

Profil for web services i helse- og sosialsektoren

Versjon 1.2

1 Innholdsfortegnelse

1	Innholdsfortegnelse	2
2	Revisjonshistorikk.....	3
3	Innledning	4
4	Status for denne versjonen	4
4.1	<i>Forholdet til andre profiler.....</i>	<i>4</i>
4.2	<i>Forhold som er vektlagt i profilen.....</i>	<i>5</i>
5	Om web services	5
5.1	<i>Anvendte standarder</i>	<i>5</i>
6	Basisprofil	6
6.1	<i>Transport.....</i>	<i>6</i>
6.2	<i>Meldingslaget.....</i>	<i>6</i>
6.3	<i>Sikkerhet.....</i>	<i>7</i>
6.4	<i>Metadata.....</i>	<i>8</i>
6.4.1	<i>Oppslag/katalog.....</i>	<i>8</i>
6.4.2	<i>Beskrivelse av metadata for tjenester.....</i>	<i>8</i>
7	Retningslinjer for serviceutvikling - tjenestelaget.....	8
7.1	<i>”Contract first” utvikling av tjenester</i>	<i>9</i>
7.2	<i>Dokumentasjon av tjenesten.....</i>	<i>9</i>
7.3	<i>Testing av tjenester.....</i>	<i>9</i>
7.4	<i>Identifikasjon av kommunikasjonsparter</i>	<i>10</i>
8	Videreutvikling av profilen	10
9	Referanser	10

2 Revisjonshistorikk

Dato	Kommentar	Ansvarlig
03.03.2009	Oppdatert etter høring	AV

3 Innledning

Dette dokumentet beskriver en profil for bruk av web services i helse- og omsorgssektoren. Profilen er tenkt som en felles plattform for implementering av web services-baserte tjenester. Intensjonen er at plattformen skal utgjøre en felles basis av protokoller og standarder som kan benyttes for å utvikle og tilby samhandlende web services på tvers av aktører i sektoren, basert på en felles samhandlingsarkitektur¹ og nasjonale infrastrukturentjenester.

4 Status for denne versjonen

Dette er versjon 1.2, som er ment å gi et utgangspunkt for pilotering og erfaringsbygging. Profilen omfatter basis protokoller og standarder for utveksling av web service meldinger. Profilen er oppdatert etter høringsrunde i sektoren høsten 2008.

4.1 Forholdet til andre profiler

Flere aktører arbeider med profilering av standarder for web services. Internasjonalt er dette aktører som OASIS og WS-I, og innenfor helseområdet bl.a. HL7 og IHE.

Denne profilen tar utgangspunkt i disse standardene og skal så langt som mulig være kompatible med gitte versjoner av disse.

- HL7s web service profil ” HL7 Version 3 Standard: Transport Specification - Web Services Profile, Release 2” – Baserer seg på basis WS-standarder (SOAP, WS-Adressing, WS-Security osv) og beskriver hvordan disse skal benyttes for å ”pakke inn” HL7 interaksjoner (meldinger), hvordan disse skal beskrives i WSDL osv. Videre stilles det krav om at WS-I Basic Profile 1.0 skal benyttes, selv om det påpekes at HL7-profilen bryter ett av kravene i denne. Også ift. andre WS-I-profiler påpekes det unntak. HL7s profil retter seg spesifikt mot tilgjengeliggjøring av HL7-baserte tjenester, og kan derfor ikke uten videre benyttes som generell WS-profil, men det er i denne profilen tatt utgangspunkt i de generelle kravene som ikke er HL7-spesifikke. Å etablere tjenester basert på HL7-profilen innebærer å finne HL7-definerte tjenester/meldinger som skal implementeres, for så å beskrive tjenesten i WSDL iht. HL7’s krav.²
- IHEs Web Services profil (IHE ITI TF Supplement Appendix V) : IHE baserer seg i stor grad på HL7’s web services profil – men beskriver i tillegg regler for hvordan IHE-transaksjoner som ikke bygger på WS skal håndteres.

For rene HL7-løsninger eller løsningen som bygger på IHE-profiler, bør de respektive profilene benyttes. For andre løsninger bør denne profilen benyttes, som baserer seg på de samme standardene.

¹ http://www.kith.no/templates/kith_WebPage_1773.aspx

² For en god oversikt over hvordan å bygge HL7-baserte web tjenester, se: <http://msdn.microsoft.com/en-us/library/ms954603.aspx>

4.2 Forhold som er vektlagt i profilen

Profilen skal basere seg på etablerte web services-standarder i endelige utgaver. Standardene skal ha bred verktøystøtte, og være leverandørnøytrale.

I denne versjonen av profilen er det vektlagt å prioritere et begrenset antall protokoller og standarder som dekker et minimumsett av funksjonalitet for implementasjon av web services. Etter hvert som behovene for utvidet funksjonalitet øker, for eksempel innen sikkerhet, pålitelighet eller styring, bør profilen utvides.

Som en basis profil for web services er det i denne omgang heller ikke vektlagt standarder for modellering eller orkestrering.

Profilen bygger primært på WS-I profilene for web services. Flere web services tjenester bygger i dag på en arkitekturtilnærning som beskrives ved navnet REST³, som ikke benytter WS-* protokollene for å etablere tjenester, men som eksponerer *ressurser* direkte over http, og gjør det mulig å gjøre handlinger (get, put, post osv.) mot disse ressursene. En slik tilnærning anses som nyttig for en del enklere tjenester, for eksempel eksponering av registerdata eller informasjon hvor det ikke stilles store krav til sikkerhet. Flere verktøy gjør det også mulig å eksponere tjenester både over REST og SOAP, slik at disse kan kjøre parallelt. Denne profilen går ikke videre inn på en slik tilnærning.

5 Om web services

Web services anvendes for å etablere system-til-system kommunikasjon mellom konsumenter og tjenestetilbydere i en tjenesteorientert arkitektur. Web-services området er under løpende utvikling, og nye forslag til standarder kommer jevnlig, mens andre blir forlatt pga liten interesse. Av eksisterende standarder er ikke alle uten videre kompatible med hverandre.

Et sentralt element i etableringen av en tjenesteorientert arkitektur er å definere en felles teknisk plattform for kommunikasjon som tjenestene kan gjøres tilgjengelig over. Et av hovedformålene ved en slik arkitektur, fra et IT ståsted, er å gjøre det lettere å integrere systemer og endre de tekniske systemene i tråd med endringer i virksomhetsprosessene. Dette forutsetter bl.a. en teknisk plattform i bunnen bygget på felles standarder for kommunikasjon, tjenesteoppdagelse, sikkerhet og styring. Denne profilen definerer en slik plattform for bygging av web service baserte tjenester i helsesektoren.

5.1 Anvendte standarder

Internasjonale standarder

WS-I Basic Profile 1.1 – Profil for interoperabil bruk av et kjernesett av web services spesifikasjoner, slik som SOAP, WSDL and UDDI,

WS-I Basic Security Profile 1.0 – Profil for bruk av WS-Security og REL, Kerberos, SAML, UserName og X.509 security token format.

³ Se for eksempel http://en.wikipedia.org/wiki/Representational_State_Transfer

WS-Security 1.0 – Beskriver hvordan signering/kryptering og autentisering skal gjøres i web services

WSDL 1.1 - Tjenestebeskrivelser

WS-Adressing (Iht. WS-I Basic Profile 1.2) – transportnøytral adressering av tjenester

SAML – Security assertions markup language

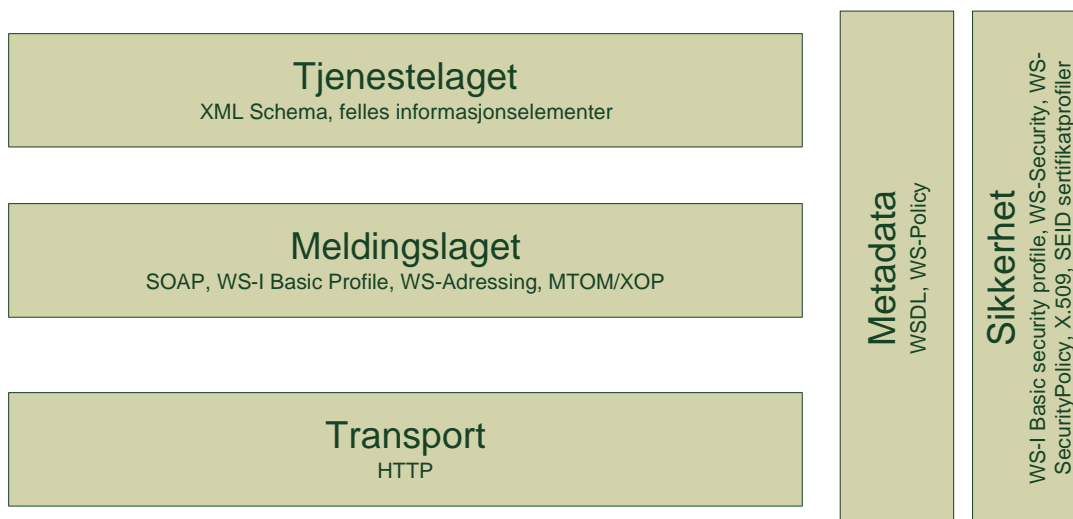
WS-Policy 1.5 – XML-basert språk for beskrivelse av tjenesters policy.

Nasjonale standarder

Kravspesifikasjon for PKI i offentlig sektor

SEID profiler for personlige sertifikater og virksomhetssertifikater

6 Basisprofil



Figur 1 - Oversikt over standarder som er med i profilen

6.1 Transport

HTTP/HTTPS er være standard transportprotokoller for web service-baserte tjenester.

6.2 Meldingslaget

”WS-I Basic Profile 1.1 Second Edition” skal være basis standard for implementasjon av web services i helsesektoren. Denne standarden omfavner andre grunnleggende standarder, som:

- SOAP: definerer meldingsstrukturen, konvolutten, for web services
- WSDL: tjenestebeskrivelser
- HTTP/HTTPS: transportprotokoll

Foruten standardene som refereres i WS-I basic profile, kan også følgende standarder benyttes:

- WS-Adressing: standardisert måte å inkludere adresseringsinformasjon for transportnøytral adressering av tjenester.

6.3 Sikkerhet

”WS-I Basic Security Profile 1.0” skal være basis standard for sikkerhet for web services i helsesektoren.

Denne standarden omfatter andre grunnleggende sikkerhetsstandarder, som:

- XML Encryption
- XML Signatures
- X.509 og username tokens

Ulike tjenester vil ha ulike sikkerhetsbehov. Det defineres derfor fire sikkerhetsnivå for autentisering mot web services:

- Usikrede tjenester: Forholder seg ikke til sikkerhetsmekanismer
- Brukernavn/passord: enkel autentisering – følger WS-I Basic Security profile 1.0 med username token, evt. SAML token basert på autentisering mot en single sign-on tjeneste basert på brukernavn/passord.
- Virksomhetsnivå: – følger WS-I Basic Security profile 1.0 med signatur basert på virksomhetssertifikat, evt SAML token basert på autentisering mot en Single-signon tjeneste signert med et virksomhetssertifikat.
- Personlig nivå: - følger WS-I Basic Security profile 1.0 med signatur basert på personlig sertifikat på nivå Person-Høyt ihht. ”Kravspesifikasjon for PKI i offentlig sektor”. Evt. SAML token basert på autentisering SAML mot en Single-signon tjeneste med sertifikat på nivå Person-Høyt.

SAML-tokens vil være aktuell å bruke for løsninger som baserer seg på føderert identitetshåndtering. SAML token må da inneholde informasjon om hvilket nivå brukeren er autentisert på (for eksempel Person-Høyt), slik at tjenesten kan gi tilgang på riktig nivå.

For sikring av konfidensialitet bør kryptert kommunikasjon over HTTPS og evt. kryptering vha. XML Encryption benyttes. Bruk av XML Encryption kan innebære utfordring ift. ytelse og bør vurderes konkret ift. behov. Retningslinjene i WS-I Basic Security profile 1.0 gjelder for kryptering på innholds nivå.

PKI-løsninger for utveksling av sensitive personopplysninger skal baseres på ”Kravspesifikasjon for PKI i offentlig sektor”. Sertifikater på virksomhetsnivå og personlige sertifikater i tråd med kravspesifikasjonen benyttes for sikring av meldingene ved utveksling av helseopplysninger.

Sertifikatene skal følge SEID-profil for personlige eller virksomhetssertifikater.

For beskrivelse av sikkerhetspolicy for tjenester bør WS-SecurityPolicy benyttes.

6.4 Metadata

6.4.1 Oppslag/katalog

På sikt må det etableres tjenester for oppdagelse (discovery) av tjenester og tjenestetilbydere med web services-baserte tjenester i helsenettet. Dagens Adressekatalog (HER) bygger på andre standarder enn de som normalt brukes for katalog for web services (UDDI). Pr. i dag må informasjon om tjenester og grensesnitt derfor utveksles på annen måte.

UDDI er mest aktuell som mekanisme for oppslagstjenester for web services. Gjennom UDDI kan tjenester publiseres og søkes opp vha et web services grensesnitt, og tjenestenes grensesnitt kan lastes ned.

Det eksisterer ingen nasjonal UDDI-katalog, og behovet for en sentral tjeneste for publisering og oppslag av web services bør vurderes.

ebXML Registry v. 3.0 bør overvåkes som fremtidig kandidat for oppslagstjeneste og lagring av tjenestebeskrivelser, skjema og annen service metadata.

6.4.2 Beskrivelse av metadata for tjenester

WS-Policy bør benyttes for å beskrive policy for tjenester og for å understøtte konfigurasjon.

7 Retningslinjer for serviceutvikling - tjenestelaget

Web services som utveksler helseopplysninger skal så langt som mulig bygge på det helsefaglige innholdet i tråd med aktuelle innholdsstandarder. I en del tilfeller kan dette innebære at WS benyttes som ren transportkanal for eksisterende meldinger, men felles medisinske innholdskomponenter bør også benyttes som basis for etablering av nye WS tjenester.

Felleskomponenter for datatyper, informasjon om organisasjoner og personer er tilgjengelig og bør benyttes ved definering av tjenester, se særlig felleskomponenter tilgjengelig fra KITH's nettsted.

Annet medisinskfaglig innhold bør ta utgangspunkt i informasjonsmodell for relevante EPJ innholdsstandarder.

Skjema for de konkrete meldingene som utveksles i en web service basert transaksjon bør utformes i samarbeid mellom tjenestetilbyder og tjenesteforbruker, med utgangspunkt i eksisterende standarder der dette eksisterer. Innholdet skal så langt som mulig være basert på felles informasjonskomponenter og strukturer som vedlikeholdes sentralt, tilsvarende som for meldingsdefinisjoner for tradisjonell meldingsutveksling. Arbeidsprosessen for tjenesteutvikling bør følge hovedstegene for standardisering som beskrevet i KITH-Rapport R18/07 "Standardiseringsprosessen og KITH-standarder".

Felles informasjonskomponenter og tjenestebeskrivelser bør derfor på sikt gjøres tilgjengelig gjennom en felles metadatatjeneste i form av et tjenesteorientert registry/repository.

7.1 "Contract first" utvikling av tjenester

I en tidlig fase av utvikling av web services ble typisk eksisterende funksjoner tilgjengeliggjort som web services og fikk autogenerated WSDL og XML for grensesnittet. Denne tilnærmingen kalles gjerne "code first" – og medfører en tett kobling mellom tjenestebeskrivelsen og implementasjonen av tjenesten. En endring i implementasjonen kan da raskt medføre at grensesnittet for tjenesten endres, noe som har konsekvenser for tjenestekonsumentene.

Det anbefalte alternativet til "code first" er "contract first", og utvikling etter denne modellen innebærer at man først definerer "kontrakten", dvs. grensesnittet for tjenesten. Denne beskrivelsen gjøres i XML Schema for de meldinger som tjenesten består av, og beskrives i en WSDL for tjenesten. Ut fra denne beskrivelsen, som opptrer som en kontrakt mellom tjenestetilbyder og konsument, kan så begge parter implementere tjeneste og kall mot tjenesten. Dette sikrer en løsere kobling mellom tjeneste og implementasjon. Hovedtrinn vil være:

1. Utarbeid XML dokument med alle data elementer som det er behov for i kontrakten i 1. Iterasjon
2. Definere datatyper på elementer som er gjentakende i XML dokumentet
3. Definere XSD med nødvendig kodeverksbeskrivelse og feilhåndteringsselementer
4. Definere versjonshåndteringsregime for tjenesten.
5. Definere WSDL som benytter input, output og SOAPFault for feilhåndtering
6. Feilhåndtering bør være beskrevet ved et eget XSD som lenkes inn i skjema til WS som utvikles
7. Beskriv autentiseringsmekanisme for tjenesten gjennom WS-Policy og WS-SecurityPolicy.
8. Beskriv noen vanlige brukstilfeller for anvendelse av tjenesten

7.2 Dokumentasjon av tjenesten

Tjenestens grensesnitt skal dokumenteres vha. en WSDL-beskrivelse. I tillegg skal tjenesten beskrives i et tjenestebeskrivelsesdokument som beskriver hvordan tjenesten skal benyttes, forutsetninger for å bruke tjenesten, sikkerhetskrav og annet.

For beskrivelse av policy for tjenesten skal WS-Policy benyttes. For beskrivelse av sikkerhetspolicy for tjenesten skal WS-SecurityPolicy benyttes.

7.3 Testing av tjenester

Testing av web service baserte tjenester kan inndeles i to hovedtilnærminger:

- **Basis testing** – Teste at tjenesten fyller basiskrav iht. de retningslinjer som er satt for tjenesteutvikling ("governance"/styringskrav). Eksempler på slike retningslinjer er HL7 web service-profil, IHE profiler og denne profilen for Web Services i helsesektoren. Kravene i disse er i hovedsak sammenfallende, og bygger på krav i profiler fra WS-I, som også utvikler testverktøy for å verifisere

samsvar med profilene. Automatiserte verktøy for å teste samsvar mot basisprofilene bør brukes før tjenestene tilgjengeliggjøres.

- **Funksjonell testing** – Testing av funksjonene og adferden til tjenesten. Denne vil avhenge av tjenestens funksjon, og det må etableres testkriterier pr. tjeneste, med testcase for input og forventede resultater.

For viktige fellestjenester bør det etableres felles godkjenningskriterier som kan inngå i den eksisterende Test- og godkjenningsordningen som KITH forvalter.

7.4 Identifikasjon av kommunikasjonsparter

Kommunikasjonsparter bør identifiseres på følgende måter:

- Virksomheter bør identifiseres vha. organisasjonsnummer fra Enhetsregisteret.
- Pasienter bør identifiseres vha. fødselsnummer, D-nummer eller H-nummer.
- Helsepersonell bør identifiseres vha. helsepersonellnummer (HPR-nummer).
- Virksomheter/avdelinger, tjenester og helsepersonell bør i tillegg identifiseres vha. HER-id.

XML struktur for beskrivelse av virksomhet og personer bør følge KITH schema med namespace: <http://www.kith.no/xmlstds/felleskomponent1>

Skjema er tilgjengelig fra: <http://www.kith.no/upload/2375/felleskomponent1.xsd>

8 Videreutvikling av profilen

Web service standardene er i løpende utvikling, og det vil være behov for oppdatering av profilen jevnlig for å inkludere nye standarder.

Pt. er særlig WS-I basic profile 1.2 på vei mot ferdigstatus. Denne inkluderer bl.a. WS-Adressing. Videre er WS-I Reliable Secure under utvikling, som spesifiserer pålitelig meldingsutveksling. Disse standardene bør inkluderes i profilen når de er i endelig utgave.

Felles retningslinjer for feilhåndtering inkl. evt. felles kodeverk for feil kan vurderes.

Behov og ønsker om endring i profilen kan meldes til meldingshjelp@kith.no

9 Referanser

HL7 Version 3 Standard: Transport Specification - Web Services Profile, Release 2

WS-I Basic Profile 1.1 – korresponderer til ”ISO/IEC 29361:2008 standard Information technology – Web Services Interoperability – WS-I Basic Profile Version 1.1”.

SAML – Security Assertions Markup Language – v. 1.1

SEID – Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater - http://www.npt.no/iKnowBase/Content/44961/SEID_Leveranse_1_v1.02.pdf