Der er kun afdækket 4 anvendelser af DGWS uden for disse programmeringsomgivelser[20].

I forbindelse med udviklingen af DGWS, fik Medcom udviklet et .NET programmeringsbibliotek, som skulle støtte anvenderne af DGWS i nogle af de mere komplekse programmeringstekniske udfordringer i dette programmeringsomgivelse. I den sideløbende pilotafprøvning af DGWS (SOSI projektet), blev et tilsvarende programmeringsbibliotek til programmeringssproget Java udviklet. Disse går hhv. under navnene SEAL.NET og SEAL.Java. Begge er gratis, Open Source og offentligt tilgængelige på Digitaliser.dk[21]. Bibliotekerne supporteres og vedligeholdes af NSI. Foruden disse to biblioteker findes der anvendelser af et kommercielt bibliotek fra firmaet MedWare. Nedenstående diagram viser, i hvilket omfang leverandørerne gør brug af disse hjælpebiblioteker.

systemtyper, hvorfor summen er højere end de faktisk afdækkede aktører.

[20] 2 anvendelser i Delphi, 1 anvendelse i iSeries/RPG og 1 anvendelse i Intersystems Caché. Ingen af disse bruger .NET eller Java komponenter.

[21] SEAL.Java: http://digitaliser.dk/resource/2593157, SEAL.NET: http://digitaliser.dk/group/375117



Figur 40 – Anvendelse af hjælpebiblioteker[22].

Figuren viser, at der er rigtig mange aktører, der vælger at anvende de tilbudte hjælpebiblioteker.

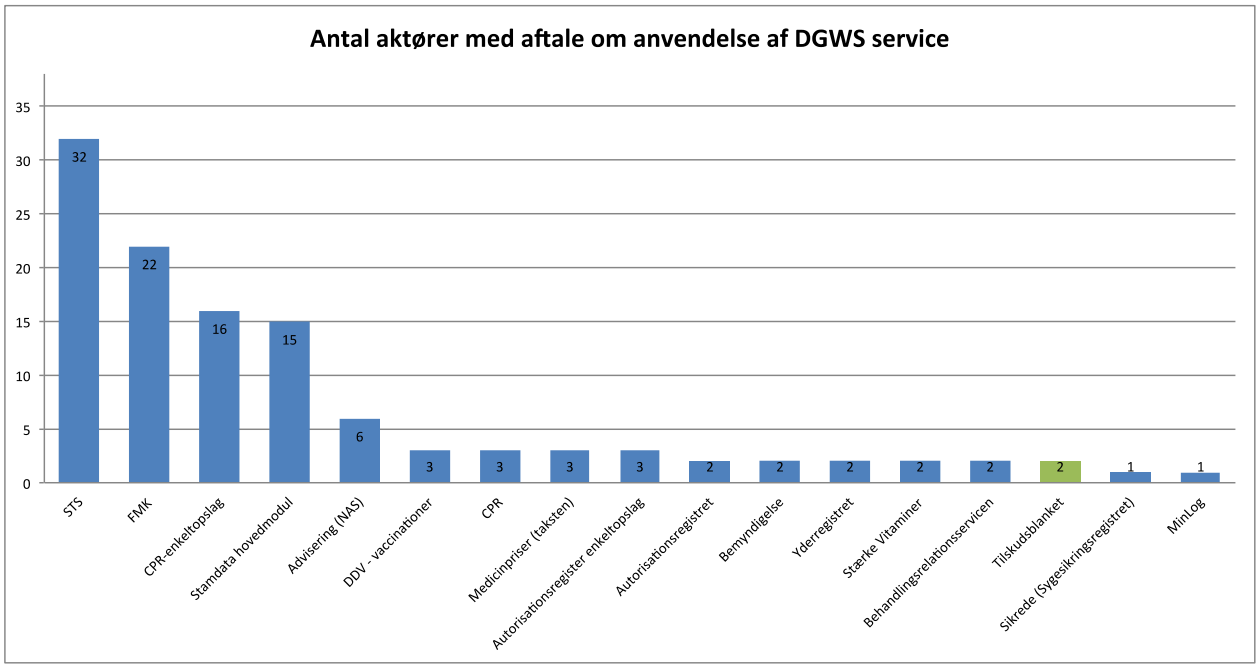
Konklusion vedrørende aktører, der anvender DGWS

- *Der er ca. 50 forskellige aktører, der anvender DGWS på sundhedsområdet.*
- *Ca. 82% af disse aktører anvender enten programmeringsomgivelserne .NET (52%) eller Java (30%).*
- *Ca. 83% af .NET udviklerne har valgt at benytte sig af SEAL.NET*
- *Ca. 93% af Java udviklerne har valgt at benytte sig af SEAL.Java*

Hvilke services udstilles?

Analysen har afdækket 18 webservices, som aktørerne enten integrerer med eller er i gang med at integrere til på NSP (på testsystemer). Anvendelsen af disse services fordeler sig som følger:

[22] Bemærk summen af leverandører i dette diagram er større end i den forrige, idet to leverandører bruger både egenudviklede DGWS biblioteker **og** et af de nationale SEAL biblioteker.



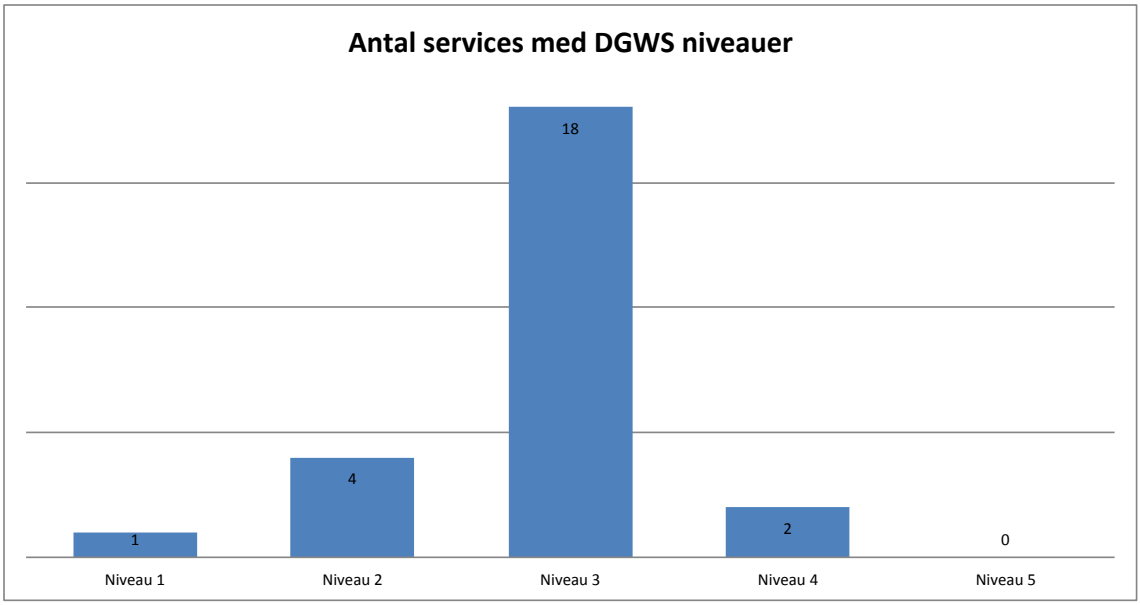
Figur 41 – Viser de 18 afdækkede web services og hvor mange aktører, der anvender hver service. De 'blå' er udviklet i Java og de 'grønne' er udviklet i .NET.

Topscoreren er naturligt nok STS servicen (autentifikation og udstedelse af sikkerhedstoken). Ud over services på NSP, udstilles også enkelte andre web services:

- Indberetning til Børnedatabasen (SSI, .NET)
- Bivirkningsindberetning (SSI, .NET)
- Dødsindberetning (SSI, .NET)
- WebReq (henvisningshotellet, MedCom, .NET)
- KommuneInformations læ-blanket service (MedCom, .NET)
- Den nationale eCPR løsning (NSI, under udvikling, Java)

Langt hovedparten af de nationale services (herunder FMK, stamdatamodulet, SOSI STS'en og øvrige NSP sikkerhedskomponenter) er udviklet i Java. Særligt STS'en og FMK løsningen må betragtes som værende kritiske i web service infrastrukturen på sundhedsområdet.

Ovenstående services anvender forskellige autentifikationsniveauer. Fordelingen af autentifikationsniveauer vises i nedenstående diagram.



Figur 42 – Fordeling af autentifikationsniveau for de udstillede services. Langt hovedparten af de nuværende services henvender sig til systemer (stamdata mv.), hvor der kræves autentifikation via system-certifikater.

I nedenstående tabel ses lidt flere informationer om hver service:

Ejer	Adgangsvej	Navn	STS	ID-kort niveau	Prg.Sprog
NSI	NSP	STS	-	-	Java + Seal
NSI	NSP	FMK	Ja	4	Java + Seal
NSI	NSP	CPR-enkeltopslag	Ja	3	Java + Seal
NSI	NSP	Stamdata hovedmodul	Ja	3	Java + Seal
NSI	NSP	Advisering (NAS)	Ja	3	Java + Seal
NSI	NSP	DDV - vaccinationer	Ja	4	Java + Seal
NSI	NSP	CPR	Ja	3	Java + Seal
NSI	NSP	Medicinpriser (taksten)	Ja	3	Java + Seal
NSI	NSP	Autorisationsregister enkeltopslag	Ja	3	Java + Seal
NSI	NSP	Autorisationsregistret	Ja	3	Java + Seal
NSI	NSP	Bemyndigelse	Ja	3	Java + Seal
NSI	NSP	Yderregistret	Ja	3	Java + Seal
NSI	NSP	Stærke Vitaminer	Ja	3	Java + Seal
NSI	NSP	Behandlingsrelationsservicen	Ja	3	Java + Seal
NSI	NSP	Tilskudsblanket	Ja	3	Java + Seal
NSI	NSP	Sikrede (Sygesikringsregistret)	Ja	3	Java + Seal
NSI	NSP	MinLog	Ja	3	Java + Seal
NSI	NSP	NSP-GW	-	-	Java + Seal
NSI	NSP	Doseringsforslag og -enheder	Ja	3	Java + Seal
NSI	NSP	Indberetning af fødselsanmeldelser	Ja	3	Java + Seal
NSI	NSP	Dokumentdelingsservice	Ja	3	Java + Seal
NSI	NSP	Samtykke	Ja	3	Java + Seal
MedCom	Direkte	Nationalt Prøvenummer service	Nej	2	.NET
MedCom	Direkte	Laboratoriesvarportalen	Nej	2	.NET + Seal
MedCom	Direkte	KommuneInformations læ-blanket service	Nej	2	.NET + Seal
MedCom	Direkte	Rekvisitionshotellet (webreq)	Nej	1	.NET + Seal
MedCom	Direkte	KIH databasen	Nej	2	Java + Seal

Konklusioner vedrørende services

- *Der udstilles pt. 27 web services, der opererer med DGWS i sundhedsvæsenet.*
- *22 af disse er tilgængelige på NSP.*
- *Hovedparten af disse services er "dataservices", der henvender sig til systemer, og hvor kravet til autentifikation er systemautentifikation (niveau 3).*
- *Pt. er det kun FMK og DDV, der anvender DGWS niveau 4 (MOCES certifikater)*
- *Der er enkelte anvendelser af DGWS, som ikke involverer udstedelse af tokens hos STS'en (niveau 1+2). Alle disse ejes af Medcom.*

Implementering af nye standarder

Hvis der skal migreres til nye standarder i sundhedsvæsenet, viser ovenstående analyse altså, at der ændres i systemer hos ca. 50 forskellige aktører. Det vil være overordentligt vanskelligt at koordinere samtidig udvikling og ibrugtagning hos så mange aktører, så en "Big Bang" implementering giver ikke mening. Der er heller ikke meget incitament hos parterne til at gøre dette på kort sigt. Mange leverandører har netop oparbejdet kompetencer i DGWS i forbindelse med FMK projektet, og vil formodentligt kun se udgifter/udfordringer i at skulle flytte til nye standarder på nuværende tidspunkt.

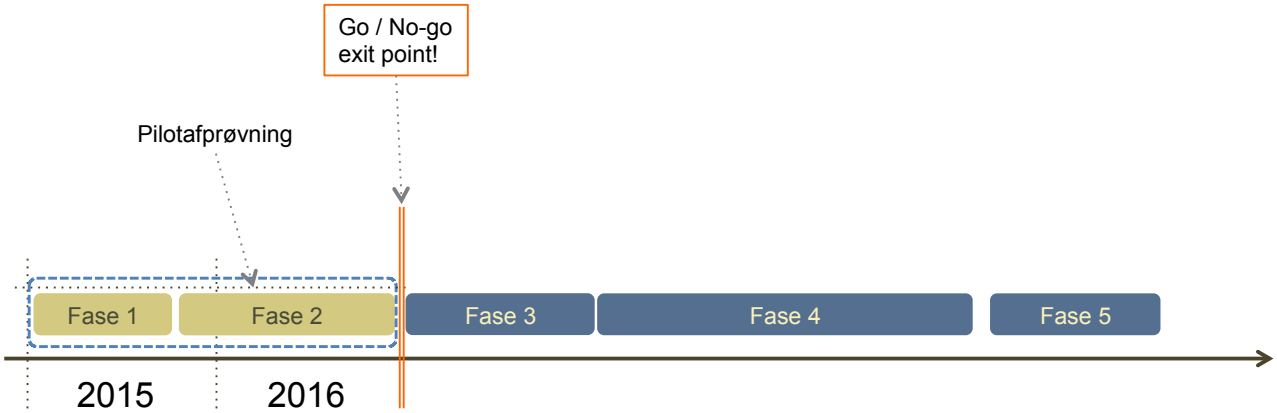
Parterne bag nærværende analyse ønsker at få belyst, hvilke gevinster og omkostninger der samlet set vil være ved at migrere til nye standarder. Af ovenstående udbredelsesanalyse ses det, at omkostningerne primært vil komme fra de mange aktørers omlægning af systemer. Ændringer i nuværende infrastruktur vil udgøre en mindre del af de forventede omkostninger i den brede migrering. Det er svært at anslå, hvor store udgifterne til den samlede migrering vil være. Grundlaget for leverandørernes estimat vil være for usikkert, da man som leverandør ikke kender beskaffenheden af den 'hjælp', der vil være at få i de kommende standarder. Der er tale om at erstatte de nuværende biblioteker med nogle referenceimplementationer og testmuligheder, hvilket ifølge leverandørerne nok vil give samme eller bedre hjælp end tidligere, men præcis hvor meget, og hvor problemstillingerne med de nye værktøjer befinder sig, kan leverandørerne ikke udtale sig om, før værktøjerne foreligger. Vælger man at fortsætte bibliotekerne, vil snitfladerne i disse ikke kunne fastholdes, da ændringerne fra nuværende til kommende standarder er relativt store, så også i dette scenarie, vil det være svært for leverandørerne at udtale sig. Er usikkerheden blot 100.000 kr. hos den enkelte leverandør (og det er endda et overordentligt konservativt bud på usikkerheden), vil usikkerheden i de samlede omkostninger ved implementeringen være +/- 5.000.000, dvs. 10.000.000 kr.

Usikkerhed i forhold til udviklingsplaner for de enkelte systemer er ligeledes med til at skabe usikkerhed i forhold til den samlede økonomi. Jo længere tid der bliver til en migrering, jo mere af migreringen vil kunne klares gennem den løbende modernisering og udskiftning af løsninger. Vil man omvendt gennemføre en hurtigere migrering end der kan klares ved almindelig modernisering og udskiftning, da vil det kræve ressourcer ud over, hvad der i dag er afsat til vedligeholdelse.

Der vil altid være mindre fejl, mangler eller uhensigtsmæssigheder i nyudviklede standarder og tilhørende hjælpeværktøjer. Disse 'børnesygdomme' vil manifestere sig som ændringer til standarderne, vejledningerne og snitflader i hjælpeværktøjer mv. Tid og omkostninger forbundet med den samlede implementering vil i høj grad afhænge af, hvor mange (eller få) af disse 'børnesygdomme' der vil være, inden den brede implementering iværksættes.

Derfor anbefaler nærværende analyse, at implementeringsstrategien følger en faseopdelt udrulning, hvor de første implementeringsfaser skal være (1) **udvikling** af standarderne og de tilhørende hjælpeværktøjer og sikkerhedskomponenter og (2) **pilotafprøvning** af disse i nogle få udvalgte systemer. I disse faser oprettes også de nødvendige vidensfora og de nødvendige governancetiltag. Alle nuværende services fortsætter parallelt med anvendelse af nuværende standarder (DGWS). Pilotafprøvningen har til hensigt at afprøve og kvalitetssikre standarder og løsninger, så 'børnesygdommene' ikke rammer alle aktørerne i sundhedsvæsenet i den brede implementering, men pilotafprøvningen har også til hensigt at give et bedre grundlag for estimering af de samlede omkostninger ved migreringen. Viser det sig, at omkostningerne ved implementeringen er for høje ift. de forventede gevinster, eller viser implementeringen at indebære risici, som parterne ikke kan imødegå eller acceptere, vil det være muligt at terminere implementeringen efter pilotafprøvningen – altså inden den brede implementering iværksættes og de store omkostninger indtræder. Pilotafprøvningen er således også et "Go / No-Go" exit punkt.

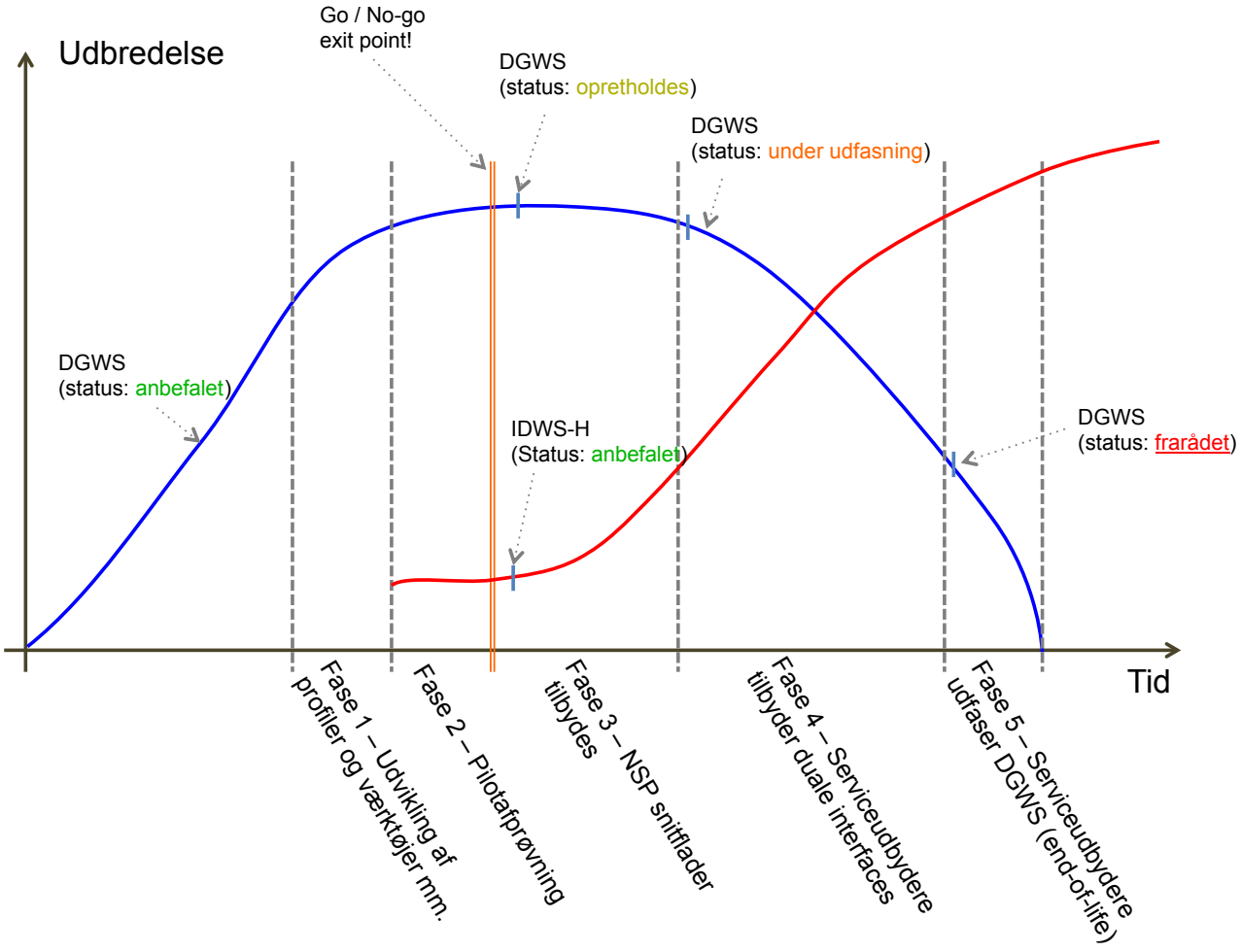
Den foreslåede faseopdelte migreringsstrategi er illustreret på nedenstående figur.



Figur 43 – Faseopdelt og gradvis implementering af de nye standarder.

I overensstemmelse med referencearkitektur for informationssikkerhed i sundhedsvæsenet, understøtter den anbefalede nye standard, at der etableres tillidsføderationer både indenfor sundhedsdomænet og imellem domæner. Disse føderationer skal baseres på et fælles "trust framework", som bør udarbejdes på fællesoffentligt regi. Denne analyse går ikke dybere ind i disse aktiviteter (se dog tabel i slutningen af dette kapitel). Dog skal der bemærkes, at gevinster, der hidrører fra etablering af føderationer, ikke vil kunne høstes inden dette "trust framework" er udarbejdet, har været i høring og er blevet ratificeret. Det forventes at disse aktiviteter i en hvis udstrækning foregår parallelt med pilotafprøvningen af de nye standarder i sundhedsvæsenet. Det forventes endvidere, at sundhedsområdet skal foretage en 'subprofilering' af dette "trust framework" til etablering af føderationer internt på sundhedsområdet.

Pilotafprøvningen bør afprøve så mange aspekter af standarden, hjælpeværktøjerne og sikkerhedsløsningerne som muligt. Derfor anbefales det, at pilotafprøvningen involverer flere leverandører, der tilsammen dækker såvel Java, .NET som rollerne web service provider og web service consumer. De involverede systemer bør også omfatte forskellige 'målgrupper', f.eks. EPJ og LPS. Et eksempel på en god pilotafprøvning kunne være FMK som serviceudbyder, to LPS leverandører (én der er på .NET platformen, én der hverken er på .NET eller Java) og en EPJ leverandør, der udvikler i Java. Pilotafprøvningen og efterfølgende faser er illustreret i nedenstående figur.



Figur 44 – Illustration af pilotafprøvning og efterfølgende udrulningsfaser.

Aktiviteter i 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**

Aktiviteter i 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**

Efter en succesfuld pilotafprøvning, vil den nye standard skifte status til 'anbefalet', mens den gamle standard skifter status til 'opretholdes'. Det betyder at alle nye services bør bruge den nye standard. I denne fase (3), som er i den første tid efter pilotafprøvningen, anbefales det at udvide alle nationale services med en nye snitflader, der overholder den nye standard, så disse altså udstiller både den nye og den gamle standard ('dualt interface'). Dette kan enten gøres på NSP, eller hos de enkelte serviceudbydere. I praksis vil dette standse udbredelsen af DGWS og sikre at den nye standard anvendes alle steder, hvor det er praktisk muligt.

Aktiviteter i fase 3	Part	Overslag (1000 kr.)
Udarbejdelse og idriftsættelse af NSP services	NSI	800
Support og vedligehold af eksisterende standarder	NSI	0[23]
I alt	**-**	**800**

I den efterfølgende fase (4) forventes det dels at leverandørerne af egen kraft ønsker at overgå til de nye standarder, for at høste kompetencekonsolideringsgevinsterne, dels at kunderne enten i kraft af mulighederne i eksisterende vedligeholdelseskontrakter, eller i kraft af tilskud til leverandøren, begynder at omlægge flere af anvendersystemerne til den nye standard. Når omkostningerne til den tilbageværende anvendelse af DGWS overstiger omkostningerne til omlægning af de resterende systemer, bør parterne i sundhedsvæsenet skifte status på DGWS til "frarådet", og sikre at de resterende systemer omlægges på relativ kort tid (fase 5).

Det periodemæssige omfang af fase 4 og 5 er svært at anslå, da det dels afhænger af de muligheder, der ligger i de nuværende systemers vedligeholdelseskontrakter, og dels af partenes fokus på omstilling. Det anslås at merudgiften til vedligeholdelse af de centrale komponenter kun udgør ca. 0,5 mill. kr. per år, mens de samlede merudgifter til forøgede vedligeholdelsesomkostninger til services med duale interfaces forventes at være noget højere (samlet set).

[23] Forventes dækket af eksisterende budgetter.

Anbefalinger vedrørende migreringsstrategi og roadmap

- *Det anbefales at implementere den nye standard gennem en faseopdelt gradvis migrering. De første faser anbefales at være forberedelse til og gennemførelse af en pilotafprøvning af den nye standard og alle de omgivende værktøjer og organiseringer.*
- *Det anbefales at anvende erfaringer fra pilotafprøvningen til senere at give et estimat på de samlede omkostninger til migrering af alle systemer til de nye standarder.*
- *Det anbefales at bruge dette estimat, og øvrige erfaringer f.eks. vedrørende observerede risici i pilotafprøvningen, til at udfærdige en businesscase for den samlede implementering. Viser business casen sig at være for ringe, kan parterne i sundhedsdomænet terminere implementeringen efter pilotafprøvningen (exit point).*
- *Det anbefales at operere med 'duale interfaces' i en periode (fase 3-5), indtil alle systemer er migreret til den nye standard.*
- *Det anbefales at parterne monitorerer de faktiske omkostninger til opretholdelse af systemer, der kun understøtter de gamle standarder. Når disse overstiger de forventelige omkostninger til omlægning af disse systemer, bør fase 5 (restimplementering/udfasning) iværksættes.*
- *Forud for og delvist parallelt med fase 1+2 skal der iværksættes aktiviteter til udarbejdelse af strategi og referencearkitektur for brugerstyring, samt "trust frameworks" i fællesoffentligt regi.*
- *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 fællesoffentlig referencearkitektur for brugerstyring.*

Nedenfor listes de aktiviteter, som Digitaliseringsstyrelsen bør iværksætte parallelt med pilotafprøvningen på sundhedsområdet. **Bemærk:** der er to aktiviteter, som pilotafprøvningen afhænger af.

Aktiviteter hos Digitaliseringsstyrelsen	Afhængigheder
Opdatering af OIOIDWS, vedligeholdelse af referenceimplementationer, oprettelse/moderering af communities mv.	Dette er en forudsætning for pilotafprøvningens fase 1
Udarbejdelse af strategi for brugerstyring på tværs af domæner	
Udarbejdelse af referencearkitektur for brugerstyring på tværs af domæner, indeholdende bl.a. borgervendt kommunikation på mobile enheder	
Afklaring af behov for fællesoffentlig løsning vedr. ”sikker browseropstart”	
Udarbejdelse af fællesoffentligt ”trust framework”	Dette er en forudsætning for pilotafprøvningens 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 nærværende tabel er gennemført. Såfremt denne fællesoffentlige pilot involverer sundhedsområdet vil det være hensigtsmæssige at pilotafprøvningen på sundhedsområdet er gennemført først.

Appendiks 1: Kommissorium for analyse vedr. sikkerhedsstandarder og –løsninger

Baggrund

Som led i den nationale strategi for digitalisering af sundhedsvæsenet er det aftalt at parterne inden udgangen af 1. kvartal 2014 gennemfører en analyse af gevinster og omkostninger ved at samordne sikkerhedsstandarder og sikkerhedsløsninger i sundhedsvæsenet med det øvrige fællesoffentlige samarbejde.

Der gennemføres en analyse med henblik på at udpege områder, der med fordel vil kunne dækkes af fælles sikkerhedsstandarder og sikkerhedsløsninger, og analysen skal pege på, hvad der skal til for at realisere sådanne fælles standarder og løsninger.

Formål

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).

Indhold

Analysen skal som minimum dække følgende:

- Kortlægning af eksisterende fællesoffentlige standarder og deres anvendelse, herunder beskrive hvorledes domænespecifikke informationer (f.eks. oplysninger om sundhedsfaglig autorisation og uddannelse indenfor sundhedsdomænet) allerede er indarbejdet, eller vil kunne indarbejdes, i standarderne.
- Identifikation af arkitektur, standarder og løsninger indenfor specifikke domæner (f.eks. på sundhedsområdet, indenfor sags- og dokumentområdet eller det kommunale område), der med fordel vil kunne anvendes på tværs af domæner.
- Kortlægning af de væsentligste browserløsninger (web applikationer) og it-tjenester (web services), med henblik på. At vurdere, hvor stor opgaven er med at omlægge disse til fælles standarder samt vurdere hvilke gevinster og omkostninger en sådan omlægning vil have.

- Kortlægning af de væsentligste infrastrukturkomponenter (brugerkataloger, sign-on løsninger, fuldmagtsløsninger etc.) med henblik på. At vurdere gevinster og omkostninger ved at migrere disse til fælles standarder samt gevinster og omkostninger ved at erstatte løsningerne med fælles løsninger. Endelig skal gevinster og omkostninger ved eventuel fælles drift vurderes.
- Beskrivelse af i hvilket omfang, der er værktøjsunderstøttelse af de identificerede og kortlagte standarder og hvilken support, der er etableret omkring arkitektur, standarder, værktøjer og infrastrukturkomponenter.
- Anbefalinger i forhold til fremtidig anvendelse af standarder og sikkerhedsløsninger, herunder at beskrive gevinster, omkostninger og risici baseret på vurdering af implementeringsmæssige, supportmæssige, driftsmæssige og brugsmæssige konsekvenser.
- Overvejelser i forhold til mulig migreringsvej. Skitsering af roadmap for gennemførelse af anbefalinger og overslag over omkostninger fordelt over tid.

Organisering og økonomi

Der nedsættes en styregruppe, bestående af Digitaliseringsstyrelsen, NSI (formand), Danske Regioner og KL. Ved arbejdets gennemførelse skal det rådgivende udvalg vedr. standarder og it-arkitektur inddrages, Styregruppen kan suppleres med yderligere deltagere efter behov.

Appendiks 2: Teknisk bilag til kommissorium

Afhængigheder til andre initiativer og projekter
Analysen koordineres med arbejdsgrupper nedsat under "Det rådgivende udvalg for Standarder og arkitektur" (RUSA), bl.a. som opfølgning på behandling og publicering af Referencearkitektur for informationssikkerhed. Denne analyse kan enten give input til nedsatte grupper (f.eks. vedr. rammeværk som Kantara IAF eller standardisering af arbejdsmæssig funktion og relation til den Fællesoffentlige Opgave Reference Model, FORM) eller ved at nedsatte arbejdsgrupper giver input til analysen (eksempelvis vedr. begrebssystem for informationssikkerhed). Relationen til den enkelte arbejdsgruppe aftales ved starten af analysen.

Resultater af denne analyse bidrager til " Foranalyse til modernisering af den fællesoffentlige it-arkitektur til datadeling" igangsat at Digitaliseringsstyrelsen, og Digitaliseringsstyrelsens foranalyse kan bidrage med input til denne analyse. Den nærmere arbejdsdeling aftales ved analysens start.

Resultater af denne analyse (f.eks. vurderinger af standarder og løsninger) kan give input til "Analyse af digital understøttelse af relevante arbejdsgange på tværs af sundhedsvæsenet", der bl.a. undersøger, hvordan der kan ske en teknologisk fremtidssikring af MedCom-kommunikationen.

Endelig leverer analysen input til referencearkitektur for nationale tjenester (efteråret 2013) og til en revision af referencearkitektur for informationssikkerhed (efteråret 2014).

Uddybning af analysens indhold

Indledende arbejde
Indledningsvis skal der ske en afgrænsning af hvilke standarder og løsninger, der er genstand for analysen. Fokus er fælles løsninger, hvorfor kandidater skal findes blandt statslige, interregionale og fælleskommunale standarder og løsninger.
Analysen bør også forholde sig til påtænkte standarder og løsninger. Der bør derfor indledningsvis ske en kortlægning af udviklingsplaner, roadmaps m.v.
I det omfang det er muligt, bør analysen baseres på resultater af allerede gennemførte analyser af enkelte standarder og løsninger. Der vil ske en kortlægning af disse.

Arkitektoniske overvejelser
Målbilleder i forhold til en fremtidig sammenhængende sikkerhedsarkitektur (med mulighed for single sign-on) drøftes. Specifikt behandles spørgsmålet om "trust" relationer, herunder i hvilket omfang det vil være fordelagtigt at etablere en eller flere "trust" føderationer baseret på fællesoffentlige standarder. Analysen bør forholde sig til anbefalingerne i den udarbejdede referencearkitektur for informationssikkerhed på sundhedsområdet og mulighederne for at der fastlægges en referencearkitektur på tværs af domæner.

Analyse af standarder
Standarder skal så vidt muligt være forenelige med fælleseuropæiske standarder anvendt i det fælleseuropæiske e-SENS projekt24, der videreudvikler og konsoliderer løsninger fra de såkaldte "Large Scale Pilots" STORK, SPOCS, PEPPOL, EpSOS og e-CODEX. Generelt bør det tilstræbes, at fællesoffentlige standarder er nationale konkretiseringer / profileringer af internationale standarder, og at sundhedsområde-specifikke standarder er profileringer af fællesoffentlige og internationale standarder.

Forud for analysen af sikkerhedsstandarder fastlægges de kriterier, som standarderne ønskes vurderet efter. Der tages udgangspunkt i det europæiske rammeværk: Common Assessment Method for Standards and Specifications (CAMSS) fra EU og vil bl.a. dække aspekter vedr. relevans, lovkrav, sammenhæng med andre standarder, anvendelighed, modenhed, åbenhed, ophavsrettigheder, markedsdækning og strategisk potentiale. Endvidere vurderes, hvilken support og governance der er etableret omkring de enkelte standarder.

Analyse af sikkerhedsløsninger
Som grundlæggende præmis skal analysen tage afsæt i, at anvendelses- ,funktionalitets- og kvalitetsmål ikke må forringes, herunder sundhedsvæsnets behov for stabil drift 24 timer i døgnet, 7 dage om ugen. De mere præcise krav til anvendelse, funktionalitet og kvalitet af de enkelte løsninger beskrives i analysen.

Såfremt driftsstabilitet og performance tilsiger det, skal fælles løsninger kunne drives såvel i en fællesoffentlig infrastruktur som i den af sundhedsområdet etablerede infrastruktur (sundhedsdatanettet, den nationale serviceplatform m.m.).

Det er vigtigt, at analysen ikke alene inddrager tekniske aspekter, men også ser på de anvendelsesmæssige, organisatoriske og økonomiske aspekter. Teknisk simple løsninger kan sagtens lede til løsninger, der kræver kompleks organisatorisk håndtering eller til løsninger, der er besværlige at håndtere for brugerne og er uforholdsmæssigt omkostningstunge. Analysen skal også beskrive, hvilken support og hvilken governance der er etableret omkring de enkelte løsninger, herunder hvordan ændringer håndteres.

Forud for analysen af sikkerhedsløsninger fastsættes præcise succeskriterier for fællesoffentlige løsninger og for løsninger anvendt på sundhedsområdet. Analysen skal herefter beskrive, i hvilket omfang de enkelte sikkerhedsløsninger lever op til de fastsatte kriterier – eller hvad der skal til for at bringe løsningerne (eller delløsninger) til dette. Der kan også opstilles specifikke succeskriterier forud for analysen af de enkelte typer af løsninger (f.eks. at brugerrettighedsstyringsløsninger skal kunne håndtere flere ansættelsesforhold for den samme bruger).

Anbefalinger
Analysen skal munde ud i en række anbefalinger vedr. ændringer (i standarder, løsninger, ejerskab, drifts- og supportorganisation, governance etc.), der med fordel kan gennemføres indenfor strategiperioden og foreslå et overordnet roadmap for gennemførelse af disse (se også nedenstående afsnit vedr. migreringsvej). Der skal foreligge et overslag over

[24] Digitaliseringsstyrelsen leder den danske deltagelse i dette projekt. De øvrige deltagere er NSI/SSI, Domstolsstyrelsen og Konkurrence- og Forbrugerstyrelsen.

omkostninger fordelt på de enkelte ændringer og en vurdering af gevinsterne ved at gennemføre det samlede roadmap. Endelig skal forudsætninger, barrierer og risici forbundet med gennemførelse af ændringerne beskrives.

Analysen kan også komme med anbefalinger af mere principiel karakter (som ikke umiddelbart leder til ændringer, der kan tids- og prisfastsættes, men som vil kræve yderligere behandling af parterne).

Anbefalinger skal som udgangspunkt følge fællesoffentlig arkitektur og standarder samt arkitektur og standarder på sundhedsområdet. Såfremt der for enkelte løsninger ønskes afvigelse herfra, skal der redegøres for sådanne afvigelser m.h.p. evt. dispensation fra gældende standarder eller m.h.p. justering af gældende standarder.

Analyse af migreringsvej

Analysen skal være helhedsorienteret og dække alle aspekter af en evt. migrering, fra udvikling over implementering til drift, support og vedligeholdelse. Det er vigtigt, at der – såfremt der ønskes en migrering – skabes en migreringsvej fra nuværende løsninger, som sikrer, at en migrering kan gennemføres i en hensigtsmæssig takt. Det bør således vurderes, hvilke migreringer, der skal gennemføres for at nye løsninger ikke skal tilpasses sikkerhedsstandarder og sikkerhedsløsninger, som man er på vej væk fra. Omvendt kan der være eksisterende løsninger, der står overfor en snarlig udskiftning, og hvor det således ikke kan betale sig at tilpasse disse til nye sikkerhedsstandarder og sikkerhedsløsninger.

Appendiks 3: Metode for afdækning af udbredelse af nuværende standard

Afdækningen af den nuværende udbredelse af DGWS har taget udgangspunkt i følgende kilder:

- **FMK programmet**s viden om anvendere af FMK
    - **Deltagere på teknikermøder.** FMK afholder jævnligt teknikermøder, hvor alle aktører, der anvender/udstiller services ifm. FMK er inviteret. Listen over deltagere kan rekvireres ved henvendelse til FMK programmet.
    - **FMK Whitelists** (testmiljøer og produktion). FMK programmet vedligeholder en liste over leverandører/aktører med teknisk adgang til FMK. Listen består af systemer, der enten allerede er certificeret til at anvende FMK (produktionsmiljøet) eller planlægger at anvende FMK (testmiljøerne). Denne liste kan anvendes til at krydschecke om alle FMK aktører blev afdækket gennem deltagerne i teknikermødet, og giver også et bud på hvilke systemer, der er involveret (systemnavne).
    - **Fælles NSP testmiljøer.** Etablering og ibrugtagning af de fælles NSP testmiljøer blev først og fremmest drevet af FMK programmets behov for disse. I den forbindelse blev der udarbejdet en liste over relevante aktører, som blev anvendt i den initielle interessenthåndtering og support af FMK.

- **NSP-operatøren**
    - **Logudtræk**. Gennem NSP operatøren blev der bestilt et logudtræk fra NSP (anvendelse af specifikke services: STS, DCC og stamdataservices). Denne giver et bud på hvilke services der anvendes, hvem der anvender dem og omfanget af anvendelsen (antal transaktioner)
    - **NSP Whitelists**. I lighed med FMK opretholdes der også teknisk adgangskontrol til NSP services pba. Indgåede aftaler om anvendelse af NSP services. Disse anvendes til at krydschecke aktørerne i ovennævnte logudtræk. Whiteliste i såvel produktions- som testmiljøerne er blevet anvendt.

- **Interviews med vidanspersoner** i NSI regi
    - Programmørerne bag SEAL.NET og SEAL.Java er blevet interviewet. Disse personer yder 2. level support og kender derfor mange af parterne på sundhedsområdet, der bruger DGWS også de parter som ikke findes i loggen på NSP (de services, der

- Interviews med **øvrige vidanspersoner**
    - Region Syddanmark. Region Syddanmark anvender DGWS internt til CPR opslag. Denne anvendelse er Regionen blevet interviewet omkring.
    - Sundhedsstyrelsen (SEI). Sundhedsstyrelsen udstiller enkelte web services, der overholder DGWS.
    - Sundhed.dk (udstilling og integration udenom NSP). Sundhed.dk udstiller en enkelt service i relation til "sikker browseropstart".
    - MedCom udstiller en række services i relation til telemedicin og databanker.

Kilder, anvendere og videnspersoner er registreret med kontaktoplysninger og fremgår af [Bilag Q – DGWS regneark]. Her findes også de data, som er udtrukket fra logs og i øvrigt opsamlet fra kilderne. Regnearket ligger til grund for graferne omkring DGWS udbredelsen i nærværende rapport.

En række aktører har alene registreret DGWS anvendelse i test, idet den nationale udrulning af FMK også dækker apotekersystemerne samt mindre segmenter som f.eks. tandlægesystemer, bostedssystemer og systemer til psykiatri. Disse er medregnet i analysen som var de i produktion, idet anvendelsen af DGWS i produktionssammenhæng er nært forestående, og impact på disse aktører vurderes at være i samme størrelsesorden som hvis de allerede var i produktion.

Appendiks 4: Uhensigtsmæssigheder og begrænsninger ved DGWS

Indledning

Siden 2006 har Den Gode Web Service (DGWS) været anvendt som standard for identitets-baserede webservices i det danske sundhedsvæsen. Gennem årene er det blevet identificeret en række mangler og uhensigtsmæssigheder ved standarden både i forhold til sikkerhed, compliance med andre standarder, samspil med andre standarder og praktisk anvendelighed. Disse uhensigtsmæssigheder opsummeres i dette appendiks og konsekvenserne af de enkle mangler afdækkes.
Henvender sig til arkitekter og teknikere, forudsætter et vis kendskab til SOAP, SAML, WS-Trust

Afgrænsninger

Nedenfor beskriver DGWS version 1.0.1 som er den af NSI anbefalede og bredt anvendte udgave af standarden.

Af forskellige parter er der gennem årene rejst kritik af DGWS som i bund og grund ikke har meget med selve standarden at gøre, men mest med besværligheder omkring anvendelsen af digital signatur, og er derfor udeladt her.

Compliance til standarder og relation til andre standarder

Autentifikationsniveau svarer ikke til gængse klassifikationer (eks. NIST assurance levels).

DGWS 1.0.1 opererer med 5 sikkerhedsniveauer, der ikke alene beskriver autentifikationsniveau, men også inkluderer aspekter som forskellige subjekt typer og uafviselighed.

Manglende overholdelse af SAML2 standarden

DGWS afviger fra SAML2 standarden på følgende tre punkter. I DGWS har:

1. <saml:Assertion> elementet et 'id' i sted for et 'ID' attribut
2. <saml:AttributeStatement> elementet et 'id' attribut som ikke er tilladt
3. <saml:SubjectConfirmation> elementet et <saml:ConfirmationMethod> subelement i sted for et 'Method' attribut

Som konsekvens heraf kan standard SAML2 rammeværk ikke umiddelbart anvendes.

Bundet til SOAP 1.1

Standarden bygger udelukkende på SOAP 1.1 og kan derfor ikke benyttes sammen med standarder som operer med SOAP 1.2 (eksempelvis 'WS for IHE transactions'). Der er valgt en egen SOAP-binding frem for at følge WS-I Simple Soap Binding Profile 1.0 (hvilket havde været det naturlige valg sammen med WS-I Basic profile 1.1).

Hård binding til hash algoritme

XMLDSig (XML Signature Syntax and Processing) standarden som DGWS bygger på er gennem RFC 4051 blevet udvidet til at tillade flere hash algoritmer i 2005, DGWS understøtter derimod udelukkende SHA-1 algoritmen til beregning af digest. 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.

Standarden uklar på nogle punkter

Der er enkelte mindre forskelle mellem eksemplerne og 'enumerationslisterne' angivet i DGWS, som har givet anledning til forskellige fortolkningsmuligheder. I praksis er det Seal bibliotekerne som de facto fastlægger fortolkningen af standarden.

DGWS specificerer ikke protokol for udstedelse af tokens

Specifikationen (DGWS 1.0.1) indeholder intet om protokol for autentifikation eller for omveksling af tokens. Her må man følge de konkrete snitfladespecifikationer til SOSI-STS. DGWS 1.1 indeholder specifikation af autentifikationsprotokol (baseret på WS-Trust), men mangler specifikation af andre tokenvekslinger.

Specifikationen forholder sig ikke til store beskeder

DGWS forholder sig ikke pt. til MTOM+XOP (krav til WS for IHE transactions). Der er dog ikke noget i DGWS der forhindrer anvendelsen af disse profiler.

Generelle mangler og uhensigtsmæssigheder

Sammenblanding af identifikationsinformationer og kontekstinformationer

DGWS definerer et såkaldt SOSI ID-Kort, som det token, der kommunikeres ift. viden om subject. ID-kortet indeholder dels en række informationer om brugeren (navne, CPR nummer etc.) men også informationer om arbejdssted (f.eks. afdeling på et sygehus). Grænsen for, hvornår disse informationer går fra at være subject-information til at være kontekstinformation er flydende, og hvis man definerer arbejdssteds-attributten til at indeholde meget fingranuleret information, vil det kræve nyudstedelse af ID-kort relativt ofte.

Derudover er indholdet af ID-kort tokenet defineret meget rigidt, så der ikke kan tilføjes felter. De informationer, der oprindeligt blev defineret til at kunne medsendes i ID-kortet, har vist sig at være utilstrækkelige, hvilket har medført at forskellige projekter har måttet definere yderligere kontekstattributter 'ved siden af' ID-kortet.

Mangelende udvidelsesmuligheder for attributter

Som ovenfor nævnt er DGWS ret "fastlåst" ift. den tilladte mængde af attributter. Mængden af attributter i et ID-kort kan ikke udvides, men nogle af attributterne er optionelle og kan derfor udelades. Dette har dog vist sig ikke at være tilstrækkeligt, hvorfor nogle af de ikke-anvendte attributter er blevet misbrugt til at kommunikere andre attributter (f.eks. sundhedsfaglig uddannelseskode) eller eksisterende er blevet omdefineret til at kunne indeholde mange forskellige værdisæt.

Relationsbegrebet ikke understøttet

DGWS nuværende attributsæt understøtter ikke relationsattributter, f.eks. vedr. behandlingsrelation, positivt eller negativt samtykke, delegering mv.

Separation af system og medarbejder informationer

DGWS opererer med både system ID-kort og bruger ID-kort. Bruger ID-kort er en udvidelse af et system ID-kort. I princippet betyder det, at brugeren ved "systemskifte" skal have nyt ID-kort, hvilket ikke er praktisk i en arbejdsdag.

Disse informationer skal hellere kommunikeres i et token, der er mere dynamisk (f.eks. som vekslede tokens i IDWS).

Manglende borger-profil (borger ID-kort)

Der er udelukkende defineret profiler for henholdsvis medarbejdere og systemer i DGWS, hvilket medfører af standarden ikke kan bruges til borger-løsninger, eksempelvis sundhedsjournalen, hvorigennem der kan vises patientens egne data hentet fra Fælles medicinkort (FMK) eller Klinisk Integreret Hjemmemonitorering (KIH).

Ingen profil for multiple assertions

DGWS understøtter ikke flere tokens fra samme eller forskellige SAML autoriteter. Det kunne f.eks. være fordelagtigt både at have informationer om bruger subject *og* system/virksomheds subject i samme besked, eller som ovenfor nævnt at have dynamiske kontekstinformationer i selvstændige eller vekslede tokens.

Sammenblanding af autentifikationsniveau og typer af principals

DGWS forholder sig én-dimensionalt til forskellige (og uafhængige) sikkerhedsaspekter, hvilket er meget uhensigtsmæssigt. F.eks. sondres der mellem niveau 3 og niveau 4, hvor der reelt er tale om samme sikkerhedsniveau men for forskellige subject typer (principals). Niveau 3 er System ID-kort udstedt på baggrund af FOCES eller VOCES certifikater. Niveau 4 er Bruger ID-kort udstedt på baggrund af MOCES certifikater. Niveau 5 er en sammenblanding af autentifikationsniveau og uafviselighed.

Services, vil i dag give adgang til data, hvis der kan præsenteres et tilstrækkeligt højt sikkerhedsniveau i ID-kortet, men dette betyder også, at en bruger (niveau 4) kan få adgang til en service, der egentlig er tiltænkt et system (niveau 3).
Subject type, autentifikationsniveau (LoA) og uafviselighed er uafhængige dimensioner, hvilket bør udtrykkes i en kommende standard.

Ikke muligt at angive om informationer er verificerede

DGWS profilerer ikke muligheden for at kunne udtale sig om STS'ens verifikationsstatus på forskellige attributter. Det efterlader ikke andre valg for STS'en end at fejle, hvis nogle af de bagvedliggende attribute-services skulle vise sig at være utilgængelige.

Tilsvarende levner det ikke mulighed for STS'en at kommunikere at en attribut er "selvdeklareret" (hvis aftagersystemet reelt er attribut-autoritet).

Kvalificering/deklarering af attributter vha. OID'er / URI

Det er i DGWS profilen ikke mulighed for at indsætte OID'er eller URI'er som kan pege på, hvorledes den enkelte attribut skal fortolkes. Nye fortolkninger eller værdisæt vil således kræve ny udgave af profilen, hvilket er uhensigtsmæssigt.

Token veksling ikke del af DGWS

DGWS forholder sig ikke til veksling af tokens. ID-kortet er et "one off" token som således både agerer som bootstrap token og service token.

Sikkerhedsudfordringer

Mangel på message integrity

DGWS understøtter kun message integrity (signatur på hele beskeden) med brugerens signatur (primært for at opnå uafviselighed) og kun på niveau 5. Message integrity handler mere om sikring af integritet af beskeden (ikke uafviselighed) gennem systemsignering.

I fremtiden vil det være mere fordelagtigt at have begge muligheder som uafhængige dimensioner af autentifikationsniveau.

Med message integrity opstår der nogle særlige problemstillinger ift. streaming af beskeder. DGWS er velegnet til streaming, da aftagere, proxies, gateways eller lignende kan nøjes med at parse SOAP headeren (eller dele af SOAP headeren) for at kunne adgangskontrollere.

Implicit trust til kaldte serviceudbydere

Som ovenfor nævnt sikrer DGWS ikke message integrity, og kræver således et sikret net (sundhedsdatanettet) og relativt ikke-reguleret "trust" inden for de sundheds-parter, der udstiller SOSI services på sundhedsdatanettet. En medarbejder (og medarbejderens arbejdsgiver), har dermed (mere eller mindre implicit) tillid til alle serviceudbydere, og at de ikke misbruger et opsnappet/logget ID-kort til at kalde andre services i brugerens navn uden brugerens viden om dette.

En bruger har ikke i den nuværende infrastruktur (nem) mulighed for at se, hvad et ID-kort er blevet brugt til.

Ingen audience restriction og ingen mulighed for at binde token til serviceaftager

I DGWS er det ikke muligt at angive *'audience restriction'* og dermed binde tokens til bestemte services, serviceudbydere eller del-føderationer. Dette forstærker igen ovennævnte misbrugsmuligheder.

DGWS understøtter ikke krypterede tokens

DGWS understøtter ikke krypterede tokens, og således ikke end-2-end fortrolighed. Dette har blandt andet vist sig at være et problem i forbindelse med sikker browseropstart, hvor tokens bliver tilgængelige for klienter og kommunikeres over et klient-netværk (og ikke bare i et lukket serversegment).

I den første version af "sikker browseropstart" (SBO1) blev et ID-kort blev kommunikeret som en URL parameter. Her var det nødvendig at udarbejde et komprimeret og krypteret ID-kort format (som altså ikke findes i DGWS). I anden version af "sikker browseropstart" (SBO2) blev ID-kortet vekslet til et krypteret OIO token.

Manglende sessions-styring/log-out mulighed

DGWS og de omgivende sikkerhedsinfrastrukturkomponenter gør det ikke muligt at "logge ud" af føderationen. Log-out sker først implicit når ID-kortet udløber i tid (24 timer). Det forstærker ovennævnte misbrugsmuligheder.

Praktiske udfordringer

Idempotente service kald

Standarden kræver at alle service kald er idempotente, konkret skal en serviceudbyder som modtager et kald med en 'MessageID' som er blevet modtaget før sende præcis samme svar tilbage uden at behandle kaldet. Dette en stor byrde for service-udbydere som i princippet skal opbevare samtlige svar de nogensinde har sendt. I praksis har f.eks. FMK begrænset sig til at kunne gensende service-svar en periode tilbage i tiden – andre serviceudbydere har undladt at leve op til dette krav.

Snæver binding af rækkefølgen af SOAP headere

DGWS tillader ikke andre SOAP headere foran dem den selv specificerer, hvilket gør standarden besværligt at arbejde med idet det praktisk kan være vanskeligt at styre rækkefølgen af headere i forskellige webservice frameworks.

Kun biblioteksunderstøttelse af DGWS på Java og .Net

Med en .Net og en Java udgave kan Seal bibliotekerne anvendes af de fleste aktører indenfor sundhedsvæsnet enten direkte eller indirekte ved at invokere biblioteket fra et andet programmeringsmiljø (Python, PHP, etc.), men der har været nogle enkle anvendere som har udviklet deres egne DGWS funktionalitet.

Tilsvarende må det forventes, at der fremover vil kunne være brug for at understøtte anvendelsen på mobile platforme.

Snæver profil til fejl beskeder

I DGWS er SOAP fault elementet meget snævert profileret og tillader ikke strukturerede fejlbeskeder. Enkle serviceudbydere har derfor defineret deres egene fejlstruktur som sendes som tekst og skal fortolkes af serviceaftagerene.

Begrænsning i message pattern

Standarden kræver at der altid sendes et svar og de eneste tilladte http status koder er 200 'OK' og 500 'Internal Server Error', derved er der ingen mulighed for one-way kald (f.eks. til asynkron afkobling, eller simple indberetninger som ikke kræver nogen svar) hvor en serviceudbydere kan svare med 202 'Accepted' og sende et tomt svar.

SOAP profil "overkill" ift. ikke sikkerhedskritiske services

DGWS opererer med samme web service profil uanset sikkerhedsniveau. Hvor DGWS er velegnet til at anvise, hvorledes digitale certifikater tages i brug, når der skal være høj grad af tillid til autentifikation af bruger, da er det en relativ kompleks profil at anvende til services, hvor der måske ikke er krav om autentifikation.

Standarden findes kun på dansk

DGWS findes kun i en dansk udgave, hvilket gør den svært anvendelig for ikke-danske aktører.

Appendiks 5: Spørgeskema til leverandører – opsummering af svar

Spørgsmål 1: Hvilke type løsninger leverer I?		
Answer Options	**Response Percent**	**Response Count**
EPJ	32,1%	9
LPS	25,0%	7
Laboratorie systemer	3,6%	1
Services på NSP	28,6%	8
Andre services	42,9%	12
Andet (angiv venligst)		12
answered question		28
skipped question		0

Spørgsmål 2: Hvor længe har virksomheden arbejdet indenfor området med web services indenfor sundhedsområdet?		
Answer Options	**Response Percent**	**Response Count**
Under 2 år	10,7%	3
2-5 år	14,3%	4
6-10 år	50,0%	14
Mere end 10 år	25,0%	7
answered question		28
skipped question		0

Spørgsmål 3: Hvor mange personer i jeres virksomhed har beskæftiget sig med web services på sundhedsområdet inden for de seneste 5 år?		
Answer Options	**Response Percent**	**Response Count**
1	10,7%	3
2-4	35,7%	10
4-9	25,0%	7
10 eller flere	21,4%	6
Ved ikke	7,1%	2
answered question		28
skipped question		0

Spørgsmål 4: Hvordan vurderer I jeres videns- og kompetenceniveau er i forhold til følgende standarder og løsninger?

Answer Options	Kender ikke	Lavt (Kender, men ingen detaljeret viden)	Mellem (Kendskab og nogen detailviden samt anvendelse)	Højt (Indgående kendskab og hyppig anvendelse)	Meget højt (Ekspertviden og rutineret anvendelse)	Response Count
DGWS	0	1	8	13	6	28
IDWS	12	8	4	3	1	28
IHE-WS	16	10	1	1	0	28
Evt. kommentarer						1
					answered question	**28**
					skipped question	**0**

Spørgsmål 5: Hvilke sikkerhedsstandarder bruger I konkret i jeres nuværende løsninger?

Answer Options	Anvendes ikke	Anvendes i enkelte løsninger	Anvendes i flere løsninger	Anvendes i alle (relevante) løsninger	Response Count
DGWS	0	6	7	13	26
IDWS	19	4	1	2	26
IHE-WS	23	2	0	0	25
Evt. kommentarer					2
				answered question	**26**
				skipped question	**2**

Spørgsmål 6: Har I haft behov for at læse specifikationen til DGWS?		
Answer Options	**Response Percent**	**Response Count**
Ja	96,4%	27
Nej	3,6%	1
Kommentar		0
	answered question	28
	skipped question	0

Spørgsmål 7: Hvis ja. Hvor meget hjalp den jer?		
Answer Options	**Response Percent**	**Response Count**
Gav ingen hjælp	0,0%	0
Gav lidt hjælp	23,1%	6
Gav nogen hjælp	57,7%	15
Hjalp os meget	19,2%	5
Kommentarer		4
	answered question	26
	skipped question	2

Spørgsmål 8: Hvilke gevinster ser I generelt ved standardiserede sikkerhedsløsninger? (Vælg de udsagn nedenfor, som I er mest enige i)		
Answer Options	**Response Percent**	**Response Count**
Brug af standarder gør det muligt for os at genbruge og konsolidere kompetencer	80,8%	21
Brug af standarder gør det muligt for os at minimere antallet af forskellige sikkerhedsløsninger	65,4%	17
Brug af standarder gør det muligt for os adgang til fælles vidensressourcer (communities etc.)	50,0%	13
Brug af standarder gør det muligt for os at anvende nationale og internationale frameworks	53,8%	14
Brug af standarder gør det muligt for os at imødekomme krav fra aftagerne af vores løsninger	23,1%	6
Brug af standarder giver os reelt ingen fordele (Forklar i tekstboxen nedenfor)	3,8%	1
	answered question	**26**
	skipped question	**2**

Spørgsmål 9: I hvor høj grad vil følgende udfordringer påvirke jeres arbejde med sikkerhedsstandarder?						
Answer Options	**Ingen indvirkning**	**Lille indvirkning**	**Nogen indvirkning**	**Stor indvirkning**	**Meget stor indvirkning**	**Response Count**
Utilstrækkelige standardspecifikationer	0	2	4	11	8	25
Utilstrækkelige vejledninger og dokumentation	0	1	5	8	11	25
Ingen eller utilstrækkelige eksempler på kommunikation (XML)	0	1	9	7	7	24
Ingen eller utilstrækkelige kodeeksempler i 'moderne' udviklingsrammeværk	0	2	10	7	6	25
Udfordringer med opbygning af nye skillsets ifm. Kommende nye standarder	0	6	11	5	2	24
Dårlig adgang til vidensressourcer (erfaringer fra andre, vidensfora, FAQ, kurser etc.)	1	5	8	7	4	25
Dårlig adgang til vidensopbygning (kurser, code camps mv.)	5	6	9	4	1	25
Dårlig adgang til udviklingssupport (en person, der kan ringes til)	1	5	11	5	3	25
Andet (angiv venligst)						3
					answered question	**25**
					skipped question	**3**

Spørgsmål 10: I hvor høj grad har I oplevet at det har været vanskeligt eller "usmart" at integrere de nuværende SEAL biblioteker i jeres løsninger?

Answer Options	Response Percent	Response Count
I meget høj grad	8,0%	2
I høj grad	12,0%	3
I nogen grad	20,0%	5
Ikke i væsentlig grad	32,0%	8
Slet ikke vanskeligt	12,0%	3
Har ikke været relevant	16,0%	4
answered question		25
skipped question		3

Spørgsmål 11: I hvor høj grad vil det påvirke støtten til jeres udvikling, hvis man i fremtiden vælger at afløse SEAL bibliotekerne med nogle eksempler/referenceimplementationer baseret på moderne rammeværk kombineret med nogle test-muligheder?

Answer Options	Response Percent	Response Count
Det vil være en kardinalbrøler!	4,2%	1
Det vil være usmart	12,5%	3
Det vil give nogenlunde samme muligheder og hjælp som nu	50,0%	12
Det vil give os bedre hjælp	12,5%	3
Det ville være super!	20,8%	5
Evt. kommentarer		4
answered question		24
skipped question		4

Spørgsmål 12: Har I haft behov for at konsultere programmeringsvejledeningerne til SEAL.Net? Hvis ja: Hvordan vil I vurdere kvaliteten dem?

Answer Options	Response Percent	Response Count
Har ikke brugt programmeringsvejledeningerne	50,0%	12
Dårlige	12,5%	3
Til lidt hjælp	25,0%	6
Til nogen hjælp	12,5%	3
Til stor hjælp	0,0%	0
De er glimrende!	0,0%	0
Evt. kommentarer		3
answered question		24
skipped question		4

Spørgsmål 13: Har I haft behov for at konsultere programmeringsvejledeningerne til SEAL.Java? Hvis ja - Hvordan vil I vurdere kvaliteten af dem?		
Answer Options	**Response Percent**	**Response Count**
Har ikke brugt programmeringsvejledeningerne	62,5%	15
Dårlige	4,2%	1
Til lidt hjælp	8,3%	2
Til nogen hjælp	16,7%	4
Til stor hjælp	8,3%	2
De er glimrende!	0,0%	0
Evt. kommentarer		2
	answered question	24
	skipped question	4

Spørgsmål 14: Har I været i kontakt med NSI Service Desk i relation med anvendelsen af sikkerhedsstandarderne? Hvis ja: Hvordan vurderer I kvaliteten af den hjælp, I har fået?		
Answer Options	**Response Percent**	**Response Count**
Har ikke haft kontakt med NSI Service Desk	48,0%	12
Dårlig	16,0%	4
Til lidt hjælp	4,0%	1
Til nogen hjælp	20,0%	5
Til stor hjælp	4,0%	1
Glimrende!	8,0%	2
Evt. kommentarer		2
	answered question	25
	skipped question	3

Spørgsmål 15: Har I været i kontakt med second level support for SEAL.Java? Hvis ja: Hvordan vurderer I kvaliteten af den hjælp, I har fået?		
Answer Options	**Response Percent**	**Response Count**
Har ikke haft kontakt med second level support for SEAL.Java	75,0%	18
Dårlig	0,0%	0
Til lidt hjælp	0,0%	0
Til nogen hjælp	4,2%	1
Til stor hjælp	12,5%	3
Glimrende!	8,3%	2
Evt. kommentarer		1
	answered question	24
	skipped question	4

Spørgsmål 16: Har I været i kontakt med second level support for SEAL.NET? Hvis ja: Hvordan vurderer du kvaliteten af den hjælp, I har fået?		
Answer Options	**Response Percent**	**Response Count**
Har ikke haft kontakt med second level support for SEAL.NET	80,0%	20
Dårlig	8,0%	2
Til lidt hjælp	0,0%	0
Til nogen hjælp	12,0%	3
Til stor hjælp	0,0%	0
Glimrende!	0,0%	0
Evt. kommentarer		1
	answered question	25
	skipped question	3

Spørgsmål 17: Sammenlignet med andre standarder, hvilket niveau synes I supporten og hjælpen omkring DGWS har været?		
Answer Options	**Response Percent**	**Response Count**
Har ikke noget sammenligningsgrundlag	28,0%	7
Under niveau	28,0%	7
På niveau	36,0%	9
Over niveau	8,0%	2
Angiv evt. hvad du sammenligner med		3
	answered question	25
	skipped question	3

Spørgsmål 18: Hvor vigtig finder du disse elementer understøtter jer i jeres implementering af sikkerhedsstandarder?						
Answer Options	**Ikke-relevant**	**Måske relevant**	**Relevant**	**Vigtigt**	**Super-vigtigt!**	**Response Count**
En god specifikation af standarden?	0	1	2	13	9	25
Reference-implementation (kodeeksempler) i moderne rammeværk (WCF, JAX WS)	1	3	1	12	8	25
Kørende test-klienter der kan afvikles i eget udviklingsmiljø	0	4	6	9	6	25
Kørende test-klienter der bruger fælles testmiljøer	0	3	6	10	6	25
Egentlige biblioteker (som SEAL.Java, Seal.NET)	1	6	4	10	4	25
Adgang til kurser	5	9	8	3	0	25
Adgang til erfa-møder	5	11	7	1	1	25
Adgang til code-camps	4	11	8	1	1	25
Adgang til udviklingssupport (én at ringe til...)	0	3	10	6	6	25
Evt. kommentarer eller forslag						4
					answered question	**25**
					skipped question	**3**

Spørgsmål 19: Har du kendskab til en specifikation eller standard, som I mener kunne tjene som eksemplarisk forbillede? (Angiv gerne URL i din kommentar)	
Answer Options	Response Count
	4
answered question	4
skipped question	24

Spørgsmål 20: Spørgeskemaet er anonymt, men nogle gange kan det give flere nuancer i svarene, hvis vi kender jeres identitet, eller hvis vi kan kontakte jer efterfølgende. Hvis anonymiteten ikke betyder så meget for jer, så angiv firma og kontaktinformationer i feltet nedenfor. Tusind tak for din hjælp! Dine input er meget vigtige for os og vi sætter stor pris på det!		
Answer Options	Response Percent	Response Count
Vil være anonym	41,7%	10
Står gerne til rådighed for evt. uddybning. (Angiv kontakt-info i tekstboxen nedenfor.)	58,3%	14
answered question		24
skipped question		4

Appendiks 6: Opsamling fra leverandørmøde

Erfaringsopsamling ang. Brug af OIO SAML, OIO IDWS, Den Gode Webservice, IHE XUA mm.

Deltagere:
Esben Andreas Dalsgaard (indkalder), NSI
Allan Hansen, Region Midt
Christian Jeppesen, Systematic
Henrik Sørensen, Sundhed.dk
Ricko Bøje Andersen, Sundhed.dk
Thomas Holme, sundhed.dk
Michael Christensen, Alexandra Instituttet
Christian Ernstsen (referent), Lakeside
Christian Gasser, Lakeside
Jan Riis, Lakeside
Lars Nico Høgfeldt, Odense Kommune
Lars Hausmann, Silverbullet
Martin Strandbygaard, Globeteam
Michael Bang Kjeldgaard, Digitaliseringsstyrelsen
Morten Kvistgaard, Arosii
Ulrik Skyt, Trifork

Afbud: NNIT og Region Syddanmark

4. Hvordan sikrer vi, at der træffes de rette valg ift. anvendte standarder?

- Involvere parterne i arbejdet, få talt med dem, der har behovet
    - Tænk ud over det snævre domæne, for der er interaktion på tværs af domæner (stat, kommuner, regioner, private aktører, og på tværs af fagområder)
- Brug tid på afprøvning af ideer og standarder, lav prototyper
    - Lavpraktisk, få involveret forskellige parter i en bredere kreds, hold fri af politik
    - Gør brug af eksperter, f.eks. etnografer og andre, der har professionelle holdninger
- Hold fokus på målgrupperne (væsensforskel på hvad en it-arkitekt og en udvikler bruger kræfter på at læse)
- Hold det simpelt!
- Gør det klart, om valgte standarder bruges til det, de er beregnet til
    - Lad det være en del af forarbejdet at præcisere scope
- Hold øje med hvem det er, der afsøger området (det betyder noget for hvad man synes er smart – og hvis det er en intern øvelse, ender man blot med at bekræfte egen viden og antagelser)
- Husk på at det tager rigtig lang tid at fase en standard ud, så brug kræfterne godt inden en standard vedtages!

    - Og sæt tid og kræfter af til overgangsperioden, hvor ny og gammel standard/version af standard er i spil samtidig – det koster!
- At lave særlige, danske standarder eller stærkt tilrettede versioner af internationale standarder (f.eks. sikkerhedsmodellerne) koster meget for anvenderne, idet der så ikke er standardunderstøttelse fra de gængse værktøjer af begreberne. Dette skal vejes op mod de fordele der er forbundet med brug af standarder, der passer rigtig godt til danske forhold.
- Foretag evaluering af historikken (hvor vanskeligt var det at benytte standarderne, blev de vedligeholdt, blev de taget i brug, osv osv).

- Forslag til standarder, der bør undersøges nærmere og evt. profileres:

    - OIOSAML
    - PHMR (HL7, MedCom har noget på vej?)
    - HL7-FIHR
    - KFOBS?

- Governance
    - Historik på (brugen af) standarder
    - Udfasning, eksplicit (og vedligeholdt) angivelse af tidshorisonter
    - Tænke "life-cycle" ind i overvejelserne, altså levetid for standarder (og de applikationer, der gør brug af standarderne)
    - Få talt med dem, der skal bruge standarderne
    - Hold standarderne opdaterede (f.eks. er kravet om SOAP 1.1 i DGWS 1.0.1 en begrænsning, der burde fjernes gennem modernisering af DGWS)

5. **Er kvaliteten af specifikationerne i orden?**
    - Der er et behov for et sted at aflevere forslag til forbedringer, og afløb for frustrationer, f.eks. omkring parallelle klassifikationer af identitet.
    - Måske et Change Board mht standarder?
    - Aktivt ejerskab fra NSI er nødvendigt

6. **Hvordan opleves kvaliteten af vejledninger, værktøjer og support?**
    - Det ville være rart med et samlet overblik over standarder og profileringer
    - En god ide med et dansk "resume" af internationale standarder, for ofte benytter vi kun et hjørne af meget store standarder, og man har ikke tid til at sætte sig ind i det hele, for derefter at konstatere at det kun var få sider, der var relevante.
    - Der er brug for et "TEST 0" miljø, hvor man helt uden aftaler ("bureaukrati") og tekniske forberedelser kan få hul igennem på under 1 dag
    - Vigtigt med højt niveau af professionalisme (især omkring SEAL)

7. **Hvordan sikrer vi bedst overholdelse af standarder?**
    - Community, aktiv deltagelse fra både NSI og alle parter
        - Kræver mere aktivitet fra alle end nu, hvor flere fora er inaktive eller helt lukkede ned

8. Gode råd til hvordan udviklere hjælpes videre?

- Set fra anvendersiden er standarder måske ikke så interessante, men operationelle indkapslinger og hjælpebiblioteker kan være en stor hjælp
- Kodeeksempler og testklienter hjælper rigtig meget
- "Pixi-bøger" kunne måske hjælpe helt nye udviklere, om ikke andet så til at få et hurtigt overblik, inden man går i dybden med at få tingene til at virke
- Mulighed for at downloade et "mini-testmiljø" (evt. "TEST 0") til egen maskine så man kan se alt hvad der sker og bedre fejlfinde
- Angiv eksplicit hvad der er obligatorisk, og hvad der er "best practice"

Konklusioner

- ✓ **K1 – Værdien af standarder**
  Standarder medvirker til at indsnævre spannet af løsningsmuligheder. Standarderne inkorporerer "best practice" i forhold til løsning af opgaven (f.eks. HL7's anvendelse af OID'er).
- ✓ **K2 – Værdien af standarder**
  Ved uoverensstemmelse mellem to parters design, kan en standard være nyttig til at fastslå, hvad der er gældende (autoritativ tolkning)
- ✓ **K3 – Værdien af standarder**
  En god profilering af standarder kan være med til at reducere opgaven med at sætte sig ind i bagvedliggende standarder.
- ✓ **K4 – Hold det simpelt**
  Som udgangspunkt skal de valgte standarder være "tynde" profileringer af internationale standarder/profiler. Det vil gøre profilerne mere kompatible med udviklingsværktøjer og –rammeværk, samt gøre det muligt at hente hjælp fra andre anvendelser i andre sammenhænge/lande.
- ✓ **K5 – Governance: Brug interessenterne aktivt**
  Valg af nye standarder skal ske ved inddragelse af de væsentligste interessenter (serviceudbydere, serviceanvendere, leverandører) i en anerkendelse af, at interessenternes behov (og behov for støtte) er *overordentligt* forskelligt. Der skal opdyrkes et *aktivt* og *modereret* community omkring profiler.
- ✓ **K6 – Governance: Pilotafprøvninger**
  Implementering af nye eller ændrede standarder skal ske gennem pilotafprøvninger. Pilotafprøvningerne skal ske med inddragelse af en stor del af kompetencespektret og gerne med inddragelse af flere domæner (især hvis standardens virkefelt ser ud til at være påvirket af opgaveglidning mellem domæner). **Bemærk:** Pilotafprøvning er en afprøvning af en operationel løsning (i drift) men i mindre skala. Det er *ikke* proof of concept.
- ✓ **K7 – Governance: Løbende evaluering og opfølgning**
  Sørg for at der sker løbende læring omkring anvendelsen af standarderne ved at foretage objektiv evaluering og synliggørelse af brugen. Dette skal også bruges til at identificere "lignende brug" af f.eks. attributter, så der på bagkant kan ske standardisering af dette.

- ✓ **K8 – Governance: Hold profilerne "levende":**
  Sørg for at standarder/profiler udvikler sig med forretningsbehov, jura, teknologi, opdaterede standarder, som profilerne benytter sig af etc.
- ✓ **K9 – Governance: Fokus på reel fornyelse og forandring**
  Sørg for stram styring af standardernes implementering, udbredelse og udfasning (lifecycle) og sørg for at afdække muligheder for (mere eller mindre 'automatisk') at forny eksisterende snitflader, så de udadtil ser ud som om de er renoverede. Dette vil nedbringe byrden ift. midlertidige løsninger.
- ✓ **K10 – Governance: 'Nogen' skal have ansvaret og overblikket**
  Det er vigtigt, at standarder ikke bare introduceres "tilfældigt". Kandidater skal som udgangspunkt vælges ud fra en række principper og kriterier (CAMMS) og 'nogen' skal have myndigheden til og ansvaret for at foretage fornøden analyse inden pilotafprøvning. Disse 'Nogen' skal også være kontaktpunkt for spørgsmål eller ideer, der går på tværs af profiler eller ligger på kanten af profilerne.
- ✓ **K11 – Sørg for løbende at udvide specifikationer**
  Observationer om behov for standardisering skal relativt hurtigt ind i specifikationerne.
- ✓ **K12 – Hold standarderne 'åbne'**
  Sørg for OID'er og/eller URI'er på alle attributter, så man kan finde frem til den entydige autoritative fortolkning (og udsteder). Det gør det også muligt at tilføje eller ændre i klassifikationer til allerede eksisterende attributter med minimal ændring til specifikationer og implementeringer.
- ✓ **K13 – Sørg for god sondring mellem obligatoriske, anbefalede og valgfrie informationer**
  Parterne efterspørger gode og solide beskrivelser af, hvad der **skal** anvendes, hvad der **bør** anvendes og hvad der **kan** anvendes.
- ✓ **K14 – Governance: Der skal være nogen, som 'bekymrer' sig om standarden**
  Erfaringen viser at man generelt godt ved, hvor man skal henvende sig ift. DGWS og SEAL, og det betragtes som meget værdifuldt.
- ✓ **K15 – Man skal kunne komme hurtigere i gang**
  Det skal være muligt at komme i gang med anvendelse af en ny standard i løbet af en halv dag. Kørende eksempler, testkode, testklienter og gode vejledninger. Man skal helst kunne komme i gang på egen hånd og i eget miljø (uden anvendelse af eksterne systemer og testmiljøer). NIAB (eget milø) -> Test0 (uden bureaukrati) -> Test 1 etc.).
- ✓ **K16 – Hjælpemidler skal understøtte hovedparten af anvenderne**
  Som udbyder af en standard skal man anerkende at man ikke kan hjælpe alle. Hvis man kan hjælpe 60%, så har man formodentligt fundet et passende niveau.
- ✓ **K17 – Der skal være nogen, som man kan kontakte**
  Kompetencespændet er enormt blandt sundhedsvæsenets leverandører, og derfor er det svært at specificere på en måde, så alle føler det nemt at anvende, men hvis/når der opstår problemer med fortolkning eller formulering, så skal der være nogen som man kan rette henvendelse til.
- ✓ **K18 – Det er en kunst at lave gode vejledninger**
  Der er brug for erfaringsopsamling og kvalitetssikring af vejledninger. Brug leverandørerne aktivt.
- ✓ **K19 – Standarder er i sig selv en gevinst, men den kan optimeres med en række hjælpemidler:**
  2. Vejledninger

3. Kodeeksempler
4. Kørende kodeeksempler (testklienter)
5. Biblioteker (primært for komplekse standarder som f.eks. sikkerhedsstandarder)

Det bliver først 'nemt' (og dermed forretningsmæssigt fordelagtigt), når standarderne understøttes langt ned i ovenstående liste (3-4). Gevinsten ved standardiseringen vil være afhængig af dette.

Appendiks 7: Ordliste

[TBD]

Appendiks 8: Referencer

[CFCS-trusselsvurdering]	"Trusselsvurdering: APT-angreb mod danske myndigheder, virksomheder og organisationer", 5. februar 2014	http://fe-ddis.dk/cfcs/CFCSDocuments/Trusselsvurdering%20-%20APT-angreb.pdf
[FMK dokumentation]	Det Fælles Medicinkort – dokumentation	http://digitaliser.dk/resource/2593547/artefact/fmk_1.4.2.4_dokumentation.pdf
[FMK services]	Det Fælles Medicinkort – dokumentation, services	http://digitaliser.dk/resource/2593547/artefact/fmk_1.4.2.4_dokumentation_-_services.pdf
[HSUID]	"Healthcare Service User Identification Header – Specification", v. 1.1, NSI, januar 2013.	Kan rekvireres ved henvendelse til NSI.
[InetOrgPerson]	"RFC 2798 – Definition of the inetOrgPerson LDAP Object Class", The Internet Society, 2000.	http://www.faqs.org/rfcs/rfc2798.html
[Kantara]		http://kantarainitiative.org
[Kerneattributter]	"Anbefalinger til kerneattributter for Bruger", It- og Telestyrelsen, 2006.	http://www.digst.dk/Arkitektur-og-standarder/Standardisering/Standarder-for-serviceorienteret-infrastruktur/~/media/Files/Arkitektur%20og%20standarder/Service%20orienteret%20infrastruktur/HoringBstkerneatrtibutterv5.pdf
[KOMBIT-ADGANG]	Det fælleskommunale støttesystem Adgangsstyring	http://www.kombit.dk/indhold/adgangsstyring
[KOMBIT-SP]	Den fælleskommunale serviceplatform	http://www.kombit.dk/serviceplatform
[KL-RA]	Den fælleskommunale rammearkitektur	http://www.rammearkitektur.dk
[NIST]	"Electronic Authentication Guideline", NIST 800-63-1, National Institute of Standards and Technology, December 2011.	http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
[NSI-standardkatalog]	Katalog over it-standarder på sundhedsområdet	http://www.ssi.dk/graphics/standardkatalog/2.0/index.html
[NSI-context-token]	Healthcare Context Token	Kan rekvireres ved henvendelse til

	Profile, v. 0.1, NSI, 11. Oktober 2012	NSI.
[NSTIC]	"National Strategy for Trusted Identities in Cyberspace", The White House, Washington, April 2011.	http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[OIO-AUTSIK]	"Vejledning vedrørende niveauer af autenticitetssikring", IT- og Telestyrelsen, 2005	http://digitaliser.dk/resource/363424/artefact/Horing.B.st.niv.autenticitetssikring.v5.pdf
[OIO-SAML]	"OIO Web SSO Profile V2.0.9 (also known as OIOSAML 2.0.9)", Digitaliseringsstyrelsen, 2012	http://digitaliser.dk/resource/2377872
[OIO-SAML-client-browser]	"OIOSAML Rich Client to Browser Scenario Version 1.0", Digitaliseringsstyrelsen, december 2012	http://digitaliser.dk/resource/2081228/artefact/OIOSAML+Rich+client+to+browser+scenario+1.0.pdf
[OIOSAML Att. Context]	Attribute Context, Version 0.1, IT- og Telestyrelsen,	Udkast. Ikke offentliggjort. Kan rekvireres ved henvendelse til NSI.
[ReferenceSikkerhed]	"Referencearkitektur for Informationssikkerhed", NSI, version 1.0, september 2013.	http://www.ssi.dk/Sundhedsdataogit/National%20Sundheds-it/~/media/Indhold/DK%20-%20dansk/Sundhedsdata%20og%20it/NationalSundhedsIt/Standardisering/Referencearkitektur%20for%20informationssikkerhed%20v%20%201%200%20nyt%20layout.ashx
[SDSD-bs-attrib-intro]	"Brugerstyringsattributter - Introduktion - Specificering af nye og ændrede attributter i id-kortet", v. 0.3, Digital Sundhed, 21. juni 2010	http://digitaliser.dk/resource/766250/artefact/Bilag+2.+Sammenh%c3%a6ngende+Brugeradministration+-+Brugerstyringsattributter+-+Introduktion_v_0_3.pdf [Bør erstattes af link til nuværende standardkatalog]
[SDSD-bs-attrib-indhold]	"Brugerstyringsattributter - Indhold - Specificering af nye og ændrede attributter i id-kortet", v. 0.6, Digital Sundhed, 21. juni 2010	http://digitaliser.dk/resource/766241/artefact/Bilag+3.+Sammenh%c3%a6ngende+brugeradministration+-+Brugerstyringsattributter+-+Indhold_v_0_6.pdf [Bør erstattes af link til nuværende standardkatalog]
[SDSD-bs-attrib-politik]	"Brugerstyringsattributter - Politikker - Specificering af nye og ændrede attributter i id-	http://digitaliser.dk/resource/766223/artefact/Bilag+4.+Sammenh%c3%a6ngende+brugeradministration+-+Brugerstyringsattributter+-+Politikker_v_0_6.pdf

	kortet", v. 0.6, Digital Sundhed, 21. juni 2010	[Bør erstattes af link til nuværende standardkatalog]
[SDSD-bs-attrib-ræsson]	"Brugerstyringsattributter - Ræssonnementer - Specificering af nye og ændrede attributter i id-kortet", v. 0.6, Digital Sundhed, 21. juni 2010	http://digitaliser.dk/resource/766214/artefact/Bilag+5.+Sammenh%c3%a6ngende+brugeradministration+-+Brugerstyringsattributter+-+R%c3%a6sonnementer_v_0_6.pdf [Bør erstattes af link til nuværende standardkatalog]
[SDSD-IDWS-H-overview]	"OIOIDWS for Healthcare 1.0, Overview – Common Web Service Profile for Healthcare in the Danish Public Sector", Digital Sundhed, 8. februar 2010	http://digitaliser.dk/resource/766205/artefact/Bilag+6+IDWS-H_Overview-v1.0.pdf [Bør erstattes af link til nuværende standardkatalog]
[SDSD-IDWS-H-aut-token]	"OIOIDWS for Healthcare, Token Profile for Authentication Tokens – Common Web Service Profile for Healthcare in the Danish Public Sector", version 1.0, Digital Sundhed, 8. februar 2010	http://digitaliser.dk/resource/766187/artefact/Bilag+7+IDWS-H_AuthenticationTokenProfile-v1.0.pdf [Bør erstattes af link til nuværende standardkatalog]
[SDSD-IDWS-H-identity-token]	"OIOIDWS For Healthcare, Token Profile For Identity Tokens 1.0 – Common Web Service Profile for Healthcare in the Danish Public Sector", Digital Sundhed, 8. februar 2010	http://digitaliser.dk/resource/766172/artefact/Bilag+8+IDWS-H_IdentityTokenProfile-v1.0.pdf [Bør erstattes af link til nuværende standardkatalog]
[SDSD model]	"Oplæg til en model til vurdering af modenhed og egnetheden af standarder på sundheds-it området", v. 0.6, Digital Sundhed, 28. september 2010.	Kan rekvireres ved henvendelse til NSI.
[SDSD-Sign-on-profile]	"Sign-On projektet: HL7-CCOW Context Management: A National Sign-on Profile", v. 0.9, SDSD, 8. marts 2010.	http://www.ssi.dk/graphics/standardkatalog/2.0/publication/181.pdf
[SDSD vurdering]	"Oplæg til vurdering af modenhed og egnetheden af OIO-IDWS ifht. DGWS", v. 0.1, Digital Sundhed, 25. september 2010.	Kan rekvireres ved henvendelse til NSI.
[Schac]	"SCHAC Attribute	http://www.terena.org/activities/tf-

	Definitions for Individual Data", v. 1.4.1, TERENA, 2011-07-05 (SCHAK = SCHema for Academia)	emc2/docs/schac/schac-schema-IAD-1.4.1.pdf
[SundJournalAttrib]	"Vejledning til kald af Sundhedsjournalen", Version 1.7.1, Sundhed.dk, 22. januar 2014.	http://teknik.sundhed.dk/fora/index.php?action=dlattach;topic=28.0;attach=82
[UNILogin Attr.]	UNI•Login webservice ws-04, UNI•C, November 2013	http://www.uni-c.dk/It-og-administration/Brugere-og-adgangsstyring/For-brugeradministratorer/~/media/UNIC/Filer/Publikationer/Tekniske%20vejledninger/uni-login-webservice_ws04.ashx
[WAYF Attr.]	WAYF attributliste	http://www.wayf.dk/component/content/article/112
[WS Federation]	"Web Services Federation Language (WS-Federation)", Version 1.2, OASIS Standard, 22. May 2009.	http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf

[Bilag XX – CAMSS]
[Bilag Q – DGWS regneark].