

Profil for CPP/CPA – partnerprofiler og avtaler
Til utprøving

Heftets tittel: Profil for CPP/CPA – partnerprofiler og avtaler
Status: Til utprøving
Versjon: 1.1

Utgitt: 03/2014

Bestillingsnummer: IS-2175

Utgitt av: Helsedirektoratet
Kontakt: Avdeling arkitektur, metode og standardisering
Postadresse: Pb. 7000 St Olavs plass, 0130 Oslo
Besøksadresse: Universitetsgata 2, Oslo

Tlf.: 810 20 050
Faks: 24 16 30 01
www.helsedirektoratet.no

Hftet kan bestilles hos: Helsedirektoratet
v/ Trykksaksekspedisjonen
e-post: trykksak@helsedir.no
Tlf.: 24 16 33 68
Faks: 24 16 33 69
Ved bestilling, oppgi bestillingsnummer: IS-2175

Forfattere: Thomas Tveit Rosenlund og Espen Stranger Seland

Rapporten er utarbeidet i samarbeid med Norsk Helsenett og NAV.

Innhold

Innledning	2
Ordforklaringer	3
1 Krav og forutsetninger	5
1.1 Funksjonelle krav	5
1.2 Begrensninger	5
2 Partnerprofiler og samhandlingsavtaler	6
2.1 Overordnet beskrivelse	6
3 Partnerprofil – CPP (Collaboration-Protocol Profile)	7
3.1 Hva er en CPP?	7
3.2 Datainnhold i CPP	7
3.3 Dataelementer i CPP	9
3.3.1 CollaborationProtocolProfile og cppid	9
3.4 Opprettelse av CPP	37
4 Samhandlingsavtale – CPA (Collaboration-Protocol Agreement)	38
4.1 Hva er en CPA	38
4.2 Tolking av en mottatt CPA	40
4.2.1 CollaborationProtocolAgreement og cpaid	40
4.2.2 CPA Gyldighetstid	40
4.2.3 PartyInfo	41
4.3 Sammenfletting av to CPP til en CPA	43
4.4 Mottak av en CPA	44
5 Referanser	45
Tillegg A: XML struktur og eksempel	47
SimplePart	47
Packaging	47
CollaborationRole	47
CollaborationRole i CPA	48
CPP struktur eksempel	49

Innledning

Om ebXML

Denne rapporten beskriver en standard for dokumentasjon av kommunikasjonsparametere i XML-syntaks [XML], basert på ebXML [EBXML] Collaboration Protocol Profile and Agreement (partnerprofil og samhandlingsavtale), versjon 2.0 [EBCPP], som skal benyttes for å beskrive tekniske parametere for elektronisk meldingsutveksling mellom parter i helsevesenet.

Bakgrunn

ebXML-rammeverket [EBXML] til Oasis definerer et eget XML-format som beskriver en partnerprofil, som kan benyttes til å opplyse andre om egne tekniske muligheter, herunder hvilke elektroniske tjenester man er i stand til å utføre.

Videre defineres det i samme XML-format en samhandlingsavtale for å dokumentere hvilke tjenester og meldinger som kan utveksles mellom to konkrete parter samt hvilke tekniske kommunikasjonsparametere som skal benyttes i denne utvekslingen. Hittil er det bare ebMS 2.0 [EBMS] som det er blitt standardisert på i helsesektoren gjennom [KITH:1037].

Erfaringer fra de siste årene og nye utfordringer i forbindelse med hva kommunikasjonsparter gjennom sine kommunikasjonspunkter er i stand til å sende og motta har resultert i behov for denne rapporten.

Målsetning

Rapporten beskriver krav til oppbygging av CPP og CPA og baserer seg på [KITH:1037], [EBMS] og [EBCPP]. Rapporten er ment brukt som grunnlag for å lage løsninger i helsesektoren for de aktørene som skal benytte seg av partnerprofiler (CPP) og samhandlingsavtaler (CPA).

Leserveiledning

Dokumentet er myntet på leverandører og it-personell som skal implementere støtte for CPP og CPA. Dette dokumentet bør leses sammen med ebXML Collaboration Protocol Profile and Agreement Specification Version 2.0 [EBCPP] og ebXML Message Service Specification v2.0 [EBMS]. For de som ikke er kjent med XML og XML Schema henvises det til referansene [XML] og [XMLS].

Ordforklaringer

Oversikt over viktige begreper brukt i rapporten.

Dokument	Etter arkivloven § 2: ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lyding, framsyning eller overføring. Forretningsdokument brukes ofte.
EPJ-dokument	En logisk avgrenset informasjonsmengde som godkjennes/signeres og gøres tilgjengelig for andre tjenesteytere som en helhet
Melding	Sammenstilling av opplysninger som overføres elektronisk mellom to aktører i henhold til en omforent standard. I denne sammenheng vil opplysningene i en melding alltid være et dokument eller et vedlegg.
Fagmelding	Melding på applikasjonslaget mellom to fagapplikasjoner (for eksempel to EPJ-systemer).
Payload	Fagmeldingen(e) som utveksles. Fagmelding(er) overføres fra en MSH til en annen MSH ved å pakke hver fagmelding i en MIME part. MIME parten som inneholder ebXML SOAP skal ha referanse(r) til MIME part(er) på vedlagte fagmeldinger.
Vedlegg	Dokument (eller EPJ-dokument) som har en spesiell type relasjon til et annet dokument (eller EPJ-dokument)
ebXML	electronic business eXtensible Markup Language. Internasjonal standard etablert i regi av UN/CEFACT og OASIS, for å etablere en åpen xml-basert infrastruktur som muliggjør global bruk av elektronisk forretningsinformasjon mellom alle typer forretningspartnere.
ebXML-konvolutt	En ebXML-konvolutt er en SOAP Envelope med ebXML-utvidelser i SOAP Header og SOAP Body. ebXML-konvolutt brukes for å pakke inn fagmeldingene og gi informasjon om de dataene som overføres.
HER-id	HER-id er en unik identifikator av en kommunikasjonspart. HER-id tildeles av Norsk Helsenett når kommunikasjonsparten blir registrert i NHN Adresseregister.
PKI	Public Key Infrastructure, funksjoner for elektronisk signering og kryptering.
MSH	Meldingshåndteringssystem (eng. MSH – Message Service Handler).
UML	Unified Modeling Language. Modelleringspråk som benyttes ved objektorientert analyse og design. Brukes her til å beskrive informasjonsmodellen.
XML	Extensible Markup Language. Et språk for å kunne strukturere informasjon i elementer.
XSD	XML Schema Definition Et XML-basert språk som benyttes for å beskrive og kontrollere innholdet i XML-dokumenter.

CPP	Collaboration-Protocol Profile. XML-dokument som beskriver hvilke muligheter en aktør har implementert for å kunne utføre elektronisk samhandling med andre aktører.
CPA	Collaboration Protocol Agreement. Utvekslingsavtale i form av et XML-dokument som kan lages ut av to aktørers CPPer og som viser de felles mulighetene de har til å utføre elektronisk samhandling med hverandre.
cppid	Attributt til <i>CollaborationProtocolProfile</i> elementet som skal inneholde en id som er unik for eier av CPP og bør være en URI, slik det er anbefalt av OASIS.
PartyInfo	Definisjon av aktøren. Inneholder standard kommunikasjonskanal (<i>defaultMshChannelId</i>) og pakkemåte (<i>defaultMshPackagingId</i>). Videre skal navnet på aktøren (<i>partyName</i>) og den tilhørende HER-id (<i>PartyId</i>) være med.
CollaborationRole	Angivelse av aktørens forhold til en gitt tjeneste (<i>Service</i>), hvilke konkrete handlinger (<i>Action</i>) som utføres i tjenesten og hvilken rolle den nevnte aktøren skal ha (<i>Role</i>).
CanSend/ CanReceive	Elementer i en CPP eller CPA hvor man definerer hvilke forretningsdokumenter som kan sendes eller mottas. Vil også inneholde referanse til hvilket <i>Packaging</i> element som benyttes til pakking av filene som sendes eller mottas.
Packaging	Element i en CPP eller CPA hvor man definerer sammensetningen av de filer som sendes eller mottas, dvs. hvordan filene er satt sammen av komponenter, inkl. header, payload, sikkerhet osv.
SimplePart	Element i en CPP eller CPA hvor man definerer innholdet i de komponenter som skal utveksles, og elementet inneholder referanser til en konkret melding (xsd).
SMTP	Simple Mail Transfer Protocol Asynkron kommunikasjon for meldingsutveksling.
HTTP	Hypertext Transfer Protocol Synkron kommunikasjon som benyttes for meldingsutveksling over Internett.
HTTPS	Sikker HTTP, ved at man krypterer ved bruk av f.eks. SSL (Secure Sockets Layer).

1 Krav og forutsetninger

1.1 Funksjonelle krav

Denne standarden setter som mål å definere hvordan CPP skal benyttes for å beskrive et sett av informasjon om en parts kommunikasjonsmuligheter. Dette innebærer blant annet:

- Identifisering av parten
- Partens kommunikasjonspunkt (edi-adresse, http endpoint, Web Service-URL, etc)
- Partens digitale sertifikater som skal benyttes
 - Sertifikatene skal legges i profilen
- Partens muligheter for meldingsutveksling og andre elektroniske tjenester, herunder
 - Tjenester (Services)
 - Mulige roller i tjenester (Roles)
 - Utveksling (Actions), detaljert ned til versjoner av meldinger ved hjelp av namespace

1.2 Begrensninger

Ikke alle elementer som inngår i [EBCPP] er obligatoriske.

2 Partnerprofiler og samhandlingsavtaler

Som definert i ebXML Business Process Specification Schema [ebBPSS]:
En Business Partner er en enhet som driver Business Transactions med en eller flere andre Business Partnere.

Meldingsutvekslingsegenskapene til en part (aktør) kan bli beskrevet av en Collaboration-Protocol Profile (CPP).

Meldingsutvekslingsavtale mellom to aktører beskrives ved en Collaboration-Protocol Agreement (CPA).

En CPA kan skapes ved å finne snittet mellom to aktørers CPPer.

Inkludert i CPP og CPA er detaljer for transport som kommunikasjonsprotokoll, meldingstjenester, sikkerhet og bindinger til en Business-Process-Specification (eller, litt enklere, prosess-spesifikasjon).

Prosessdokumentasjoner kan lages som ebBPSS dokument eller med vanlige UML-modeller som beskriver interaksjoner mellom de to aktørene i et bestemt elektronisk forretningssamarbeid.

I dag vil de fleste meldingene utveksles i henhold til ebMS 2.0 (beskrevet i dokument [KITH-rapport 1037-2011 Rammeverk for elektronisk meldingsutveksling i helsevesenet](#) [KITH:1037] og ebXML Message Service Specification v2.0 [EBMS]) men i enkelte tilfeller kan det som beskrives være en Webservice. Et eksempel på dette er eResept, hvor asynkrone tjenester er definert som ebXML-tjenester mens synkrone tjenester er definert som Webservice-tjenester.

2.1 Overordnet beskrivelse

En CPP definerer egenskapene til en aktør i en eller flere elektroniske forretningsprosesser.

Disse egenskapene omfatter blant annet identitet på aktøren, hvilke meldinger aktøren kan sende og motta, samt hvilke transportprotokoller, edi-adresser og sertifikater som kan benyttes.

En CPA representerer hva to aktører er i stand til å utføre i en eller flere forretningsprosesser med hverandre.

3 Partnerprofil – CPP (Collaboration-Protocol Profile)

3.1 Hva er en CPP?

En CPP er et XML-dokument som beskriver hvilke muligheter en aktør har implementert i sin systemløsning (summen av fagsystem og tilhørende meldingshåndterings-/kommunikasjons-system) for å kunne utføre elektronisk samhandling med andre aktører.

Det er verdt å bemerke at en partnerprofil ikke inneholder informasjon om aktørens organisasjon eller de helserelaterte ytelser som tilbys.

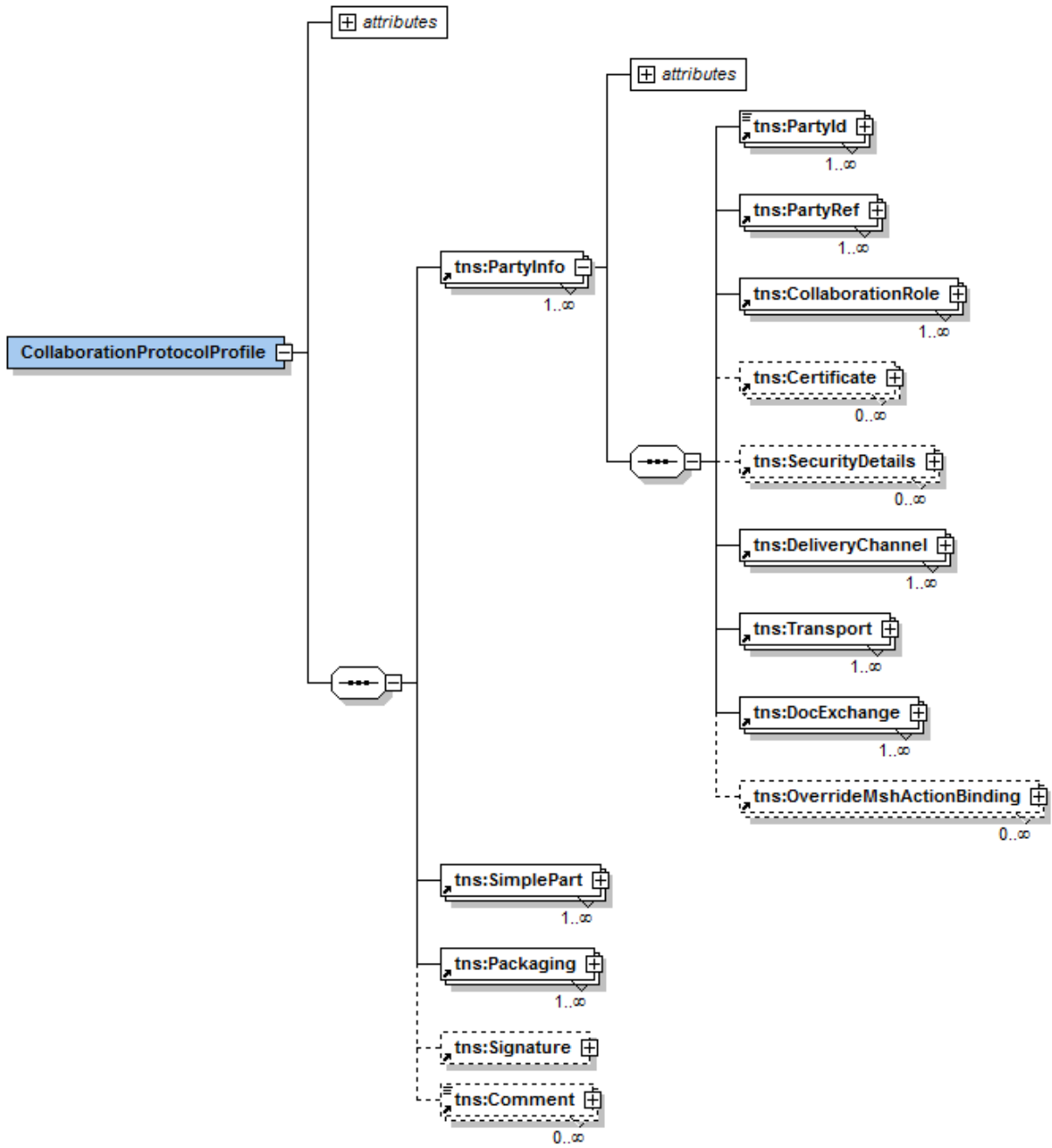
To CPPer er grunnlaget for en CPA som er nødvendig for å kunne starte opp elektronisk samhandling mellom to kommunikasjonspunkter.

CPP brukes i henhold til arkitektur for CPP/CPA [Referanse kommer].

3.2 Datainnhold i CPP

Hovedelementene i en CPP er beskrivelse av:

- Aktørens identitet (f.eks. HER-id)
- Hvilke prosesser aktøren er i stand til å utføre elektronisk (for eksempel eResept, Sykmelding, etc.)
- Hvilke meldingstyper og meldingsversjoner aktøren kan sende og/eller motta
- Hvilke roller aktøren innehar i de aktuelle prosessene
- Hvilke kommunikasjonskanaler, protokoller og tilhørende parametere som gjelder for denne formidlingen
- Hvilken sikkerhet (signaturer og kryptering) som skal benyttes
- Hvordan meldinger er sammensatt i en meldingsutveksling (msg_header, payload/fagmelding, meldingsversjoner, sikkerhet, komprimering etc.)



Figur 1: CPP - Collaboration-Protocol Profile

3.3 Dataelementer i CPP

3.3.1 *CollaborationProtocolProfile* og *cppid*

I rotelementet *CollaborationProtocolProfile* finnes det et påkrevd *cppid* attributt som er en unik id for dokumentet (CPPen). Verdien av *cppid* settes av den aktøren som eier/utsteder CPPen.

cppid må være unikt for parten som representerer CPPen. Den trenger ikke være unik innenfor helsesektoren. Det er opp til implementasjonen å velge oppbygging av *cppid*.

Plassering	<i>/CollaborationProtocolProfile</i>
Type	rotnode - container node
Tekstnoder	Ingen
Attributter	<i>cppid</i> Type: string Innhold: non-empty-string / URI Bruk: Påkrevd Unik identifikator for CPP <i>Version</i> Type: string Innhold: Versjonsidentifikasjon av CPP. Fast verdi = "2_0b" Bruk: Påkrevd
Indre elementer	<i>PartyInfo</i> <i>SimplePart</i> <i>Packaging</i> <i>Signature</i> <i>Comment</i>

3.3.1.1 PartyInfo

PartyInfo inneholder aktørens navn (*partyName*) og annen identifikasjon av aktøren, samt sammensetting (*defaultMshPackageld*) av signalmeldinger og kommunikasjonskanal (*defaultMshChannelld*) som benyttes for disse.

Aktørens alminnelige navn defineres i *partyName* attributtet i et menneskelesbart format.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p><i>partyName</i> Type: string Innhold: Aktørens alminnelige navn Bruk: Påkrevd</p> <p><i>defaultMshChannelld</i> Type: string Innhold: Verdien hentes fra attributtet <i>channelld</i> under elementet <i>DeliveryChannel</i> Bruk: Påkrevd Kommunikasjonskanal som skal benyttes hvis intet annet er spesifisert for den oppgitte tjenesten.</p> <p><i>defaultMshPackageld</i> Type: string Innhold: Verdien hentes fra attributtet <i>id</i> under elementet <i>Packaging</i> Bruk: Påkrevd Meldingssammensetning som skal benyttes hvis intet annet er spesifisert for den oppgitte tjenesten.</p>
Indre elementer	<i>PartyId</i> <i>PartyRef</i> <i>CollaborationRole</i> <i>Certificate</i> <i>SecurityDetails</i> <i>DeliveryChannel</i> <i>Transport</i> <i>DocExchange</i>

3.3.1.1.1 PartyId

PartyId skal være den samme som benyttes i ebXML Messaging [EBMS]

PartyId fra CPP skal gjenspeiles i CPA og være med i ebXML-konvolutten i en ebXML-forsendelse.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/PartyId</i>
Type	container node
Tekstnoder	Verdi relatert til <i>type</i>
Attributter	<p><i>type</i></p> <p>Type: string</p> <p>Innhold: "HER" eller annen unik ID</p> <p>Bruk: Påkrevd For aktører tilknyttet Norsk Helsenett skal HER-id benyttes. For å sikre tilbakekompatibilitet med de som ennå ikke har gått over til HER kan flere id'er benyttes, eventuelt også i tillegg til HER: "ENH", "orgnummer", "commonname" eller annen unik idtype man enes om.</p> <p>Eksempel: <code><PartyId type="HER">91093</PartyId></code></p>
Indre elementer	Ingen

3.3.1.1.2 PartyRef

PartyRef er et påkrevd element og skal inneholde en beskrivende URI. Det er ikke påkrevd at URLen peker til en gyldig adresse.

Elementet benyttes bl.a. av Reseptformidler slik at de ut fra CPPen kan avgjøre hvilken "type" aktør det er som sender inn CPP.

Eks. `<tns:PartyRef xlink:href="http://reseptformidleren.no/eResept/Lege" xlink:type="simple"/>`

For denne type bruk må verdiene dokumenteres utenfor dette dokumentet.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/PartyRef</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p><i>xlink:href</i></p> <p>Type: string</p> <p>Innhold: non-empty-string / URI</p> <p>Bruk: Påkrevd Referanse til ytterligere informasjon om aktør</p>
Indre elementer	Ingen

3.3.1.1.3 CollaborationRole

CollaborationRole refererer til en kobling mellom en tjeneste (*Service*) og den prosessrollen (*Role*) som aktøren er i stand til å fylle i en forretningsprosess. Det kan være flere *CollaborationRole*, én for hver tjeneste og rolle aktøren kan kombinere, og det er ingen begrensning på hvor mange *CollaborationRole* som kan være definert i en CPP.

For hver *CollaborationRole* er det angitt en *Role* og en *Service* (via *ServiceBinding*) i tillegg til en referanse til den prosessen tjenesten og rollen tilhører, samt sertifikat som skal benyttes (via *ApplicationCertificateRef*).

Videre under *CollaborationRole* beskrives hvilke utgående og inngående handlinger (*Action*) som aktøren er i stand til å utføre i den aktuelle prosessen.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	<i>ProcessSpecification</i> <i>Role</i> <i>ApplicationCertificateRef</i> <i>ServiceBinding</i>

3.3.1.1.3.1 ProcessSpecification

Navnet på prosessen den aktuelle tjenesten tilhører.

ProcessSpecification gir koblingen til prosessdokumentasjon som definerer samspillet mellom de to partene på et overordnet nivå. Prosessspesifikasjonen kan være på formen ebXML Business Process Specification Schema [ebBPSS], men kan også uttrykkes på andre måter.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ProcessSpecification</i>
Type	container node
Tekstnoder	ingen
Attributter	<i>name</i> Type: string Innhold: Navn på aktuell prosess Bruk: Påkrevd <i>version</i> Type: string Innhold: Prosessens versjonsnummer, for eksempel eResept v2.4 Bruk: Påkrevd <i>uuid</i> Type: string Innhold: uuid Bruk: Påkrevd

	<p>Sammen med <i>version</i> skal dette identifisere prosessen unikt i helsesektoren.</p> <p>Xlink:href Type: string Innhold: URI til prosess Bruk: Påkrevd – URI trenger ikke resolve til en faktisk adresse</p> <p>Xlink:type Type: fixed Innhold: Fast verdi ="simple" Bruk: Påkrevd</p>
Indre elementer	Ingen

3.3.1.1.3.2 *Role*

Rollen som parten kan fylle i den aktuelle prosessen. En aktør kan kun inneha én rolle av gangen. Verdien i *Role* skal også med i ebXML-konvolutten under */eb:MessageHeader/eb:From/eb:Role* og */eb:MessageHeader/eb:To/eb:Role*.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/Role</i>
Type	empty node
Tekstnoder	ingen
Attributter	<p>name Type: string Innhold: Navn på aktuell rolle innen prosessen Bruk: Påkrevd</p> <p>Xlink:href Type: String Innhold: URI til rollebeskrivelse. URI trenger ikke å peke til en faktisk adresse. Bruk: Påkrevd</p> <p>Xlink:type Type: fixed Innhold: Fast verdi ="simple" Bruk: Påkrevd</p>
Indre elementer	Ingen

3.3.1.1.3.3 *ApplicationCertificateRef*

Referanse til *Certificate* elementet som inneholder sertifikatet som skal benyttes til kryptering.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ ApplicationCertificateRef</i>
Type	empty node
Tekstnoder	Ingen
Attributter	<p>certId Type: IDREF Innhold: ID til <i>Certificate</i> element Bruk: Påkrevd</p>
Indre elementer	Ingen

3.3.1.1.3.4 *ServiceBinding*

Informasjon om tjenesten som benyttes for å fylle rollen. Har indre elementer som beskriver hva aktøren er i stand til å sende og motta.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ServiceBinding</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	<i>Service</i> <i>CanSend</i> <i>CanReceive</i>

3.3.1.1.3.4.1 *Service*

Tjenesten man benytter, eksempelvis *eResept* eller *HarBorgerEgenandelFritak*. Verdien i *Service* og tilhørende type-attributt skal også med i ebXML-konvolutten under */eb:MessageHeader/eb:Service*.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ServiceBinding/Service</i>
Type	empty node med attributt
Tekstnode r	Tjenestenavn
Attributter	<i>type</i> Type: non-empty.string Innhold: type Tjenestenavn f.eks "string", "kithService" eller annen avtalt type. Typen vil normalt være definert sammen med verdien. Bruk: Påkrevd hvis Tjenestenavn ikke er en URI
Indre elementer	Ingen

3.3.1.1.3.4.2 *CanSend*

Her defineres hva en aktør er i stand til å sende (*Action*) innenfor en *Service* og inneholder også referanse til hvilken pakkemåte (*Packaging*) som skal benyttes, samt andre parametere som er nødvendige for å utføre denne handlingen.

Hvilken melding som skal utveksles i den aktuelle handlingen vil være definert under *SimplePart* delen i CPPen. Den aktuelle *SimplePart* er linket gjennom den pakkemåte som benyttes av denne handlingen og som er definert i *Packaging* delen av CPPen.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ServiceBinding/CanSend</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	<i>ThisPartyActionBinding</i>

3.3.1.1.3.4.2.1 *ThisPartyActionBinding*

Dette elementet inneholder informasjon om den aktuelle meldingen som skal sendes.

Meldingen som sendes i denne aktuelle meldingsutvekslingen, eks. *Rekvirering* eller *EgenandelForespørsel* defineres i *action* attributtet.

packageld attributtet refererer til hvilken pakkemåte/sammensetning (*Packaging*) som skal benyttes for meldingen i den aktuelle utvekslingen.

Fra *Packaging* refereres det videre til en spesifikk *SimplePart* hvor den konkrete meldingen som utveksles er definert.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ServiceBinding/CanSend/ThisPartyActionBinding</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p>action</p> <p>Type: string</p> <p>Innhold: Navn på hendelsen</p> <p>Bruk: Påkrevd</p> <p>id</p> <p>Type: ID</p> <p>Innhold: Unik id for utvekslingen innen CPPen</p> <p>Bruk: Påkrevd</p> <p>packageld</p> <p>Type: IDREF</p> <p>Innhold: Ref. til den aktuelle <i>Packaging</i> som benyttes for denne konkrete utvekslingen</p> <p>Bruk: Påkrevd</p> <p>xlink:type</p> <p>Type: string</p> <p>Innhold: Fast verdi = "simple"</p> <p>Bruk: Påkrevd</p>
Indre elementer	<i>BusinessTransactionCharacteristics</i> <i>Channeld</i>

3.3.1.1.3.4.2.1.1 *BusinessTransactionCharacteristics*

BusinessTransactionCharacteristics inneholder opplysninger om kommunikasjon, sikkerhet og signering knyttet til den aktuelle handlingen.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ServiceBinding/CanSend/ThisPartyActionBinding/BusinessTransactionCharacteristics</i>
Type	empty node
Tekstnoder	Ingen
Attributter	<p><i>isAuthenticated</i></p> <p>Type: string</p>

Innhold: enum ("none", "transient", "persistent", "persistent-and-transient")
Bruk: Påkrevd
For SMTP normalt "persistent"
Transient autentisering kan gjøres med en sikker transportprotokoll som SSL, mens persistent autentisering kan gjøres med digital signatur.

isAuthorizationRequired

Type: string
Innhold: enum("true", "false") Fast verdi ="false"
benyttes
Bruk: Påkrevd

isConfidential

Type: string
Innhold: enum ("none", "transient", "persistent", "persistent-and-transient")
Bruk: Påkrevd
For SMTP normalt "persistent"
Transient konfidensialitet kan sikres med en sikker transportprotokoll som SSL, mens persistent konfidensialitet kan gjøres med kryptering.

timeToAcknowledgeReceipt

Type: string
Innhold: Format *XML Schema Duration*
Bruk: Påkrevd
Angir tiden fra en melding er mottatt til Acknowledgement må sendes.

isNonRepudiationReceiptRequired

Type: string
Innhold: Fast enum("true", "false") Fast verdi ="true"
benyttes
Bruk: Påkrevd

isNonRepudiationRequired

Type: string
Innhold: enum("true", "false") Fast verdi ="true"
benyttes
Bruk: Påkrevd

isTamperProof

Type: string
Innhold: enum ("none", "transient", "persistent", "persistent-and-transient")
Bruk: Påkrevd
For SMTP normalt "persistent"
Transient sikring mot endringer kan gjøres med en sikker transportprotokoll som SSL, mens persistent sikring mot endringer kan gjøres med digital signatur.

	<p><i>timeToPerform</i></p> <p>Type: string</p> <p>Innhold: Format XML Schema Duration</p> <p>Bruk: Påkrevd</p> <p>Angir tiden fra en melding er sendt til respons skal være mottatt i form av forretningsdokument. (I helsesektoren som regel en AppRec hvor man har en standardverdi = P4D. Dvs. at AppRec skal være mottatt innen 96 timer etter mottak av melding).</p>
Indre elementer	Ingen

3.3.1.1.3.4.2.1.2 *ChannelId*

ChannelId inneholder ID til *DeliveryChannel*.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ServiceBinding/CanSend/ThisPartyActionBinding/ChannelId</i>
Type	text node
Tekstnoder	ID på den kommunikasjonskanalen som benyttes for denne konkrete utvekslingen. Hentes fra attributtet <i>channelId</i> i elementet <i>DeliveryChannel</i> .
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.3.4.3 *CanReceive*

Her defineres hva en aktør er i stand til å motta (*Action*) innenfor en *Service* og inneholder også referanse til hvilken pakkemåte (*Packaging*) som skal benyttes, samt andre parametere som er viktige for å utføre denne handlingen.

Hvilken melding som skal utveksles vil være definert under *SimplePart* delen i CPPen. Den aktuelle *SimplePart* er linket gjennom den pakkemåte som benyttes og som er definert i *Packaging* delen av CPPen.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/CollaborationRole/ServiceBinding/CanReceive</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	<i>ThisPartyActionBinding</i>

3.3.1.1.3.4.3.1 *ThisPartyActionBinding*

Se tilsvarende kapittel under *CanSend* (kap. 3.3.1.1.3.4.2.1)

3.3.1.1.3.4.3.1.1 *BusinessTransactionCharacteristics*

Se tilsvarende kapittel under *CanSend* (kap. 3.3.1.1.3.4.2.1.1)

3.3.1.1.3.4.3.1.2 ChannelId

Se tilsvarende kapitel under CanSend (kap. 3.3.1.1.3.4.2.1.2)

3.3.1.1.4 Certificate

En CPP kan inneholde flere instanser av dette elementet. Hver instans av *Certificate* skal inneholde informasjon om ett sertifikat. *Certificate*-elementer kan refereres til fra flere steder i en CPP. Sertifikatet representert i et *Certificate*-element kan være et virksomhetssertifikat (kryptering eller signering) eller et SSL sertifikat.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Certificate</i>
Type	container node
Tekstnoder	Ingen
Attributter	certId Type ID Innhold Unik id innenfor CPP Bruk Påkrevd
Indre elementer	ds:KeyInfo

3.3.1.1.4.1 ds:Keyinfo

Elementet kan inneholde nøkler, navn, sertifikater og annen informasjon om offentlige nøkler. *KeyInfo* er spesifisert ihht XMLDsig. I helsevesenet er PKI basert på X509 sertifikater påkrevd. Dermed benyttes kun elementet *X509Data* for å beskrive et sertifikat, de øvrige indre elementene skal normalt ikke være med.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Certificate/ds:KeyInfo</i>
Type	container node
Tekstnoder	Ingen
Attributter	id Type ID Innhold Unik id innenfor CPP Bruk Påkrevd
Indre elementer	<i>ds:KeyName</i> <i>ds:KeyValue</i> <i>ds:RetrievalMethod</i> ds:X509Data <i>ds:PGPData</i> <i>ds:SPKIData</i> <i>ds:MgmtData</i>

3.3.1.1.4.1.1 ds:X509Data

Elementet er av typen container node som kan beskrive identifikatorer for nøkler eller sertifikater. *X509Data* er spesifisert ihht XMLDsig. For CPP skal elementet inneholde *X509Certificate*, de øvrige indre elementene kan være med ved behov.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Certificate/ds:KeyInfo/ds:X509Data</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen

Indre elementer	<i>ds:X509IssuerSerial</i> <i>ds:X509SKI</i> <i>ds:X509SubjectName</i> <i>ds:X509Certificate</i> <i>ds:X509CRL</i>
-----------------	---

3.3.1.1.4.1.1.1 *ds:X509Certificate*

Elementet inneholder en base64 kodet streng som representerer et X509 sertifikat.

Det er viktig for effektiv bruk av CPP at sertifikatet legges med i profilen.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Certificate/ds:KeyInfo/ds:X509Data/ds:X509Certificate</i>
Type	Base64Binary
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.5 *SecurityDetails*

Ikke påkrevd. Kan inneholde informasjon om hvilke rotsertifikater som denne profilen stoler på.

3.3.1.1.6 *DeliveryChannel*

DeliveryChannel referer til de kommunikasjonsmåter som skal benyttes for de hendelser (*Action*) som er definert under *CollaborationRole*. En *DeliveryChannel* skal inneholde referanse til et *Transport* element og et *DocExchange* element. En CPP skal inneholde minst én *DeliveryChannel*, men kan inneholde flere etter behov. Dersom en aktør har mulighet for å kommunisere over både SMTP og HTTP vil det være definert en *DeliveryChannel* for hver kommunikasjonsprotokoll. Resendingsbehov kan variere mellom sendinger og dette kan støttes ved å definere flere *DeliveryChannel*'s som refererer til forskjellige *DocExchange*.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DeliveryChannel</i>
Type	container node
Tekstnoder	Ingen
Attributter	<i>channelId</i> Type: ID Innhold: id Bruk: Påkrevd, unik <i>transportId</i> Type: IDREF Innhold: id Bruk: Påkrevd <i>docExchangeld</i> Type: IDREF Innhold: id Bruk: Påkrevd

Indre elementer	MessagingCharacteristics
-----------------	---------------------------------

3.3.1.1.6.1 MessagingCharacteristics

Beskriver de attributtene som gjelder for overføring av meldinger over en gitt kanal. Attributtene under kan defineres fast for alle meldinger over en kanal, eller man kan definere det på en "per melding" basis.

Plassering	/CollaborationProtocolProfile/PartyInfo/DeliveryChannel/MessagingCharacteristics
Type	container node
Tekstnoder	Ingen
Attributter	<p>syncReplyMode</p> <p>Type: string</p> <p>Innhold: mshSignalsOnly, responseOnly eller none (signalsOnly, signalsAndResponse)</p> <p>Bruk: Påkrevd <i>For all SMTP trafikk skal det stå "none". For HTTP-trafikk må det først finnes ut om man skal ha asynkron eller synkrone svar. Skal man ha asynkrone svar vil det typisk returneres en Acknowledgment eller Error over samme sesjon. En Acknowledgment er et signal og det skal stå "mshSignalsOnly". Dersom det skal være synkrone svar skal det stå "responsesOnly". Verdierne "signalsOnly" og "signalsAndResponse" skal ikke benyttes dersom ikke det er spesielle behov som må tilfredsstilles.</i></p> <p>ackRequested</p> <p>Type: string</p> <p>Innhold: always, never eller perMessage</p> <p>Bruk: Påkrevd Forteller om det i SOAP-konvolutt skal etterspørres en Acknowledgment fra mottaker av melding. <i>Hovedregelen er at det skal stå "always" for all SMTP trafikk.</i> For HTTP kan det være hensiktsmessig å bruke verdien "never" der responsen kommer i samme HTTP sesjon. Da er det ikke behov for noen Acknowledgment.</p> <p>ackSignatureRequested</p> <p>Type: string</p> <p>Innhold: always, never eller perMessage</p> <p>Bruk: Påkrevd Forteller om det i SOAP konvolutt skal etterspørres en signert Acknowledgment fra mottaker av melding. <i>Hovedregelen her er at det skal stå "always" dersom annet ikke er avtalt.</i></p> <p>duplicateElimination</p> <p>Type: string</p> <p>Innhold: always, never eller perMessage</p>

	Bruk: Påkrevd Forteller om det i SOAP konvolutt skal stå at mottaker skal duplikateliminere denne meldingen. Hovedregelen her er at det skal stå "always" dersom annet ikke er avtalt. Actor Type: string Innhold: Bruk: Ikke påkrevd
Indre elementer	Ingen

3.3.1.1.7 *Transport*

Transport referer til de kommunikasjonsmåter som aktøren benytter til å sende eller motta meldinger/hendelser. Den kommunikasjonsmåten som er definert under *Transport* er den eneste gyldige kommunikasjonsmåten som kan være referert i *DeliveryChannel*.

Det vil være definert en *Transport* for hver *DeliveryChannel* som benyttes, som f.eks. for SMTP, HTTP osv. Det vil også kunne være definert flere *Transport* for samme kommunikasjonsmåte hvis det er aktuelt å benytte flere kanaler.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport</i>
Type	container node
Tekstnoder	Ingen
Attributter	<i>transportId</i> Type: ID Innhold: id Bruk: Påkrevd, unik
Indre elementer	<i>TransportSender</i> <i>TransportReceiver</i>

3.3.1.1.7.1 *TransportSender*

Angir data om avsenderen i en *DeliveryChannel*. Det er normalt kun *TransportProtocol* som benyttes for SMTP, mens for HTTP benyttes både *TransportProtocol* og *TransportClientSecurity*.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportSender</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	<i>TransportProtocol</i> <i>AccessAuthentication</i> <i>TransportClientSecurity</i>

3.3.1.1.7.1.1 *TransportProtocol*

Beskriver protokollen som benyttes i en *DeliveryChannel*. Den vanligste verdien i helsesektoren er SMTP, men også HTTP benyttes. Andre protokoller som f.eks. FTP er også lovlige verdier. Her kan man potensielt også legge inn *WebService*.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportSender/TransportProtocol</i>
Type	text node med attributt
Tekstnoder	Protokollen benyttet til kommunikasjon. F.eks "SMTP", "HTTP", "FTP"
Attributter	version Type: string Innhold: Versjon av protokollen HTTP versjon 1.1 SMTP enten ingen versjon eller 1.0 FTP enten "FTP", "SFTP", "FTP over SSH" eller "FTPS" Bruk: Påkrevd
Indre elementer	Ingen

3.3.1.1.7.1.2 AccessAuthentication

Kan angi krav til autentisering for transporten. Ikke brukt i helsesektoren.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportSender/AccessAuthentication</i>
Type	text node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.7.1.3 TransportClientSecurity

Brukes til å angi sikkerheten på transportnivå. I praksis vil det si SSL for HTTP. TLS for SMTP kan også angis, men TLS benyttes ikke i helsesektoren.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportSender/TransportClientSecurity</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	TransportSecurityProtocol ClientCertificateRef ServerSecurityDetailsRef EncryptionAlgorithm

3.3.1.1.7.1.3.1 TransportSecurityProtocol

Her angis SSL for HTTPS.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportSender/TransportClientSecurity/TransportSecurityProtocol</i>
Type	text node med attributt
Tekstnoder	Fast verdi = "SSL"
Attributter	version Type: string

	Innhold: Versjon av protokollen (f.eks. 3.0) Bruk: Påkrevd
Indre elementer	Ingen

3.3.1.1.7.1.3.2 *ClientCertificateRef*

Angir SSL-sertifikat brukt i HTTPS dersom aktøren må identifisere seg på transportnivå. Kun aktuelt ved krav til 2-veis SSL.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportSender/TransportClientSecurity/ClientCertificateRef</i>
Type	empty node
Tekstnoder	Ingen
Attributter	certId Type: IDREF Innhold: Referanse til sertifikatets Id i CPP Bruk: Påkrevd
Indre elementer	Ingen

3.3.1.1.7.1.3.3 *ServerSecurityDetailsRef*

Ikke brukt i helsesektoren.

3.3.1.1.7.1.3.4 *EncryptionAlgorithm*

Ikke brukt i helsesektoren.

3.3.1.1.7.2 *TransportReceiver*

Angir data om mottakeren i en *DeliveryChannel*. Det er normalt kun *TransportProtocol* som benyttes for SMTP, mens for HTTP benyttes både *TransportProtocol* og *TransportClientSecurity*.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportReceiver</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	<i>TransportProtocol</i> <i>AccessAuthentication</i> <i>Endpoint</i> <i>TransportServerSecurity</i>

3.3.1.1.7.2.1 *TransportProtocol*

Beskriver protokollen som benyttes i en *DeliveryChannel*. Vanligste verdien i helsesektoren er SMTP, men også HTTP er i bruk, og andre som FTP er også lovlige verdier. Her kan man potensielt også legge inn WebService.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportReceiver/TransportProtocol</i>
Type	text node med attributt
Tekstnoder	Protokollen benyttet til kommunikasjon. F.eks. SMTP, HTTP, FTP

Attributter	version Type: string Innhold: Versjon av protokollen Bruk: Påkrevd
Indre elementer	Ingen

3.3.1.1.7.2.2 AccessAuthentication

Ikke brukt i helsesektoren

3.3.1.1.7.2.3 Endpoint

Angir edi-adressen i denne *DeliveryChannel*. For SMTP angis en epostadresse. For HTTP og FTP angis en URL.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportReceiver</i>
Type	container node
Tekstnoder	Ingen
Attributter	uri Type: uri Innhold: URI til endpoint Bruk: Påkrevd type Type: enumeration Innhold: Fast verdi ="allPurpose". OASIS sin standard tillater andre verdier, men de er ikke i bruk i helsesektoren. Bruk: Valgfri
Indre elementer	Ingen

3.3.1.1.7.2.4 TransportServerSecurity

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportReceiver</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	TransportSecurityProtocol ServerCertificateRef <i>ClientSecurityDetailsRef</i> <i>EncryptionAlgorithm</i>

3.3.1.1.7.2.4.1 TransportSecurityProtocol

Her angis sikkerhetsprotokoll for transporten. For HTTPS er det f.eks "SSL".

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportReceiver/TransportClientSecurity/TransportSecurityProtocol</i>
Type	text node med attributt
Tekstnoder	F.eks. "SSL"
Attributter	version Type: string Innhold: Versjon av protokollen (f.eks. 3.0)

	Bruk: Påkrevd
Indre elementer	Ingen

3.3.1.1.7.2.4.2 *ServerCertificateRef*

Angir SSL sertifikat brukt i HTTP.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/Transport/TransportReceiver</i>
Type	container node
Tekstnoder	Ingen
Attributter	<i>certId</i> Type: IDREF Innhold: Referanse til sertifikatets Id i CPP Bruk: Påkrevd
Indre elementer	Ingen

3.3.1.1.7.2.4.3 *ClientSecurityDetailsRef*

Ikke benyttet i helsesektoren.

3.3.1.1.7.2.4.4 *EncryptionAlgorithm*

Ikke benyttet i helsesektoren.

3.3.1.1.8 *DocExchange*

DocExchange angir de parameterne som gjelder for de enkelte kommunikasjonsmåtene og sikkerheten knyttet til forsendelsene.

Det skal angis parametere for antall re-sendinger, intervall mellom hver sending, duplikatsjekk, hvilken sikkerhetsalgoritme og hvilken hashfunksjon skal benyttes til å signere og kryptere forsendelsen inkludert hvilke sertifikater som skal legges til grunn.

Minst en av *ebXMLSenderBinding* og *ebXMLReceiverBinding* må være i bruk.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange</i>
Type	container node
Tekstnoder	Ingen
Attributter	<i>docExchangeld</i> Type: ID Innhold: id Bruk: Påkrevd, unik for dokumentet
Indre elementer	<i>ebXMLSenderBinding</i> <i>ebXMLReceiverBinding</i>

3.3.1.1.8.1 *ebXMLSenderBinding*

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding</i>
Type	container node

Tekstnoder	Ingen
Attributter	version Type: string Innhold: Versjon av ebMS Kun "2.0" i bruk i helsesektoren i dag. Bruk: Påkrevd
Indre elementer	ReliableMessaging PersistDuration SenderNonRepudiation <i>SenderDigitalEnvelope</i> <i>NamespaceSupported</i>

3.3.1.1.8.1.1 *ReliableMessaging*

ReliableMessaging er den delen av standarden som dekker sikker levering med leveringsbekreftelse og duplikateliminerings. Dette er Påkrevd i helsesektoren.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/ReliableMessaging</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	Retries RetryInterval MessageOrderSemantics

3.3.1.1.8.1.1.1 *Retries*

Angir hvor mange ganger MSH skal resende hvis den ikke får enten en Acknowledge, som betyr at meldingen er mottatt, eller en Error, som betyr at meldingen ikke kan mottas. Når det ikke er flere resendinger igjen og meldingen fortsatt ikke er bekreftet mottatt er den å anse som ikke levert.

NAV og eResept har som regel satt verdien "4".

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/ReliableMessaging/Retries</i>
Type	text node
Tekstnoder	Antallet resendinger som skal utføres ved manglende Acknowledge/Error. Default verdi er 4.
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.8.1.1.2 *RetryInterval*

Angir hvor ofte MSH skal prøve å resende meldinger.

NAV har som regel 12 timer. eResept har 4 timers intervall.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/ReliableMessaging/RetryInterval</i>
------------	---

Type	text node
Tekstnoder	Intervall mellom re-sendinger. Format: <i>XML Schema Duration</i> . F.eks: "PT12H" = 12 timer
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.8.1.1.3 *MessageOrderSemantics*

Angir om MSH har ansvar for å levere meldinger i rekkefølge.

I helsesektoren er det ikke støtte for å angi eller kreve rekkefølge på meldingene. Derfor skal verdien alltid være *NotGuaranteed*.

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/ReliableMessaging/MessageOrderSemantics</i>
Type	text node
Tekstnoder	<i>NotGuaranteed</i>
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.8.1.2 *PersistDuration*

PersistDuration angir minste tiden som en ebXML MSH må ha meldingen liggende for duplikateliminerings (evt. levering i rekkefølge.)

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/PersistDuration</i>
Type	text node
Tekstnoder	Tidsintervall. Format <i>XML Schema Duration</i> Minimumstid "P4D" = 4 dager
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.8.1.3 *SenderNonRepudiation*

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/SenderNonRepudiation</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	<i>NonRepudiationProtocol</i> <i>HashFunction</i> <i>SignatureAlgorithm</i> <i>SigningCertificateRef</i>

3.3.1.1.8.1.3.1 *NonRepudiationProtocol*

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/SenderNonRepudiation/NonRepudiationProtocol</i>
Type	text node

Tekstnoder	"http://www.w3.org/2000/09/xmldsig#"
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.8.1.3.2 HashFunction

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/SenderNonRepudiation/HashFunction</i>
Type	text node
Tekstnoder	"http://www.w3.org/2000/09/xmldsig#sha1"
Attributter	Ingen
Indre elementer	Ingen

3.3.1.1.8.1.3.3 SignatureAlgorithm

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/SenderNonRepudiation/SignatureAlgorithm</i>
Type	text node
Tekstnoder	RSA-SHA1
Attributter	<p>enumerationType</p> <p>Type: string Bruk: Ikke i bruk</p> <p>oid</p> <p>Type: string Innhold: Fast verdi ="1.2.840.113549.1.1.5" Bruk: Påkrevd</p> <p>w3c</p> <p>Type: string Innhold: Fast verdi =" http://www.w3.org/2000/09/xmldsig#rsa-sha1" Bruk: Påkrevd</p>
Indre elementer	Ingen

3.3.1.1.8.1.3.4 SigningCertificateRef

Plassering	<i>/CollaborationProtocolProfile/PartyInfo/DocExchange/ebXMLSenderBinding/SenderNonRepudiation/SigningCertificateRef</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p>certId</p> <p>Type: IDREF Innhold: Referanse til Id til sertifikatet brukt til signering av ebXML konvolutt Bruk: Påkrevd</p>
Indre elementer	Ingen

3.3.1.1.8.1.4 *SenderDigitalEnvelope*

Ikke brukt i helsesektoren.

3.3.1.1.8.1.4.1 *DigitalEnvelopeProtocol*

Ikke brukt i helsesektoren.

3.3.1.1.8.1.4.2 *EncryptionAlgorithm*

Ikke brukt i helsesektoren.

3.3.1.1.8.1.4.3 *EncryptionSecurityDetailsRef*

Ikke brukt i helsesektoren.

3.3.1.1.8.1.5 *NamespaceSupported*

Ikke brukt i helsesektoren.

3.3.1.1.8.2 *ebXMLReceiverBinding*

Ikke brukt i helsesektoren.

3.3.1.1.8.2.1 *ReliableMessaging*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.1.1 *Retries*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.1.2 *RetryInterval*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.1.3 *MessageOrderSemantics*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.2 *PersistDuration*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.3 *ReceiverNonRepudiation*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.3.1 *NonRepudiationProtocol*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.3.2 *HashFunction*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.3.3 *SignatureAlgorithm*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.3.4 *SigningSecurityDetailsRef*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.4 *ReceiverDigitalEnvelope*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.4.1 *DigitalEnvelopeProtocol*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.4.2 *EncryptionAlgorithm*

Ikke i bruk i helsesektoren.

3.3.1.1.8.2.4.3 *EncryptionCertificateRef*

Ikke i bruk i helsesektoren.

3.3.1.2 *SimplePart*

SimplePart angir de meldingstyper og meldingsversjoner som blir benyttet av de forskjellige hendelsene. *SimplePart* refereres til av *Packaging*-element som igjen benyttes i de aktuelle hendelsene som er definert under *CollaborationRole*.

Plassering	<i>/CollaborationProtocolProfile/SimplePart</i>
Type	container node
Tekstnoder	Ingen
Attributter	<i>id</i> Type: ID Innhold: Navn på meldingen som benyttes Bruk: Påkrevd, unik <i>mimetype</i> Type: String Innhold: Fast verdi = "application/xml" Bruk: Påkrevd
Indre elementer	<i>NamespaceSupported</i>

3.3.1.2.1 *NamespaceSupported*

I *NamespaceSupported* elementet under *SimplePart* må det defineres referanser til den melding (XSD) de nevnte komponenter inneholder. I "*location*"-attributtet i *NamespaceSupported* elementet angis det korrekte namespace på de meldingene man skal og har mulighet til å utveksle. Eventuelt vil man også kunne benytte "*version*"-attributtet for å angi hvilken versjon den angjeldende melding har.

For meldinger som benytter hodemeldingen anbefales det å oppgi to *NamespaceSupported* elementer, ett for hodemeldingen og ett for hvert hovedvedlegg til hodemeldingen (vanligvis første dokumentreferanse i hodemeldingen).

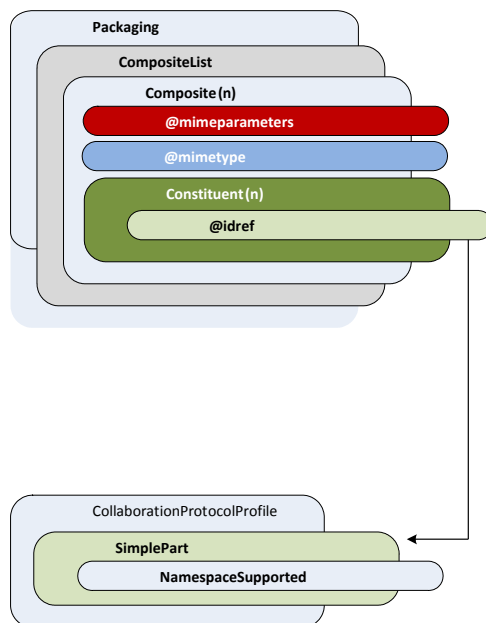
Plassering	<i>/CollaborationProtocolProfile/SimplePart/NamespacedSupported</i>
Type	text node
Tekstnoder	Korrekt namespace til meldingen som benyttes Eksempel: http://www.kith.no/xmlstds/eresept/m1/2010-05-01
Attributter	<p>location</p> <p>Type: anyURI Innhold: Korrekt filnavn på XSD som benyttes Bruk: Påkrevd Eksempel: «ER-M1-2010-05-01.xsd»</p> <p>version</p> <p>Type: String Innhold: Versjonsnummer på meldingen som benyttes. Versjonsnummer gjenspeiler meldignsversjonen for fagmeldingen. Bruk: Påkrevd Eksempel: «2.4»</p>
Indre elementer	Ingen

3.3.1.3 Packaging

Packaging angir hvilke måter de enkelte meldinger skal pakkes. Meldingene defineres i egne *SimplePart* elementer (kap. 3.3.1.1.7) som igjen blir referert fra *Packaging*. Hvert *Packaging* element er referert fra de enkelte *CanSend* (kap. 3.3.1.1.3.4.2) eller *CanReceive* (kap. 3.3.1.1.3.4.3) elementene under *CollaborationRole* (kap. 3.3.1.1.3).

Sammensetningen av de filer som sendes eller mottas er angitt i *Packaging* elementet i CPP. Navnet på det aktuelle *Packaging* elementet må refereres fra "packagingId"-attributtet i *ThisPartyActionBinding* elementet som ligger under *CanSend* og/eller *CanReceive* elementene. *CanSend* og *CanReceive* er definert under *CollaborationRole*.

I *Packaging* elementet må det defineres referanse til et *SimplePart* element hvor de komponenter som skal utveksles er definert. Hvis filen skal krypteres og/eller komprimeres skal denne referansen angis i *Constituent* elementet som ligger under *Packaging/CompositeList/Encapsulation*. Hvis ikke, skal referansen til *SimplePart* angis i *Constituent* elementet som ligger under *Packaging/CompositeList/Composite*.



Figur 2: CPP - Packaging og SimplePart

Et konkret eksempel (eResept-meldingen M18 benyttes som eksempel) for å illustrere *Packaging* og *SimpleType*:

```
<tns:SimplePart tns:id="message_erm18_v2p4r1" tns:mimetype="application/xml">
  <tns:NamespaceSupported
    tns:location="MsgHead-v1_2.xsd"
    tns:version="1.2">http://www.kith.no/xmlstds/msghead/2006-05-24</tns:NamespaceSupported>
  <tns:NamespaceSupported
    tns:location="ER-M18-2010-10-01.xsd"
    tns:version="2.4.1">http://www.kith.no/xmlstds/eresept/m18/2010-10-01</tns:NamespaceSupported>
</tns:SimplePart>

<tns:SimplePart tns:id="msg_header" tns:mimetype="text/xml">
  <tns:NamespaceSupported
    tns:location="msg-header-2_0.xsd"
    tns:version="2.0">http://www.oasis-open.org/committees/ebxml-msg/schema/
  </tns:NamespaceSupported>
</tns:SimplePart>

<tns:Packaging tns:id="package_oppgjorskrav_v2p4r1">
  <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
  <tns:CompositeList>
    <tns:Encapsulation tns:id="zip_erm18_v2p4r1" tns:mimetype="application/x-gzip" tns:mimeparameters="type=application/x-gzip">
      <tns:Constituent tns:idref="message_erm18_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Encapsulation tns:id="enc_erm18_v2p4r1" tns:mimetype="application/pkcs7-mime" tns:mimeparameters="smime-type=&quot;enveloped-data&quot;">
      <tns:Constituent tns:idref="zip_erm18_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Composite tns:id="msg_erm18_v2p4r1" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
      <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
      <tns:Constituent tns:idref="enc_erm18_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Composite>
  </tns:CompositeList>
</tns:Packaging>
```

Indre elementer defineres før de refereres, slik at det ytterste elementet alltid er nederst i listen.

To grunnelementer defineres som *SimplePart*.

- Meldingen M18 som definert av KITH (message_ERM18_v2p4r1)
- ebXML header som definert av OASIS (msg_header)

Deretter bygges det nye strukturer basert på disse:

- En innkapsling av meldingen M18 ved at den pakkes med gzip (zip_ERM18_v2p4r1)
- En innkapsling av den pakkede meldingen M18 ved at den krypteres med PKCS7 (enc_ERM18_v2p4r1)
- Et kompositt av ebXML-header og den krypterte, pakkede meldingen M18 (msg_ERM18_v2p4r1). Dette er selve ebMS-meldingen som utveksles.

På denne måten har man en konsis, entydig og oversiktlig beskrivelse av det som skjer med meldingen M18 fra den er ferdig signert til den er klar til å bli oversendt mottaker. Om dette tolkes maskinelt eller bare benyttes som dokumentasjon er implementasjonsavhengig.

Plassering	<i>/CollaborationProtocolProfile/Packaging</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p>id</p> <p>Type: ID</p> <p>Innhold: Navn på meldingen som benyttes</p> <p>Bruk: Påkrevd</p> <p>Verdien blir referert til i <i>packageId</i> attributtet i <i>/CollaborationProtocolProfile/PartyInfo/ CollaborationRole/ServiceBinding /CanSend/ ThisPartyActionBinding</i> og <i>../CanReceive/ ThisPartyActionBinding</i></p> <p>mimetype</p> <p>Type: string</p> <p>Innhold: Fast verdi = "application/xml"</p> <p>Bruk: Påkrevd</p>
Indre elementer	<i>ProcessingCapabilities CompositeList</i>

3.3.1.3.1 *ProcessingCapabilities*

Definert av OASIS for å beskrive om MSH støttet MIME lesing og/eller skrivning. Alle relevante MSHer støtter dette i dag. Den er derfor av mer historisk interesse og begge verdier vil i helsesektoren alltid være "true".

Plassering	<i>/CollaborationProtocolProfile/Packaging/ProcessingCapabilities</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p>generate</p> <p>Type: string</p> <p>Innhold: Fast verdi = "true"</p> <p>Bruk: Påkrevd</p> <p>parse</p>

	Type: string Innhold: Fast verdi = "true" Bruk: Påkrevd
Indre elementer	Ingen

3.3.1.3.2 CompositeList

CompositeList inneholder et antall *Encapsulation* og/eller *Composite* elementer som hver tilsvarer en innpakket eller sammensatt melding som skal utveksles. Hvordan meldingen er sammensatt defineres under *Encapsulation* og *Composite* elementene.

Plassering	/CollaborationProtocolProfile/Packaging/CompositeList
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	Encapsulation Composite

3.3.1.3.2.1 Encapsulation

Encapsulation forteller hvordan et meldingselement er pakket inn. Dette kan f.eks være kryptering eller komprimering av hele eller deler av payload. Man bygger en *Encapsulation* (innpakking) som inneholder en forekomst av et *Constituent* element, samt en innpakking eller transformering for den aktuelle versjonen av den melding som skal utveksles.

Plassering	/CollaborationProtocolProfile/Packaging/CompositeList/Encapsulation
Type	container node
Tekstnoder	Ingen
Attributter	id Type: ID Innhold: Intern referanse innen <i>Packaging/CompositeList</i> Bruk: Required mimeparameters Type: string Innhold: F.eks "smime-type="enveloped-data"" Bruk: Required mimetype Type: string Innhold: mime-parameter som forteller om innholdet. F.eks "type=application/pkcs7-mime" for kryptering eller "type=application/x-gzip" for gzip komprimering Bruk: Required
Indre elementer	Constituent

3.3.1.3.2.1.1 Constituent

Constituent inneholder en referanse til et konkret *SimplePart*, *Composite* eller

Encapsulation element hvor den aktuelle meldingen som skal utveksles og versjonen denne har er definert.

Plassering	<i>/CollaborationProtocolProfile/Packaging/CompositeList/Encapsulation/Constituent</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p>idref</p> <p>Type: ID</p> <p>Innhold: Referanse til den aktuelle <i>/CollaborationProtocolProfile/SimplePart</i>, <i>/CollaborationProtocolProfile/Packaging/CompositeList/Composite</i> eller <i>/CollaborationProtocolProfile/Packaging/CompositeList/Encapsulation</i> hvor meldingen er definert</p> <p>Bruk: Required Verdi hentes fra "id" attributtet i <i>SimplePart</i>, <i>Composite</i> eller <i>Encapsulation</i></p>
Indre elementer	Ingen

3.3.1.3.2.2 *Composite*

Det anbefales å definere en forekomst av *Packaging/CompositeList/Composite* (pakke) for hver meldingsversjon. Man bygger et *Composite* (pakke) som inneholder en forekomst av et *Constituent* element for message header, samt et *Constituent* element for den aktuelle versjonen av den melding som skal utveksles.

Plassering	<i>/CollaborationProtocolProfile/Packaging/CompositeList/Composite</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p>id</p> <p>Type: ID</p> <p>Innhold: Intern referanse innen <i>Packaging/CompositeList</i></p> <p>Bruk: Påkrevd</p> <p>mimeparameters</p> <p>Type: string</p> <p>Innhold: Fast verdi = "type=text/xml"</p> <p>Bruk: Påkrevd</p> <p>mimetype</p> <p>Type: string</p> <p>Innhold: Fast verdi = "multipart/related"</p> <p>Bruk: Påkrevd</p>
Indre elementer	Constituent

3.3.1.3.2.2.1 *Constituent*

Constituent inneholder en referanse til et konkret *SimplePart*, *Composite* eller *Encapsulation* element hvor den aktuelle meldingen som skal utveksles og versjonen denne har er definert.

Plassering	<i>/CollaborationProtocolProfile/Packaging/CompositeList/Composite/Constituent</i>
Type	container node
Tekstnoder	Ingen
Attributter	<p><i>idref</i></p> <p>Type: IDREF</p> <p>Innhold: Referanse til den aktuelle <i>/CollaborationProtocolProfile/SimplePart</i>, <i>/CollaborationProtocolProfile/Packaging/CompositeList/Composite</i> eller <i>/CollaborationProtocolProfile/Packaging/CompositeList/Encapsulation</i> hvor meldingen er definert</p> <p>Bruk: Påkrevd Verdi hentes fra "<i>id</i>" attributtet i <i>SimplePart</i>, <i>Composite</i> eller <i>Encapsulation</i></p>
Indre elementer	Ingen

3.3.1.4 *Signature*

Dersom CPP skal signeres så må signaturen(e) ligge i dette elementet. *Signature* i henhold til *cpp-cpa-2_0b.xsd* må ikke forveksles med *ds:Signature* i henhold til *xmldsig-core-schema.xsd*. *Signature* i henhold til *cpp_cpa.xsd* fungerer kun som en container for kryptografisk(e) signatur(er). Dersom *Signature* er til stede i profilen må den inneholde minst en og maks 3 *ds:Signature*. Den som signerer en CPP bør være eieren av profilen og/eller en tiltrodd tredjepart av eieren.

Plassering	<i>/CollaborationProtocolProfile/Signature</i>
Type	container node
Tekstnoder	Ingen
Attributter	Ingen
Indre elementer	<i>ds:Signature</i>

3.3.1.4.1 *ds:Signature*

CPP skal signeres digitalt i overensstemmelse med [XMLDSIG]. Parten eller en tiltrodd tredjepart som opptrer på vegne av parten sitt digitale virksomhetssertifikat skal benyttes.

Hovedtrekkene for generering av innhold i *ds:Signature* i CPP er lik for generering av signatur for ebXML konvolutt slik det er beskrevet i [KITH:1037]. Kun det som er forskjellig er beskrevet her.

3.3.1.4.1.1 *ds:SignatureMethod*

Skal ha verdi:

```
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
```

3.3.1.4.1.2 *ds:Reference*

Det skal kun være en forekomst av *ds:Reference*. Elementet skal referere til CPPen. Følgende transforms skal benyttes:

```
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
```

```
<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

3.4 Opprettelse av CPP

En CPP bør fortrinnsvis skapes/endres ved konfigurering av aktørens systemløsning, for eksempel når systemet implementeres, ved oppgraderinger, eller konfigurasjonsendringer. Eksempler på endringer som skal resultere i ny CPP:

- Sertifikatbytte
- Endringer i endepunktsadresse
- Endringer i støttede meldinger/meldingsversjoner
- Endringer i tjenestestrukturen til organisasjonen

4 Samhandlingsavtale – CPA (Collaboration-Protocol Agreement)

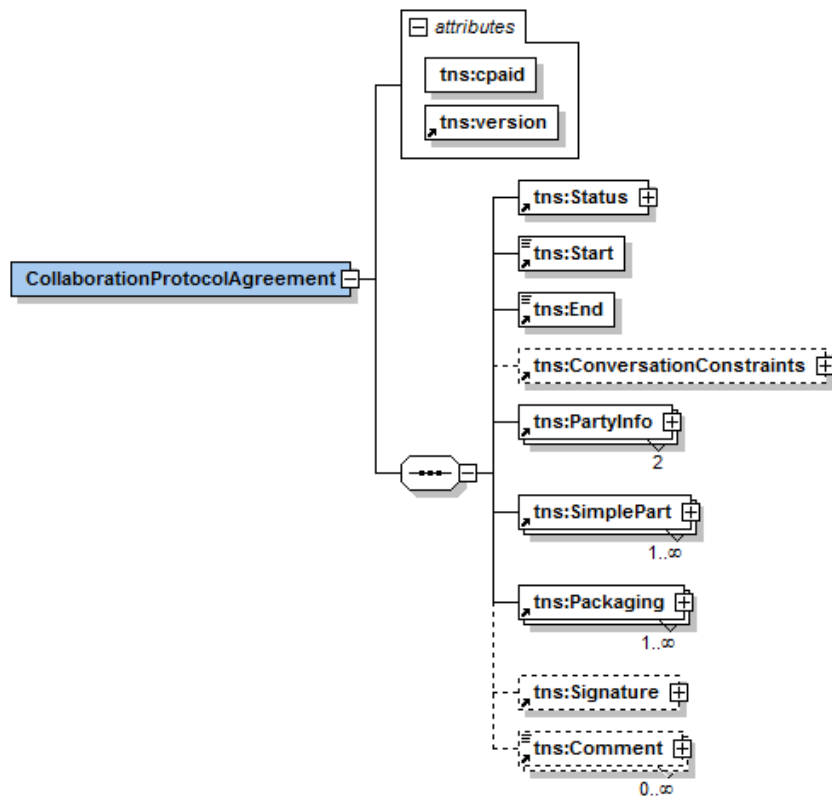
4.1 Hva er en CPA

En CPA er et XML-dokument som beskriver den faktiske meldingsutveksling som kan skje mellom to aktører og de konkrete kommunikasjonsparametere som skal benyttes i denne meldingsutvekslingen. En CPA representerer snittet av de to aktørenes CPPer, dvs. det som er felles, og kan etableres på grunnlag av aktørenes publiserte CPPer.

Hovedelementene i en CPA er følgende:

- De to aktørenes identiteter (f.eks. HER-id)
- Hvilke prosesser samhandlingen gjelder for (for eksempel utveksling av en elektronisk sykmelding mellom lege og NAV)
- Hvilke meldinger og meldingsversjoner man kan sende og/eller motta
- Hvilke roller aktørene kan inneha i de aktuelle prosessene
- Hvilket tidsrom avtalen gjelder for
- Kommunikasjonskanaler, protokoller og tilhørende parametere
- Sikkerhet, signaturer og hvilke type sertifikater som skal benyttes
- Pakking av filer (hvordan filene skal settes sammen av header, payload, sikkerhet osv.)

CPA er egnet for høyfrekvent kommunikasjon eller der hvor man ønsker en økt sikkerhet, f.eks. ved forhåndsgodkjenning av kommunikasjonspartnere. Aktørenes applikasjoner kan konfigureres opp ved hjelp av en CPA.



Figur 3: CPA - Collaboration-Protocol Agreement

4.2 Tolking av en mottatt CPA

CPAen inneholder mye informasjon og dette kapitlet beskriver hva minstekravet er for bruk av informasjon fra CPA for å kunne sende og motta meldinger over *ebXML*.

4.2.1 *CollaborationProtocolAgreement* og *cpaid*

Fra *CollaborationProtocolAgreement* elementet hentes et Påkrevd *cpaid* attributt som er en unik id for dokumentet. Verdien av *cpaid* settes av den aktøren som genererer CPAen og brukes av begge som identifikasjon i meldingsutvekslingen.

cpaid skal være en URI, slik det er anbefalt fra OASIS. Hvilke verdier *cpaid* skal settes sammen av er nærmere beskrevet i dokumentet "Rammeverk for elektronisk meldingsutveksling i helsevesenet" utgitt av KITH [[KITH:1037](#)].

Verdien i *cpaid* attributtet skal brukes som verdien av *CPAId* elementet i en *ebXML* Message Header for bruk i henhold til *ebXML* Messaging 2.0 standarden. Verdien av *cpaid* skal være unik og en ny CPA skal alltid ha en ny *cpaid*.

4.2.2 CPA Gyldighetstid

Gyldigheten av en CPA er gitt av *Start* og *End* elementene. Disse ser slik ut:

```
<tp:Start>2009-11-26T14:26:21Z</tp:Start>  
<tp:End>2011-04-16T09:16:08Z</tp:End>
```

Hvis startdatoen settes til tidspunktet for opprettelsen av CPA eller tidligere, betyr dette at den kan tas i bruk umiddelbart. Hvis startdatoen er fram i tid kan CPA leses inn umiddelbart, men ikke tas i bruk før det tidspunktet som er angitt i *Start* elementet. Dette kan være relevant både ved sertifikatbytter eller ved innføring av nye meldinger som ikke skal tas i bruk før på et gitt tidspunkt. Sluttdatoen, tidspunktet angitt i *End* elementet, bør ikke være senere enn tidspunktet for utløpsdato i det sertifikatet som går ut først av partenes sertifikater.

NB! Når sluttdato er nådd skal CPAen og tilhørende cpaid ikke lenger benyttes!

Det vil være behov for å ha overlappende gyldighetsperioder på CPAer med tanke på sertifikatbytter eller e-postadressebytte.

I noen tilfeller vil det også være behov for å tilbakekalle en CPA med én gang en ny CPA er utstedt.

Per nå er det ikke laget regler for hvordan man skal tilbakekalle en CPA som allerede er utstedt.

4.2.3 PartyInfo

Det finnes en *PartyInfo* struktur for hver av de to kommunikasjonspartene i en CPA.

4.2.3.1 partyName

Dette er partens navn i dagligtale på menneskelesbar form. *partyName* skal ikke tas med i ebXML konvolutten.

4.2.3.2 PartyId

I all ebXML kommunikasjon over Norsk Helsenett, skal det kun brukes HER-id for å identifisere aktøren, *PartyId type="HER"*. Enhver fravikelse av denne regelen skal dokumenteres og grunngis.

For aktører som ikke kommuniserer over Norsk Helsenett kan ENH benyttes for å identifisere aktøren, *PartyId type="ENH"*.

PartyId skal benyttes i ebXML konvolutten i en ebXML forsendelse.

4.2.3.3 PartyRef

En rolle i en prosess (tjeneste), f.eks. Utleverer, kan bestå av flere ulike aktørgrupper, eks. Bandasjist og Apotek. I de tilfeller det er behov for å skille de ulike aktørgruppene fra hverandre til tross for at de innehar samme aktive rollen kan *PartyRef* benyttes. Elementet har ingen spesiell betydning i en CPA, men kan benyttes av aktører som beskrevet ovenfor. Det anbefales at man benytter en beskrivende URL som verdi i elementet.

Eksempel:

```
<tp:PartyRef xlink:href="http://reseptformidleren.no/eResept/rekvirent" />
<tp:PartyRef xlink:href="http://reseptformidleren.no/eResept/apotek" />
<tp:PartyRef xlink:href="http://reseptformidleren.no/eResept/bandasjist" />
```

4.2.3.4 CollaborationRole[n]

Her angis partens forhold til en gitt tjeneste.

Det kan være flere *CollaborationRole* for hver part i en CPA. For hver *CollaborationRole* er det gitt en *Role* og en *Service*.

Merk!

eResept har etablert synkron meldingsutveksling ved bruk av Webservice og for disse utvekslingene benyttes det ikke CPA. De CollaborationRole som gjelder for eResept sine synkrone meldingsutvekslinger kan imidlertid beholdes når ny CPP dannes. Den som er ansvarlig for å danne CPA på bakgrunn av CPP vil utelate de synkrone meldingsutvekslingene som gjelder for eResept når den nye CPAen dannes.

Evt. overflødige Packaging og SimplePart elementer som en følge av dette vil også utelates i den nye CPAen.

4.2.3.4.1 *Role*

Den aktive rollen parten spiller i den aktuelle tjenesten. Denne skal benyttes i *ebXML* konvolutten i en *ebXML* forsendelse.

4.2.3.4.2 *Service*

Selve tjenesten man benytter, eks. *eResept* eller *HarBorgerEgenandelFritak*. *Service* skal benyttes i *ebXML* konvolutten i en *ebXML* forsendelse.

4.2.3.4.3 *Action [m]*

Handlingen som utføres i denne meldingsutvekslingen til denne tjenesten, eks. *Rekvirering* eller *EgenandelForesporsel*.

Det kan være flere *Action* for hver tjeneste. *Action* skal benyttes i *ebXML* konvolutten i en *ebXML* forsendelse.

4.2.3.5 *TransportSender*

De parameterne som avsender benytter i sin kommunikasjon med mottaker angis i *TransportSender*.

4.2.3.5.1 *Protokoll*

Protokollen som det er besluttet å benytte i utvekslingen, kan være enten *SMTP*, *HTTP* eller *FTP*.

4.2.3.6 *TransportReceiver*

Kommunikasjonsparametrene som mottaker benytter i sin kommunikasjon med avsender angis i *TransportReceiver*.

4.2.3.6.1 *Protokoll*

Protokollen som det er besluttet å benytte i utvekslingen, kan være enten *SMTP*, *HTTP* eller *FTP*.

4.2.3.6.2 *Endpoint*

Her angis adressen som skal benyttes for denne meldingsutvekslingen. *Endpoint* kan være enten en e-post adresse (kjent som edi-adresse) eller en *HTTP* adresse.

Endpoint skal ikke med i *ebXML* konvolutten, men angir hvor *ebXML*-meldingen skal leveres.

4.2.3.7 *SimplePart*

I *NamespaceSupported* elementet under *SimplePart* finner man referanser til den melding (xsd) de nevnte komponenter inneholder. Se 3.3.1.2 for detaljer om syntaks og datainnhold.

4.2.3.8 *Packaging*

I *Packaging*-elementet finner man hvordan filene er satt sammen, samt om payload skal krypteres og/eller komprimeres.

Hvis filen er kryptert og/eller komprimert vil dette være angitt i et *Constituent*-element som ligger under *Packaging/CompositeList/Encapsulation*. Hvis ikke filen er kryptert og/eller komprimert, vil referansen til *SimplePart* være angitt i *Constituent*-elementet som ligger under *Packaging/CompositeList/Composite*.

Det bør være definert en instans av *Packaging/CompositeList/Composite*, evt. med tilhørende *Packaging/CompositeList/Encapsulation*, som skal ha underliggende *Constituent*-element, for hver meldingsversjon.

For å lese et *Packaging*-element starter man nederst i strukturen hvor det ytterste elementet er definert og leser seg oppover i strukturen hvor man til slutt refererer til den tilhørende *SimplePart* (selve meldingen (xsd)):

- Nederst i strukturen er det definert et *Composite* element som er selve ebMS-meldingen som utveksles. *Composite* elementet består av en ebXML-header (*msg_header*) og den krypterte, pakke fagmeldingen (f.eks. *msg_ERM18_v2p4r1*).
- Hvis den pakke fagmeldingen er kryptert vil det være definert et *Encapsulation* element hvor fagmeldingen (f.eks. *enc_ERM18_v2p4r1*) dekrypteres med PKCS7.
- Hvis meldingen er komprimert er den pakket med f.eks. gzip (f.eks. *zip_ERM18_v2p4r1*)
- Videre refereres det til den tilhørende *SimplePart* hvor fagmeldingen er referert (f.eks. *message_ERM18_v2p4r1*).

På denne måten har man en konsis, entydig og oversiktlig beskrivelse av det som skjer med meldingen M18 fra den er mottatt til den kan videresendes til fagapplikasjonen. Om man tolker dette maskinelt eller bare benytter dette som dokumentasjon er implementasjonsavhengig.

4.2.3.9 *Comment*

Dersom en samhandlingsavtale (CPA) er opprettet på bakgrunn av en CPP, skal cppid dokumenteres ved hjelp av *Comment* elementet i CPA.

Innholdet i *Comment* kan være tekst på formen "*Basert på CPP XXXXXX og YYYYYY*" der XXXXXX og YYYYYY typisk vil være partenes CPP-id'er.

4.2.3.10 *Sertifikat*

Sertifikatet som skal benyttes til å signere ebXML kommunikasjonen for hver part.

Krypteringssertifikat skal angis for hver part.

Når et sertifikat er definert i en CPA skal kun dette sertifikatet benyttes.

4.3 **Sammenfletting av to CPP til en CPA**

Sammenfletting av 2 partnerprofiler (CPP) til en samhandlingsavtale (CPA) skal

gjøres i henhold til OASIS' standard for CPP/CPA, "*Collaboration-Protocol Profile and Agreement Specification, version 2.0*" (<http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf>).

4.4 Mottak av en CPA

Mottatt CPA må kunne leses av mottaker. MSH oppdateres basert på innholdet av mottatt CPA.

Følgende informasjon skal kunne leses ut av en CPA:

- cpaid="xxx:yyy:zzz"
- Den andre partens signeringssertifikat
- Den andre partens krypteringssertifikat
- CPA Startdato
- CPA Enddato
- Begge parters PartyId
- En eller flere NamespaceSupported elementer

5 Referanser

I arbeidet med å utvikle denne spesifikasjonen er det referert til følgende dokumenter:

[DSIG]	XML-Signature Syntax and Processing, W3C Anbefaling 12. februar 2002 http://www.w3.org/TR/xmlsig-core/ http://www.ietf.org/rfc/rfc3275.txt
[ebBPSS]	ebXML Business Process Specification Schema Version 1.01 http://www.ebxml.org/specs/ebBPSS.pdf
[EBMS]	OASIS og UN/CEFACT: ebXML Message Service Specification. Versjon 2.0. http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf XML Schema for konvolutten: ebXML SOAP Extension Elements Schema http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
[EBCPP]	OASIS og UN/CEFACT: Collaboration-Protocol Profile and Agreement Specification Version 2.0, http://www.oasis-open.org/committees/download.php/204/ebcpp-2.0.pdf
[EBXML]	ebXML: http://www.ebxml.org/
[ENV]	CEN: ENV 13608-2: Health informatics – Security for healthcare communication Part 2: Secure data objects.
[ENV2]	CEN: ENV 13608-3: Health informatics – Security for healthcare communication Part 3: Secure data channels
[SOAP]	W3C SOAP 1.1 http://www.w3.org/TR/SOAP/ XML Schema: http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
[SOAPAttach]	SOAP Messages with Attachments, John J. Barton, Hewlett Packard Labs; Satish Thatte and Henrik Frystyk Nielsen, Microsoft, Published Oct 09 2000 2777 http://www.w3.org/TR/2000/NOTE-SOAP-attachments-20001211
[XML]	Extensible Markup Language (XML) 1.0 (Second Edition) http://www.w3.org/TR/2000/REC-xml-20001006
[XMLS]	XML Schema Part 0: Primer: http://www.w3.org/TR/xmlschema-0/ Part 1: Structures: http://www.w3.org/TR/xmlschema-1/ Part 2: Datatypes: http://www.w3.org/TR/xmlschema-2/
[XMLDSIG]	Joint W3C/IETF XML-Signature Syntax and Processing specification: http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/
[NSAM]	Nasjonal samhandlingsarkitektur. KITH-notat 29.03.06.
[KITH:1037]	Rammeverk for elektronisk meldingsutveksling i helsevesenet, http://www.kith.no/upload/6390/KITH_1037-2011_RammeverkForMeldingsutveksling-v1_1.pdf

[KITH:1029]	Adresseopplysninger i nasjonale meldingsstandarder, http://www.kith.no/upload/6392/KITH-1029-2011-AdresseopplysningerNasjonaleMeldingsstandarder.pdf
-------------	--

Tillegg A: XML struktur og eksempel

En viktig funksjon for CPP er å uttrykke hvilke meldingsversjoner en kommunikasjonspart kan utveksle med andre aktører. Prinsipper for hvordan XML strukturen i CPP skal bygges opp, for å beskrive hvilke meldingsversjoner kommunikasjonsparten støtter, er beskrevet i kapittel 3.3.1.3 Packaging. Dette tillegget utdyper den beskrivelsen, og viser ett konkret eksempel på en CPP.

Informasjonen om hvilke meldinger som støttes i hvilke Service/Action/Roles defineres i tre elementer som lenkes sammen ved hjelp av id'er:

- CollaborationRole
- Packaging
- SimplePart

SimplePart

SimplePart angir ett konkret namespace som kan refereres av et eller flere Packaging element. Hvis meldingstypen benytter hodemelding angis både Hodemeldingsnamespace og namespace for den konkrete fagmeldingen.

Packaging

Packaging angir hvordan SimplePart elementer skal settes sammen til en konkret meldingsinstans. Komprimering og kryptering angis i Encapsulation. Sammensetning av meldingskonvolutt og pakket/krypterte data angis i Composite elementet. Man kan bare pakke en versjon av XML-meldinger i ett Packaging element.

CollaborationRole

I CollaborationRole knyttes Service, Action og Role som en aktør kan fylle i prosess sammen med sending eller mottak (CanSend/CanRecieve) av en forhåndsdefinert pakke (Package) som igjen angir meldingsversjon gjennom SimplePart. Hver CollaborationRole kan bare bestå av en aktuell versjon av meldinger (Packages).

CollaborationRole vil vanligvis bestå av ett meldingspar i form av en CanSend og en CanRecieve, vanligvis en fagmelding og tilhørende versjon av applikasjonskvittering. I mer kompliserte prosesser kan en CollaborationRole også inneholde henvisning til andre meldinger (se eksempel).

Det skal ikke defineres flere CanSend/CanRecieve som henviser til forskjellige versjoner av samme melding i en CollaborationRole Dette for å definere entydig hva slags meldingsversjoner enhver aktør støtter.

CollaborationRole i CPA

ServiceBinding elementet definerer knytningen mellom en Action og hvilke meldingspakker/versjoner som kan sendes/mottak (gjennom CanSend og CanRecieve). En CPP kan inneholde mange CollaborationRoles som knytter samme Service/Action par til forskjellige versjoner av fagmeldingene på denne måten. Den resulterende CPA'en vil imidlertid bare inneholde èn binding mellom den aktuelle Service/Action og meldingsversjonen. To kommunikasjonsparter kan med andre ord bare avtale å sende en versjon av meldingen seg i mellom. Dette er viktig fordi en del fagsystem er avhengig av at kombinasjonen Service/Action er unik innenfor en CPA. Legg også merke til at Action vanligvis vil følge kodeverk 8279, meldingens funksjon.

CPP struktur eksempel

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:CollaborationProtocolProfile xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:tns="http://www.oasis-
open.org/committees/ebxml-cppa/schema/cpp-cpa-2_0.xsd" xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" tns:cppid="cpp-nhn-eks" tns:version="string"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-cppa/schema/cpp-cpa-2_0.xsd cpp-cpa-2_0.xsd">
  <tns:PartyInfo tns:partyName="PARTYNAME" tns:defaultMshChannelId="asyncSMTPChannelA2"
tns:defaultMshPackageId="package_mshsignal">
    <tns:PartyId tns:type="HER">HERID</tns:PartyId>
    <tns:PartyId tns:type="ENH">ORGNR</tns:PartyId>
    <tns:PartyId tns:type="orgnummer">ORGNR</tns:PartyId>
    <tns:PartyRef xlink:href="https://www.nav.no/about.html" xlink:type="simple"/>
  </tns:PartyInfo>
  <tns:CollaborationRole>
    <!-- v2p4r1 -->
    <tns:ProcessSpecification tns:name="Reseptoppgjor" tns:version="2.4.1"
xlink:href="http://www.helsedirektoratet.no/processes/eResept.xml" xlink:type="simple" tns:uuid="9584df74-571a-487f-bc5c-
jj438sg294bd"/>
    <tns:Role tns:name="Utleverer" xlink:href="http://www.helsedirektoratet.no/processes#Utleverer" xlink:type="simple"/>
    <tns:ApplicationCertificateRef tns:certId="default_crypt_cert"/>
    <tns:ServiceBinding>
      <tns:Service tns:type="string">OppgjorsKontroll</tns:Service>
      <tns:CanSend>
        <tns:ThisPartyActionBinding tns:action="Oppgjorskrav" tns:id="Oppgjorskrav1"
tns:packageId="package_oppgjorskrav_v2p4r1" xlink:type="simple">
          <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
          <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
        </tns:ThisPartyActionBinding>
      </tns:CanSend>
      <tns:CanSend>
        <tns:ThisPartyActionBinding tns:action="Svarmelding" tns:id="Reseptoppgjor_Svarmelding1"
tns:packageId="package_apprec_v1p0" xlink:type="simple">
          <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
          <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
        </tns:ThisPartyActionBinding>
      </tns:CanSend>
      <tns:CanReceive>
        <tns:ThisPartyActionBinding tns:action="Oppgjorsresultat" tns:id="Oppgjorsresultat1"
tns:packageId="package_oppgjorsresultat_v2p4r1" xlink:type="simple">
          <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
          <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
        </tns:ThisPartyActionBinding>
      </tns:CanReceive>
      <tns:CanReceive>
        <tns:ThisPartyActionBinding tns:action="Utbetaling" tns:id="Utbetaling1"
tns:packageId="package_utbetaling_v2p4r1" xlink:type="simple">
          <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
          <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
        </tns:ThisPartyActionBinding>
      </tns:CanReceive>
      <tns:CanReceive>
        <tns:ThisPartyActionBinding tns:action="Svarmelding" tns:id="Bekreftelse1"
tns:packageId="package_apprec_v1p0" xlink:type="simple">
          <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
          <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
        </tns:ThisPartyActionBinding>
      </tns:CanReceive>
    </tns:ServiceBinding>
  </tns:CollaborationRole>
  <tns:CollaborationRole>
    <!-- v2p5 -->
    <tns:ProcessSpecification tns:name="Reseptoppgjor" tns:version="2.5"
xlink:href="http://www.helsedirektoratet.no/processes/eResept.xml" xlink:type="simple" tns:uuid="9584df74-571a-487f-bc5c-
jj438sg294bd"/>
  </tns:CollaborationRole>
</tns:CollaborationProtocolProfile>
```

```

<tns:Role tns:name="Utleverer" xlink:href="http://www.helsedirektoratet.no/processes#Utleverer" xlink:type="simple"/>
<tns:ApplicationCertificateRef tns:certId="default_crypt_cert"/>
<tns:ServiceBinding>
  <tns:Service tns:type="string">OppgjorsKontroll</tns:Service>
  <tns:CanSend>
    <tns:ThisPartyActionBinding tns:action="Oppgjorskrav" tns:id="Oppgjorskrav5"
tns:packageId="package_oppgjorskrav_v2p5" xlink:type="simple">
      <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
      <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
    </tns:ThisPartyActionBinding>
  </tns:CanSend>
  <tns:CanSend>
    <tns:ThisPartyActionBinding tns:action="Svarmelding" tns:id="Reseptoppgjor_Svarmelding5"
tns:packageId="package_apprec_v1p0" xlink:type="simple">
      <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
      <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
    </tns:ThisPartyActionBinding>
  </tns:CanSend>
  <tns:CanReceive>
    <tns:ThisPartyActionBinding tns:action="Oppgjorsresultat" tns:id="Oppgjorsresultat5"
tns:packageId="package_oppgjorsresultat_v2p5" xlink:type="simple">
      <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
      <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
    </tns:ThisPartyActionBinding>
  </tns:CanReceive>
  <tns:CanReceive>
    <tns:ThisPartyActionBinding tns:action="Utbetaling" tns:id="Utbetaling5"
tns:packageId="package_utbetaling_v2p5" xlink:type="simple">
      <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
      <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
    </tns:ThisPartyActionBinding>
  </tns:CanReceive>
  <tns:CanReceive>
    <tns:ThisPartyActionBinding tns:action="Svarmelding" tns:id="Bekreftelse5"
tns:packageId="package_apprec_v1p0" xlink:type="simple">
      <tns:BusinessTransactionCharacteristics tns:isAuthenticated="none" tns:isAuthorizationRequired="false"
tns:isConfidential="none" tns:isIntelligibleCheckRequired="false" tns:isNonRepudiationReceiptRequired="true"
tns:isNonRepudiationRequired="true" tns:isTamperProof="none" tns:timeToPerform="P180M"/>
      <tns:ChannelId>asyncSMTPChannelA2</tns:ChannelId>
    </tns:ThisPartyActionBinding>
  </tns:CanReceive>
</tns:ServiceBinding>
</tns:CollaborationRole>
<tns:Certificate tns:certId="default_sign_cert">
  <ds:KeyInfo>
    <ds:X509Data>
      <!-- <ds:X509Certificate>${cpp.certificate.nonrep}</ds:X509Certificate> -->
      <ds:X509Certificate>NONREPSERTIFIKATIB64</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</tns:Certificate>
<tns:Certificate tns:certId="default_crypt_cert">
  <ds:KeyInfo>
    <ds:X509Data>
      <!-- <ds:X509Certificate>${cpp.certificate.crypt}</ds:X509Certificate> -->
      <ds:X509Certificate>CONFIDSERTIFIKATIB64</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</tns:Certificate>
<tns:Certificate tns:certId="default_ssl_cert">
  <ds:KeyInfo>
    <ds:X509Data>
      <!-- <ds:X509Certificate>${cpp.certificate.ssl}</ds:X509Certificate> -->
      <ds:X509Certificate>SSLSERTIFIKATIB64</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</tns:Certificate>
<tns:SecurityDetails tns:securityId="trustAnchorsAndPolicy"/>

```

```

<tns:DeliveryChannel tns:channelId="asyncSMTPChannelA2" tns:docExchangeId="docexchange_smtp_eresept"
tns:transportId="transportSMTP_eresept">
  <tns:MessagingCharacteristics tns:ackRequested="always" tns:ackSignatureRequested="perMessage"
tns:duplicateElimination="perMessage" tns:syncReplyMode="none"/>
</tns:DeliveryChannel>
<tns:Transport tns:transportId="transportSMTP_eresept">
  <tns:TransportSender>
    <tns:TransportProtocol tns:version="1.1">SMTP</tns:TransportProtocol>
  </tns:TransportSender>
  <tns:TransportReceiver>
    <tns:TransportProtocol tns:version="1.1">SMTP</tns:TransportProtocol>
    <tns:Endpoint tns:type="allPurpose" tns:uri="mailto://EPOSTADRESSE"/>
    <!-- <tns:Endpoint tns:type="allPurpose" tns:uri="{cpp.endpoint.smtp.eresept}"/> -->
  </tns:TransportReceiver>
</tns:Transport>
<tns:DocExchange tns:docExchangeId="docexchange_smtp_eresept">
  <tns:ebXMLSenderBinding tns:version="2.0">
    <tns:ReliableMessaging>
      <tns:Retries>4</tns:Retries>
      <tns:RetryInterval>PT240M</tns:RetryInterval>
      <tns:MessageOrderSemantics>NotGuaranteed</tns:MessageOrderSemantics>
    </tns:ReliableMessaging>
    <tns:PersistDuration>P2D</tns:PersistDuration>
    <tns:SenderNonRepudiation>
      <tns:NonRepudiationProtocol
tns:version="string">http://www.w3.org/2000/09/xmldsig#</tns:NonRepudiationProtocol>
      <tns:HashFunction>http://www.w3.org/2000/09/xmldsig#sha1</tns:HashFunction>
      <tns:SignatureAlgorithm tns:oid="1.2.840.113549.1.1.5" tns:w3c="http://www.w3.org/2000/09/xmldsig#rsa-
sha1">RSA-SHA1</tns:SignatureAlgorithm>
      <tns:SigningCertificateRef tns:certId="default_sign_cert"/>
    </tns:SenderNonRepudiation>
  </tns:ebXMLSenderBinding>
  <tns:ebXMLReceiverBinding tns:version="2.0">
    <tns:ReliableMessaging>
      <tns:Retries>4</tns:Retries>
      <tns:RetryInterval>PT240M</tns:RetryInterval>
      <tns:MessageOrderSemantics>NotGuaranteed</tns:MessageOrderSemantics>
    </tns:ReliableMessaging>
    <tns:PersistDuration>P2D</tns:PersistDuration>
    <tns:ReceiverNonRepudiation>
      <tns:NonRepudiationProtocol
tns:version="string">http://www.w3.org/2000/09/xmldsig#</tns:NonRepudiationProtocol>
      <tns:HashFunction>http://www.w3.org/2000/09/xmldsig#sha1</tns:HashFunction>
      <tns:SignatureAlgorithm tns:oid="1.2.840.113549.1.1.5" tns:w3c="http://www.w3.org/2000/09/xmldsig#rsa-
sha1">RSA-SHA1</tns:SignatureAlgorithm>
    </tns:ReceiverNonRepudiation>
  </tns:ebXMLReceiverBinding>
</tns:DocExchange>
</tns:PartyInfo>
<tns:SimplePart tns:id="msg_header" tns:mimetype="application/xml">
  <tns:NamespaceSupported tns:location="msg-header-2_0.xsd" tns:version="2.0">http://www.oasis-
open.org/committees/ebxml-msg/schema</tns:NamespaceSupported>
</tns:SimplePart>
<tns:SimplePart tns:id="message_apprec_v1p0" tns:mimetype="application/xml">
  <tns:NamespaceSupported tns:location="AppRec-v1-2004-11-21.xsd"
tns:version="1.0">http://www.kith.no/xmlstds/apprec/2004-11-21</tns:NamespaceSupported>
</tns:SimplePart>
<tns:SimplePart tns:id="message_erm18_v2p4r1" tns:mimetype="application/xml">
  <tns:NamespaceSupported tns:location="MsgHead-v1_2.xsd" tns:version="1.2">http://www.kith.no/xmlstds/msghead/2006-05-
24</tns:NamespaceSupported>
  <tns:NamespaceSupported tns:location="ER-M18-2010-10-01.xsd"
tns:version="2.4.1">http://www.kith.no/xmlstds/eresept/m18/2010-10-01</tns:NamespaceSupported>
</tns:SimplePart>
<tns:SimplePart tns:id="message_erm18_v2p5" tns:mimetype="application/xml">
  <tns:NamespaceSupported tns:location="MsgHead-v1_2.xsd" tns:version="1.2">http://www.kith.no/xmlstds/msghead/2006-05-
24</tns:NamespaceSupported>
  <tns:NamespaceSupported tns:location="ER-M18-2013-04-16.xsd"
tns:version="2.5">http://www.kith.no/xmlstds/eresept/m18/2013-04-16</tns:NamespaceSupported>
</tns:SimplePart>
<tns:SimplePart tns:id="message_erm22_v2p4r1" tns:mimetype="application/xml">
  <tns:NamespaceSupported tns:location="MsgHead-v1_2.xsd" tns:version="1.2">http://www.kith.no/xmlstds/msghead/2006-05-
24</tns:NamespaceSupported>
  <tns:NamespaceSupported tns:location="ER-M22-2006-10-06.xsd"
tns:version="2.4.2">http://www.kith.no/xmlstds/eresept/m22/2006-10-06</tns:NamespaceSupported>
</tns:SimplePart>
<tns:SimplePart tns:id="message_erm22_v2p5" tns:mimetype="application/xml">

```

```

    <tns:NamespaceSupported tns:location="MsgHead-v1_2.xsd" tns:version="1.2">http://www.kith.no/xmlstds/msghead/2006-05-
24</tns:NamespaceSupported>
    <tns:NamespaceSupported tns:location="ER-M22-2006-10-06.xsd"
tns:version="2.5">http://www.kith.no/xmlstds/eresept/m22/2006-10-06</tns:NamespaceSupported>
    </tns:SimplePart>
    <tns:SimplePart tns:id="message_erm23_v2p4r1" tns:mimetype="application/xml">
    <tns:NamespaceSupported tns:location="MsgHead-v1_2.xsd" tns:version="1.2">http://www.kith.no/xmlstds/msghead/2006-05-
24</tns:NamespaceSupported>
    <tns:NamespaceSupported tns:location="ER-M23-2006-10-06.xsd"
tns:version="2.4.1">http://www.kith.no/xmlstds/eresept/m23/2006-10-06</tns:NamespaceSupported>
    </tns:SimplePart>
    <tns:SimplePart tns:id="message_erm23_v2p5" tns:mimetype="application/xml">
    <tns:NamespaceSupported tns:location="MsgHead-v1_2.xsd" tns:version="1.2">http://www.kith.no/xmlstds/msghead/2006-05-
24</tns:NamespaceSupported>
    <tns:NamespaceSupported tns:location="ER-M23-2006-10-06.xsd"
tns:version="2.5">http://www.kith.no/xmlstds/eresept/m23/2006-10-06</tns:NamespaceSupported>
    </tns:SimplePart>
    <tns:Packaging tns:id="package_mshsignal">
    <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
    <tns:CompositeList>
    <tns:Composite tns:id="msh_signal" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
    <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
    </tns:Composite>
    </tns:CompositeList>
    </tns:Packaging>
    <tns:Packaging tns:id="package_apprec_v1p0">
    <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
    <tns:CompositeList>
    <tns:Encapsulation tns:id="enc_apprec_v1p0" tns:mimetype="application/pkcs7-mime" tns:mimeparameters="smime-
type=&quot;enveloped-data&quot;">
    <tns:Constituent tns:idref="message_apprec_v1p0" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Composite tns:id="msg_apprec_v1p0" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
    <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
    <tns:Constituent tns:idref="enc_apprec_v1p0" tns:excludedFromSignature="false"/>
    </tns:Composite>
    </tns:CompositeList>
    </tns:Packaging>
    <tns:Packaging tns:id="package_oppgjorskrav_v2p4r1">
    <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
    <tns:CompositeList>
    <tns:Encapsulation tns:id="zip_erm18_v2p4r1" tns:mimetype="application/x-gzip"
tns:mimeparameters="type=application/x-gzip">
    <tns:Constituent tns:idref="message_erm18_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Encapsulation tns:id="enc_erm18_v2p4r1" tns:mimetype="application/pkcs7-mime" tns:mimeparameters="smime-
type=&quot;enveloped-data&quot;">
    <tns:Constituent tns:idref="zip_erm18_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Composite tns:id="msg_erm18_v2p4r1" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
    <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
    <tns:Constituent tns:idref="enc_erm18_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Composite>
    </tns:CompositeList>
    </tns:Packaging>
    <tns:Packaging tns:id="package_oppgjorskrav_v2p5">
    <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
    <tns:CompositeList>
    <tns:Encapsulation tns:id="zip_erm18_v2p5" tns:mimetype="application/x-gzip" tns:mimeparameters="type=application/x-
gzip">
    <tns:Constituent tns:idref="message_erm18_v2p5" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Encapsulation tns:id="enc_erm18_v2p5" tns:mimetype="application/pkcs7-mime" tns:mimeparameters="smime-
type=&quot;enveloped-data&quot;">
    <tns:Constituent tns:idref="zip_erm18_v2p5" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Composite tns:id="msg_erm18_v2p5" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
    <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
    <tns:Constituent tns:idref="enc_erm18_v2p5" tns:excludedFromSignature="false"/>
    </tns:Composite>
    </tns:CompositeList>
    </tns:Packaging>
    <tns:Packaging tns:id="package_oppgjorsresultat_v2p4r1">
    <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
    <tns:CompositeList>

```

```

    <tns:Encapsulation tns:id="enc_erm22_v2p4r1" tns:mimetype="application/pkcs7-mime" tns:mimeparameters="smime-
type=&quot;enveloped-data&quot;">
      <tns:Constituent tns:idref="message_erm22_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Composite tns:id="msg_erm22_v2p4r1" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
      <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
      <tns:Constituent tns:idref="enc_erm22_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Composite>
  </tns:CompositeList>
</tns:Packaging>
<tns:Packaging tns:id="package_oppgjorsresultat_v2p5">
  <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
  <tns:CompositeList>
    <tns:Encapsulation tns:id="enc_erm22_v2p5" tns:mimetype="application/pkcs7-mime" tns:mimeparameters="smime-
type=&quot;enveloped-data&quot;">
      <tns:Constituent tns:idref="message_erm22_v2p5" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Composite tns:id="msg_erm22_v2p5" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
      <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
      <tns:Constituent tns:idref="enc_erm22_v2p5" tns:excludedFromSignature="false"/>
    </tns:Composite>
  </tns:CompositeList>
</tns:Packaging>
<tns:Packaging tns:id="package_utbetalings_v2p4r1">
  <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
  <tns:CompositeList>
    <tns:Encapsulation tns:id="enc_erm23_v2p4r1" tns:mimetype="application/pkcs7-mime" tns:mimeparameters="smime-
type=&quot;enveloped-data&quot;">
      <tns:Constituent tns:idref="message_erm23_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Composite tns:id="msg_erm23_v2p4r1" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
      <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
      <tns:Constituent tns:idref="enc_erm23_v2p4r1" tns:excludedFromSignature="false"/>
    </tns:Composite>
  </tns:CompositeList>
</tns:Packaging>
<tns:Packaging tns:id="package_utbetalings_v2p5">
  <tns:ProcessingCapabilities tns:generate="true" tns:parse="true"/>
  <tns:CompositeList>
    <tns:Encapsulation tns:id="enc_erm23_v2p5" tns:mimetype="application/pkcs7-mime" tns:mimeparameters="smime-
type=&quot;enveloped-data&quot;">
      <tns:Constituent tns:idref="message_erm23_v2p5" tns:excludedFromSignature="false"/>
    </tns:Encapsulation>
    <tns:Composite tns:id="msg_erm23_v2p5" tns:mimeparameters="type=text/xml" tns:mimetype="multipart/related">
      <tns:Constituent tns:idref="msg_header" tns:excludedFromSignature="false"/>
      <tns:Constituent tns:idref="enc_erm23_v2p5" tns:excludedFromSignature="false"/>
    </tns:Composite>
  </tns:CompositeList>
</tns:Packaging>
<tns:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Signature>
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue/>
      </Reference>
    </SignedInfo>
    <SignatureValue/>
  </Signature>
</tns:Signature>
<tns:Comment xml:lang="no">Skal erstatte tidligere CPA med cpaid XXXXXX</tns:Comment>
</tns:CollaborationProtocolProfile>

```



Helsedirektoratet

Pb. 7000 St Olavs plass, 0130 Oslo

Tlf.: 810 20 050

Faks: 24 16 30 01

www.helsedirektoratet.no

