Direktoratet for e-helse

AMQP spesifikasjon

Spesifikasjon av meldingsutveksling med helsenorge.no

[Rapportnummer]

Kolofon

Publikasjonens tittel:
AMQP spesifikasjon helsenorge.no

Utgitt:
[Sett inn dato]

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Postadresse:
Postboks 6737 St. Olavs plass, 0130 OSLO

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70
www.ehelse.no

Rapporten kan lastes ned på:
www.ehelse.no

Forord

Dette dokumentet inneholder spesifikasjon av meldingsutveksling med helsenorge.no basert på den internasjonale standarden AMQP. Dokumentet etablerer en profil for bruk av AMQP og spesifiserer krav til feilhåndtering.

Innhold

Dokumenthistorikk 5

1 Meldingsutveksling helsenorge.no 6

1.1 Synkrone tjenester 6

1.2 Asynkrone tjenester 6

2 AMQP Meldingsutveksling 7

2.1 AMQP Profil 8

2.2 AMQP Feilhåndtering 14

3 PKI-sjekkliste 23

3.1 Asynkron, send melding 23

3.2 Asynkron, motta melding 24

3.3 Synkron, send og motta melding 24

3.4 Synkron, hent og send melding 25

3.5 Henting av meldinger fra AMQP-kø 25

Dokumenthistorikk

Versjon	Dato	Innhold/Endring
0.1	24.10.2016	Første versjon av profil, basert på dokumenter AMQP profil v 1.2 og Digital Dialog - Feilhåndtering v1.21
0.2	30.11.16	Flyttet PKI sjekkliste fra implementasjonsguide Digital dialog til profil for meldingsutveksling (dette dokument).
0.3	05.12.16	Distribuert til leverandører innen Pleie og omsorg
0.31	14.12.16	La til ny feilkode i avsnitt 2.2.3 for validering av mottagers her Id.
1.0	27.03.17	Lagt til valgfritt Application property i AMQP attributter og klargjort bruken av øvrige attributter. Presisert resending og Id-er i avsnitt 2.2.5
1.01	9.06.17	Lagt til validering av fagmeldingens mottager HER id og AMQP Her Id i avsnitt 2.2.3 Presisert ansvarsovergang ved mottak av positiv applikasjonskvittering i avsnitt 2.1.1.1
1.02	08.11.17	Presisert håndtering av error kø, og innhold som skal sendes på denne. Beskrevet i avsnitt 2.2.6 Endret håndtering av ulikhet mellom AMQP Avsender HER-Id og fagmelding Avsender HER-Id. Tidligere ga dette melding på Error kø, endret til negativ applikasjonskvittering.
1.1	16.11.18	Nye attributter på AMQP header; Role, Service,, action og conversationId Tydeliggjort skille mellom meldingstjener og applikasjon i prosesser i avsnitt 2.2.1 og 2.2.2. Beskrevet krav til synkronisering av klokker for klienter. Lagt ti lhåndtering av duplikate meldinger. Profil publisert på Sarepta.ehelse.no

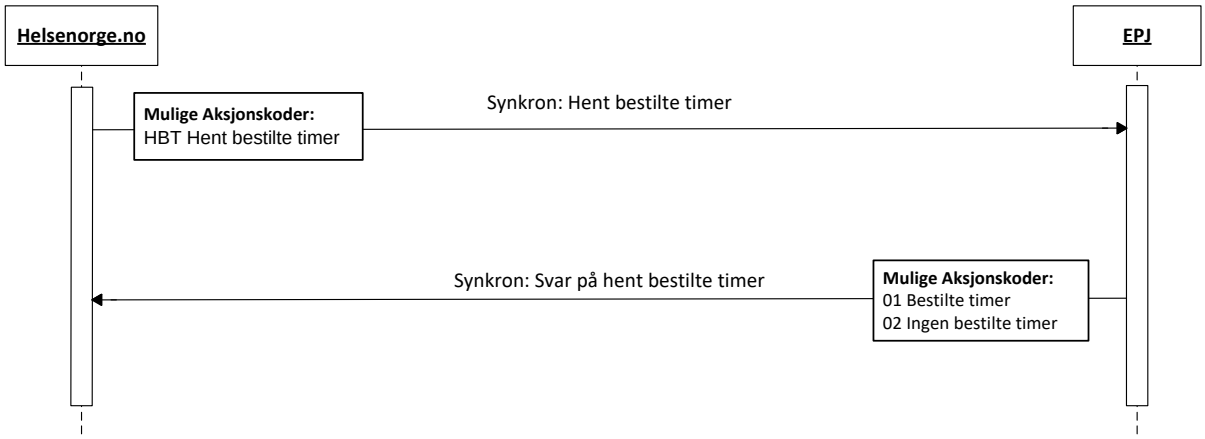
1 Meldingsutveksling helsenorge.no

Helsenorge.no inneholder tjenester rettet mot alle innbyggere. Ambisjonen er å gjøre innbyggernes hverdag enklere med digitale tjenester tilpasset alle deler av helse- og omsorgsektoren.

For å sende meldinger mellom de ulike partene benyttes AMQP som transportprotokoll. Norsk Helsenett (NHN) har etablert en Meldingsutveksler (MU), som bruker meldingskøer. Meldingsutveksleren er realisert med Microsoft Service Bus. Meldingene er i utgangspunktet asynkrone og benyttes fortrinnsvis til meldingsutveksling. I noen tilfeller benyttes også meldingsutveklsing for å tilby synkrone tjenester, i utganspunktet bør dette løses av mekanismer for datadeling.

1.1 Synkrone tjenester

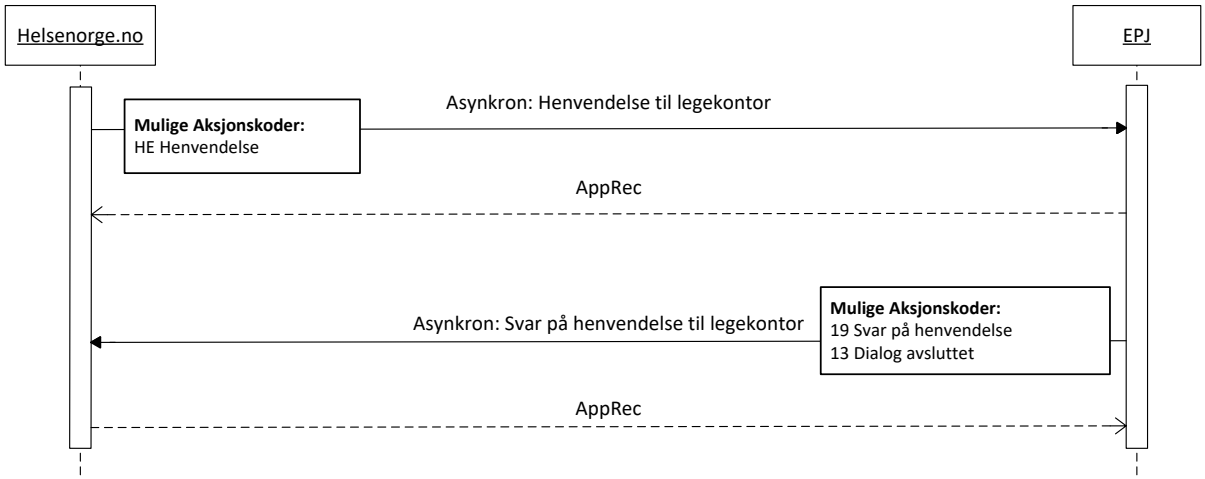
Sekvensdiagram for et eksempel av synkron tjeneste er vist i figuren under:



Figur 1: Synkron tjeneste

1.2 Asynkrone tjenester

Sekvensdiagram for et eksempel av asynkron tjeneste er vist i figuren under:



Figur 2: Asynkron tjeneste

2 AMQP Meldingsutveksling

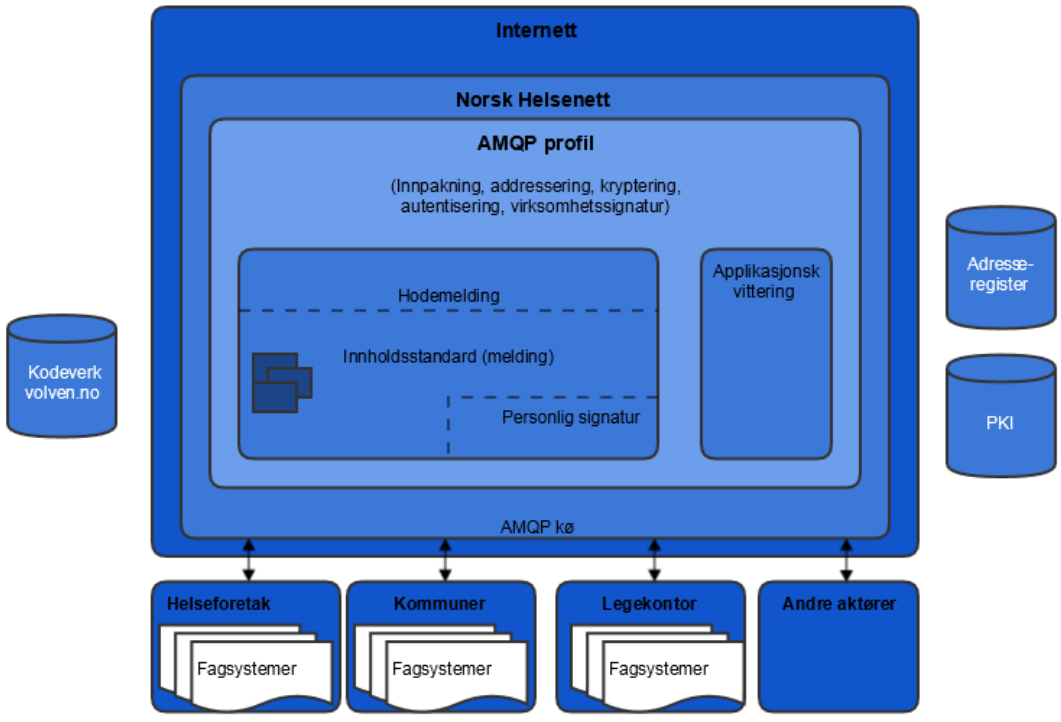
Ved innføring av Digital Dialog fastlege, var det behov for en mekanisme for synkron meldingsutveksling. Synkrone meldinger er ikke godt støttet med standard for meldingsutveksling basert på SMTP og ebXML. Bruk av AMQP ble derfor pilotert, og benyttes som transportprotokoll mot helsenorge.no. En viktig begrunnelse for valg av AMQP for synkrone kall er økt sikkerhet ved at alle kall initierers fra innsiden ved at mottager lytter på en kø. Ved bruk av standarder for datadeling som for eksempel web service, vil kall initieres fra utsiden og mot mange små aktører som ikke kan forutsettes å ha robuste sikkerhetsmekanismer for sikring av eksterne kall.

Meldingsutveksling ved SMTP har også noen operasjonelle utfordringer:

- Ikke garantert leveranse
- Mulighet til å sende til epostadresse som ikke eksisterer
- Behov for transportkvitteringer for å verifisere transport av meldinger og håndtere resending

Disse utfordringene reduseres ved bruk av AMQP som transportprotokoll.

Meldingsutveksling via AMQP er vist på figuren under med lignende notasjon som i standard for meldingsutveksling:

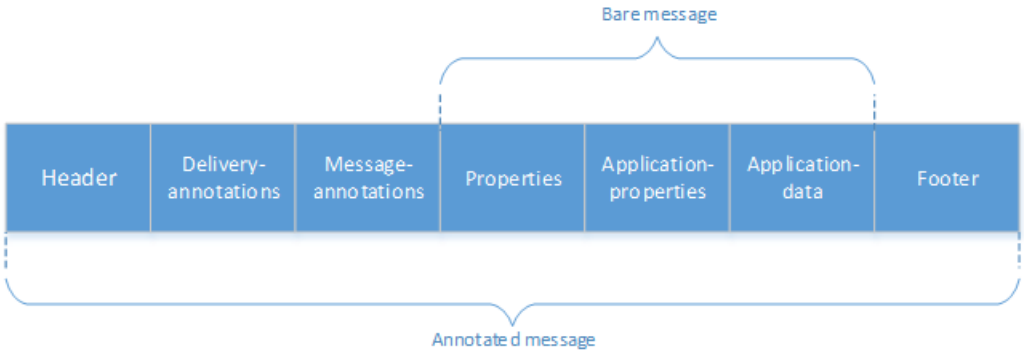


Figur 3: Meldingsutveksling AMQP

Dette kapittelet beskriver AMQP profil som er utarbeidet og validering/feilhåndtering som benyttes ved utveksling av meldinger

2.1 AMQP Profil

En AMQP melding består av «Bare message» som er meldingen generert av avsender. Denne er «immutable», dvs. det hverken kan eller vil ikke skje en eneste endring fra «Bare message» er sendt til den er levert

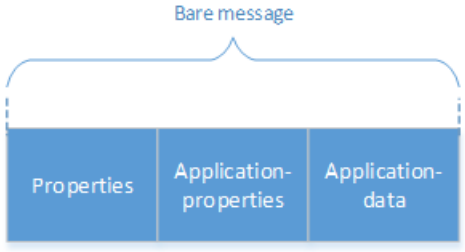


Figur 4: AMQP meldingsstruktur

«Annotated message» inneholder de tilleggsblokkene AMQP Message Broker trenger for å transportere meldingen korrekt frem til mottaker.

«Bare message» består av:

- Application data: Selve innholdet i meldingen, dvs. fagmeldingen
- Properties: Liste over predefinerte nøkler og deres verdier (dersom de er satt). Eks. «reply-to» eller «subject».
- Application properties: Egendefinerte nøkler og deres verdier. Eks. “cpa-id”. Alle er av typen String.



Figur 5: AMQP Bare message

De øvrige elementene er:

- Header 0 eller 1 forekomst, inneholder leveranseattributter for meldingen.
- Delivery annotations 0 eller 1 forekomst, inneholder ikke-standard leveranseattributter for meldingen. Ikke i bruk
- Message annotations 0 eller 1 forekomst
- Footer 0 eller 1 forekomst

2.1.1 Videreføring av prinsipper og funksjonalitet i ebXML/ebMS

ebMS V2.0 er tidligere benyttet som bærer hovedsakelig fordi meldinger skulle transporteres over SMTP. ebXML rammeverket benyttes i dag for håndtering av:

- Trygghet for at meldingen kommer fram ved bruk av transportkvitteringer
- Sikkerhet. SMTP som protokoll har svært lite innebygget sikkerhet

Med AMQP-protokollen eksisterer det en struktur som er egnet for å plassere de samme, standardiserte feltene og verdiene som benyttes i ebMS V2. Bruk av ebMS sammen med AMQP vurderes som lite hensiktsmessig og gir et ekstra lag med innkapsling som tilfører lite verdi.

ebXML-transpportkvittering (ebXML Acknowledgment) er håndtert ved følgende funksjonalitet i AMQP:

- Avsender kan kun skrive til en meldingskø som eksisterer og er tilgjengelig
- Krav til bruk av kommunikasjonsparametre (CPP og CPA), mottager har aktivt valgt å støtte en kommunikasjonsprosess.
- Positiv bekreftelse på at skriving til kø er OK
- Sendingsforsøket feiler dersom meldingskø er utilgjengelig

Feilmelding (ebXML Error Signal) er håndtert ved følgende funksjonalitet i AMQP (avsnitt 2.2 i AMQP spesifikasjon)

- Transaksjonsbasert lesing av køen med støtte for å bekrefte at lesing og behandling av melding har gått bra før den slettes fra køen.
- Leseoperasjon der transaksjonen ikke avsluttes, vil resultere i at meldingen etter N antall forsøk havner på mottagers Deadletter kø
- Bruk av Error-kø der mottager sender en feilmelding som inneholder feilkode og en feilstatus, samt referanse til den opprinnelige meldingsutvekslingen
- Krav til prosesser og rutiner for håndtering av error og deadletterkø

Applikasjonskvittering benyttes for å kvittere positivt eller negativt på selve fagmeldingen, dette er likt både for AMQP og ebXML.

Med AMQP som protokoll er det også full sporbarhet av meldinger, slik at NHN som driftsleverandør kan identifisere status for en melding, hvem som har skrevet melding og hvem som eventuelt har mottat og tatt melding fra kø.

2.1.1.1 Ansvarsoverdragelse for behandling av melding

AMQP følger retningslinjer fra veileder for applikasjonskvitteringen som ble laget i 2016(kapittel 4)
https://ehelse.no/standarder-kodeverk-og-referansekatalog/standarder-og-referansekatalog/veiledning-til-riktig-bruk-av-applikasjonskvittering-hisd-11682016

Her er det definert at ansvaret for behandling av melding overføres ved mottak av positiv applikasjonskvittering:

«Applikasjonskvittering brukes for å bekrefte eller avkrefte om en fagmelding har kommet korrekt fram til fagsystemet. Når positiv applikasjonskvittering er mottatt, skal avsender av fagmeldingen kunne være sikker på at fagmeldingen er kommet frem, at innholdet er i rett format, og at meldingen er klar for behandling i mottakers fagsystem. Det betyr således at mottaker har overtatt ansvaret for den videre behandlingen av fagmeldingen. Applikasjonskvitteringen er derfor avgjørende for tilliten til den elektroniske samhandlingen.»

Dette betyr også at det er avsender sitt ansvar å følge opp en sendt melding helt til en får en positiv applikasjonskvittering.

For synkrone tjenester som ikke benytter applikasjonskvittering, overdras ikke ansvaret til mottager av meldingen.

2.1.2 AMQP attributter

AMQP versjon 1.0 (http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-overview-v1.0-os.html) skal benyttes i henhold til profilen under.

Bokstavkodene for kolonnen Required/optional betyr følgende:

- R = Feltet er påkrevd i alle sammenhenger når det sendes en AMQP-melding
- R2 = Feltet er kun påkrevd når AMQP-meldingen brukes for å melde transportfeil
- O = Feltet er valgfritt og skal kun brukes i henhold til beskrivelsen av feltet
- O2 = Feltet er valgfritt og skal kun brukes når AMQP-meldingen brukes for å melde transportfeil og i henhold til beskrivelsen av feltet

Application properties er utvidet med attributter fra SOAP:Header i ebXML for å sikre at meldingsutveksling foregår på rikitg måte.

AMQP-blokk	Required/ Optional	Felt	Innhold
Properties	R	messageId	Unik id på UUID-format. messageId identifiserer en AMQP melding unikt og er uavhengig av eventuell meldingsId for fagmeldingen som sendes.
	O	userId	*Ikke angitt.*
	R	To	Id for kø-en meldingen skal sendes til (f.eks. <HerId>_sync). Det skal oppgis full id slik den er registrert i Adresseregisteret.
	R	Subject	Angir meldingsinnhold med kodeverdi fra kodeverk 8279 «Meldingens funksjon»: http://volven.helsedirektoratet.no/produkt.asp?id=237513&catID=3&subID=8. Når innholdet i Application-data er en soap fault melding skal subject settes til «AMQP_SOAP_FAULT».
	R	replyTo	Id for kø-en returmelding skal sendes til (f.eks. <HerId>_sync). Det skal oppgis full id slik den er registrert i Adresseregisteret.
	R	correlationId	Unik id for et sett av transaksjoner som hører sammen. ID på UUID-format. Attributtet benyttes for synkrone meldinger, for å knytte svarmelding til forespørsel.
	R	contentType	Settes til en av verdiene basert på:

			• Kun kryptert innehold: «application/pkcs7-mime; smime-type=enveloped-data» • Kun signert innehold: «application/pkcs7-mime; smime-type=signed-data» • Signert og kryptert innehold: «application/pkcs7-mime; smime-type=signed-and-enveloped-data» • Usignert og ukryptert soap melding: «application/soap+xml»
	O	contentEncoding	*Ikke angitt.*
	O	absoluteExpiry Time	*Ikke angitt.*
	O	creationTime	*Ikke angitt.*
	O	groupId	*Ikke angitt.*
	O	groupSequence	*Ikke angitt.*
	O	replyToGroupId	*Ikke angitt.*
Application Properties	O	cpaId	Id for CPA-avtale dersom dette finnes. Dersom det ikke foreligger en CPA-avtale skal ikke feltet tas med i AMQP-meldingen.
	O	Service	Id til Service fra CPA
	O	Action	Id til Action fra CPA
	R	applicationTime Stamp	Tidsstempel for generering av AMQP-meldingen. Formatet skal være i henhold til ISO 8601 (CCYY-MM-ddThh:mm:ssTZD). Tidspunkt skal oppgis i UTC. Dersom lokal tid benyttes skal tidssone angis. Eksempel: 2014-02-26T12:45:32+02:00.
	R	fromHerId	HER-id for avsender
	O	fromRole	Rolle til avsenderr av melding,satt i henhold til rolle fra CPA
	R	toHerId	HER-id til mottaker.
	O	toRole	Rolle til mottager av melding,satt i henhold til rolle fra CPA
	O	ConversationId	Unik identifikasjon for et sett meldinger som utgjør en konversasjon
	R2	originalMessageId	Feltet skal inneholde messageId fra den

			meldingen som AMQP-transportfeilmeldingen gjelder for
	R2	receiverTime Stamp	Tidsstempel for når mottaker prøvde å behandle den meldingen som feilet.
	R2	errorCondition	Lesbar og maskinlesbar kode som beskriver feilårsak
	R2	errorDescription	Lesbar tekst som beskriver feilårsaken
	O2	errorCondition Data	Inneholder tilleggsdata i forbindelse med feilmelding. F.eks. i forbindelse med manglende påkrevde felter kan man gjengi manglende felter på en maskinlesbar måte. Dersom ikke tilleggsdata finnes skal feltet ikke tas med.
Application-data	R		Den krypterte fagmeldingen (tilsvarende «Payload» i ebMS) plasseres direkte i «Application Data» uten noen form for MIME-encoding/konvertering. Dvs. at en skriver/leser de krypterte dataene til/fra AMQP-meldingen på samme måte som om en skriver til/fra en fil (dataene er en byte-array, byte[]).

2.1.3 AMQP Køoppsett

Følgende køer benyttes ved meldingsutveksling:

- **Async**: Brukes ved asynkrone operasjoner. Time to Live (TTL) for async kø bruker default setting til service bus slik at melding ikke timer ut.
- **Sync**: Brukes ved synkrone operasjoner. TTL = 15 sekunder
- **Error**: Brukes ved kjente feilsituasjoner, beskrevet i AMQP Feilhåndtering
- **Deadletter**: Innkommende meldinger rutes til deadletter-køen dersom mottaker forsøker å lese meldingen fra kø flere enn 10 ganger uten at transaksjonen avsluttes.

Køoppsettet opprettes automatisk av MU dersom tjenestebuss aktiveres for en virksomhet i Adresseregisteret. Køoppsettet opprettes for alle eksisterende kommuniksasjonsparter og eventuelle kommunikasjonsparter som opprettes senere vil også få opprettet det samme køoppsettet.

2.1.3.1 Error-kø

Error-køen er en del av køoppsettet som er beskrevet i AMQP-spesfikasjonen for Helsenorge.no.

2.1.3.1.1 *Formål*

Formålet med error-køen er å varsle avsender om feil med meldingen som kun avsender kan rette.

2.1.3.1.2 Bruk

2.1.4 Error-køen skal kun benyttes for de feilsituasjoner beskrevet i avsnitt 2.1.6 Synkronisering av klokke

For sending og mottak av meldinger er det viktig og påkrevd at klokken på klienten er synkronisert med en sentral tidsserver. Dette kreves blant annet for:

- Sikre at synkrone meldinger håndteres korrekt
- Sikre at tidsstempel i fagmelding er riktige, disse brukes i noen tilfeller for sortering av meldinger

For synkronisering av klokker er det flere tilgjengelige tidsservere på internett og disse kan velges fritt.NHN tilbyr en tidstjener for applikasjoner på helsenett, denne er vist i tabellen under.

Server	Beskrivelse
Time.windows.com	Standard tidsserver for windows, krever tilgang til internett
ntp.nhn.no	Tidsserver tilgjengelig på Helsenett

AMQP Feilhåndtering. Interne feil hos mottager, skal ikke rapporteres til avsender av melding.

2.1.4.1.1 Monitorering

Error-køen skal monitoreres slik at feilen kan rettes, og eventuelt gi sluttbruker beskjed om at en utgående melding har feilet hos motpart og at motparten derfor ikke kunne prosessere meldingen. Sluttbruker skal bli presentert med angitt årsak og mulighet til å resende meldingen etter at feilsituasjon er rettet.

2.1.4.2 **Deadletter-kø**

Alle køer på MU tilbyr en sekundær sub-kø som kalles deadletter. Køen opprettes automatisk og kan ikke slettes eller på annen måte forvaltes uavhengig av hovedenheten.

2.1.4.2.1 Formål

Formålet med deadletter-køen er å holde på innkommende meldinger som ikke kan prosesseres av mottaker på det gitte tidspunktet. Årsaken til at meldingen havner på deadletter kan være flere, men i hovedsak skal det dreie det seg om at ett eller flere bakenforliggende system er nede, nettverksbrudd e.l.

2.1.4.2.2 Bruk

Meldinger som havner på deadletter-køen må analyseres for feilkilde ved å undersøke systemlogger som tilbys av mottakers software-applikasjon. Normalt skal årsaken til feil være rettbar, og melding kan re-prosesseres ved å legge melding tilbake på kø spesifiert i «to»-feltet i AMQP properties.

2.1.4.2.3 Monitorering

Deadletter-køen skal monitoreres slik at det gis anledning til å identifisere feilen og reprosessere disse meldingene etter at feilsituasjon er rettet.

2.1.5 Sertifikater

AMQP-broker anbefales å holde en lokal cache av sertifikater for systemoptimalisering.

Følgende skal valideres for sertifikater ved inngående og utgående meldinger:

- Er innenfor gyldighetsperioden
- Har korrekt bruksområde
    - Benytt OID verdi 2.5.29.15 - Key Usage for å kvalitetsikre bruksområdet til sertifikatet

- Ikke er tilbakekalt/revokert ved å gjøre en Online Revocation Check
- Dersom validering-serveren til sertifikatutsteder er nede skal operasjonen avbrytes og det kan forsøkes på nytt etter et egendefinert tidsrom.

Dersom validering av offentlige sertifikat feiler, skal cache invalideres og nye sertifikater hentes fra adresseregisteret. Meldingen skal beholdes, og dekryptering eller validering skal gjøres på nytt med det nye sertifikatet når dette er lastet ned og installert.

For løsninger som støtter parallelle sertifikater skal nyeste sertifikat benyttes som default. Dette for å gjøre overgang fra gammelt til nytt sertifikat så smidig som mulig og minimere risiko for feil ved utløp av gammelt sertifikat.

Mekanismene over vil også håndtere sertifikatbytter.

2.1.6 Kryptering og signering av fagmelding i AMQP

Den krypterte og signerte fagmeldingen («Payload» i ebMS) plasseres direkte i AMQP Application Data uten noen form for MIME-encoding/konvertering. Dvs. at en skriver/leser de krypterte dataene til/fra AMQP-meldingen på samme måte som om en skriver til/fra en fil (dataene er en byte-array, byte[]). For signering benyttes «encapsulated data». Ved bruk av både signering og kryptering skal fagmeldingen først signeres og deretter krypteres. Cryptographic Message Syntax benyttes for signering og kryptering, og prosessen for dette er:

1. Signerer fagmeldingen (encapsulated, ikke detached)
    1. Input er komplett fagmelding + virksomhetssertifikat med Key Usage = «Non-Repudation»
    2. Output er signert fagmelding
2. Deretter kryptereres den signerte fagmeldingen
    1. Input er signert fagmelding fra pkt. 1.2 + virksomhetssertifikat med Key Usage = «Data Encipherment»
    2. Output er kryptert fagmelding
3. Til sist opprettes en AMQP Message:
    1. ContentType = “application/pkcs7-mime; smime-type=signed-and-enveloped-data”
    2. Body = Output fra 2.2

Signerering og krypterering benytter virksomhetssertifikater registrert i Adresseregisteret

2.1.7 Synkronisering av klokke

For sending og mottak av meldinger er det viktig og påkrevd at klokken på klienten er synkronisert med en sentral tidsserver. Dette kreves blant annet for:

- Sikre at synkrone meldinger håndteres korrekt
- Sikre at tidsstempel i fagmelding er riktige, disse brukes i noen tilfeller for sortering av meldinger

For synkronisering av klokker er det flere tilgjengelige tidsservere på internett og disse kan velges fritt.NHN tilbyr en tidstjener for applikasjoner på helsenett, denne er vist i tabellen under.

Server	Beskrivelse
Time.windows.com	Standard tidsserver for windows, krever tilgang til internett

ntp.nhn.no	Tidsserver tilgjengelig på Helsenett

2.2 AMQP Feilhåndtering

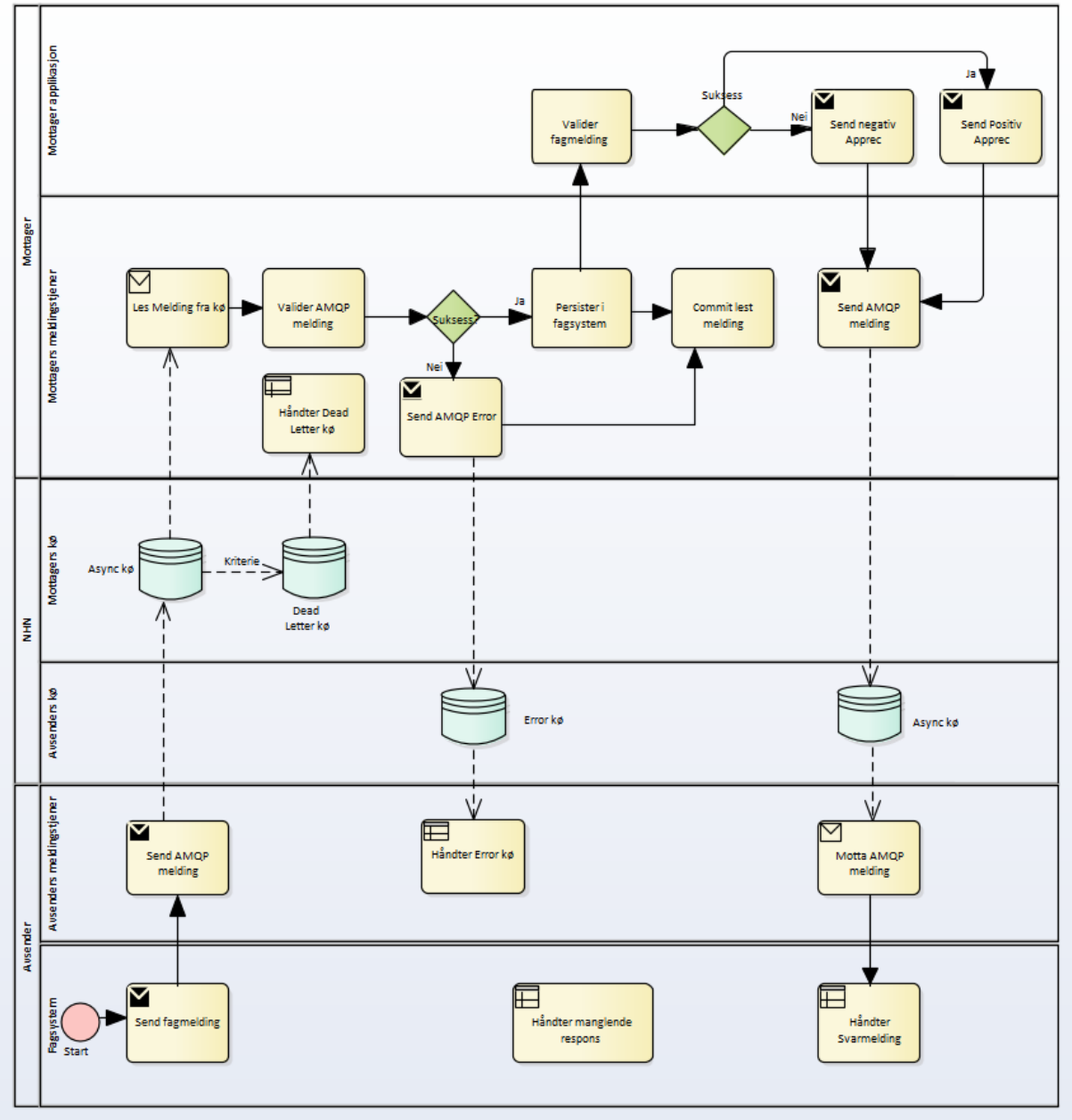
Meldingsutveksling benytter følgende mekanismer for å ivareta leveringssikkerhet og at avsender får beskjed om feil som oppstår når mottaker henter ned en melding fra kø og prosesserer meldingen:

- **AMQP-Error**: benyttes ved feilsituasjoner som oppstår i forbindelse ved validering av sertifikater i signerings- og krypteringssammenheng, feil encoding på Payload eller manglende påkrevde felter på AMQP-konvolutt.
- **Negativ AppRec**: brukes dersom fagmelding ikke kan tolkes eller ev. lagres/behandles av mottakers system.
- **Temakoder ved feilsituasjoner**: benyttes når fagmeldingen har passert stegene for tolkning og lagring/behandling slik at positiv AppRec er sendt, men det oppstår en situasjon som rapporteres tilbake til avsender som en feilsituasjon eller avvik.
- **Resending ved manglende AppRec**: Dersom avsender ikke mottar en AppRec etter en definert tidsperiode skal meldingen resendes

Håndtering av de ulike mekanismene er ytterligere detaljert i underavsnitt.

2.2.1 Prosess asynkrone tjenester

For asynkron kommunikasjon er prosessen for sending av meldinger, inkludert feilhåndteringsprosessen vist i figuren under.



Figur 6: Prosess for asynkron meldingsutveksling

Stegene i prosessen er kortfattet beskrevet i tabellen under.

Tabell 1: Prosesssteg asynkron meldingsutveksling

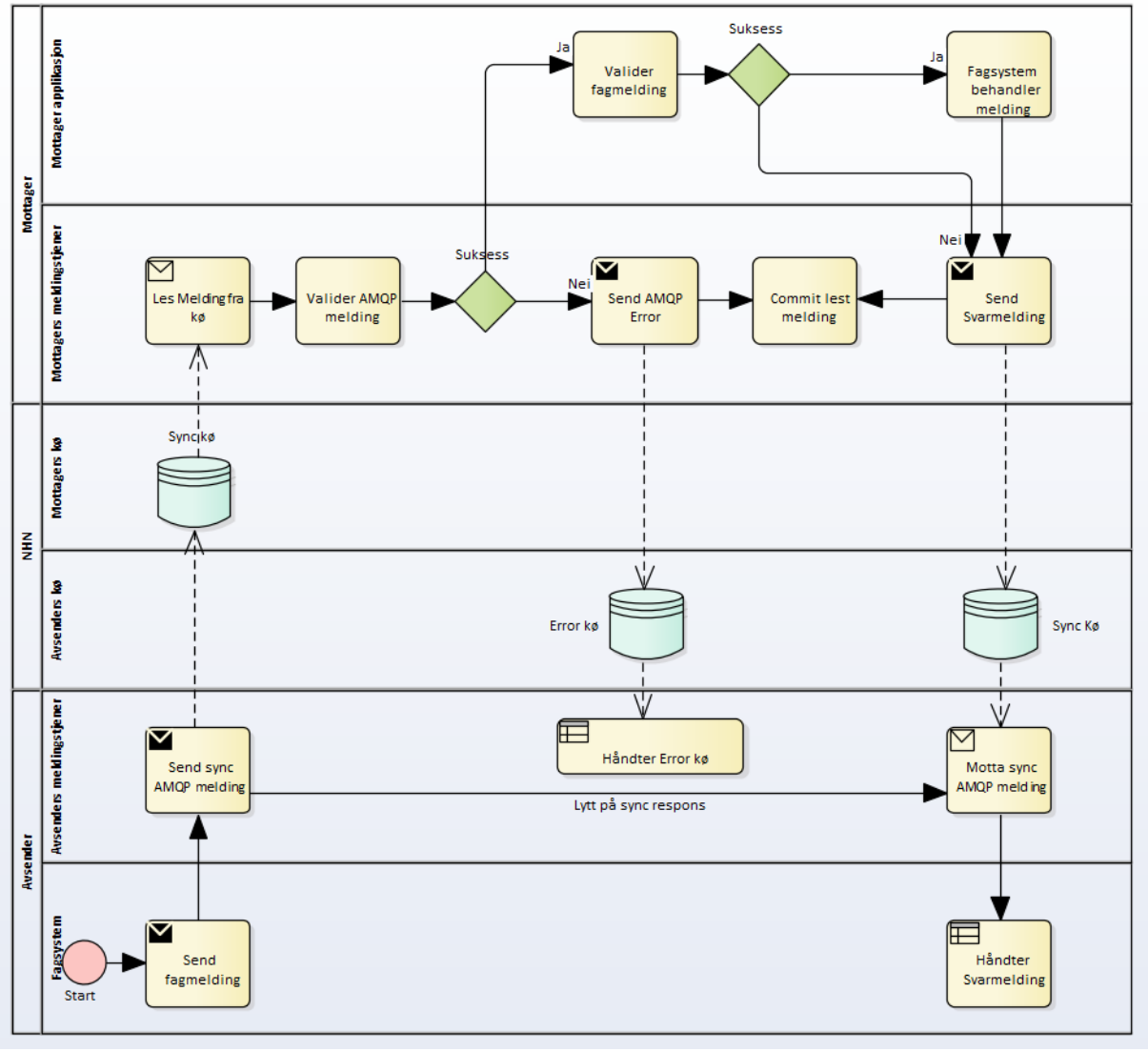
#	Steg	Beskrivelse
1.	Send fagmelding	Fagsystem oppretter melding, sendes til meldingstjener.
2.	Send AMQP melding	Meldingstjener sender melding, legges på mottagers Async kø.
3.	Les melding fra kø	Mottager meldingstjener leser melding fra kø

4.	Valider AMQP melding	Melding valideres i henhold til beskrivelse i avsnitt 2.2.3. Dersom validering feiles skal melding sendes til avsenders Error kø
5.	Send AMQP Error	Feil oppstått som følge av validering av AMQP melding og definert i avsnitt 2.2.3 skal sendes til AMQP Error kø. Andre interne feil eller andre feilkilder skal ikke føre til melding på Error kø.
6.	Valider fagmelding	Fagmelding valideres i henhold til beskrivelse i avsnitt 2.2.3
7.	Persister i fagsystem	Dersom melding validerer OK, persisteres melding i fagsystem for videre behandling.
8.	Send negativ apprec	Dersom fagmelding ikke valideres OK, sendes en negativ apprec til avsenders async kø
9.	Commit lest melding	Melding commites fra kø når en av følgende er oppfylt: - Melding persistert OK i fagsystem - AMQP Error sendt Hvis melding forsøkes lest 10 ganger uten at den commites vil den leggges på Dead letter kø.
10.	Send positiv apprec	Positiv apprec til avsenders Async kø
11.	Håndter Dead letter kø	Mottager må ha en prosess for å håndtere Dead letter kø. Alle meldinger som forsøkes lest 10 ganger uten å bli commited vil legges på Dead letter kø. Rotårsak til feil rettes og melding kan legges tilbake på async kø for prosessering
12.	Håndter Error kø	Prosess for å håndtere og rette opp meldinger som ikke validerer OK i henhold til spesifikasjon
13.	Håndter Aprec	Prosess for å håndtere positive og negative Apprec.
14.	Håndter manglende respons	Dersom avsender har skrevet melding til kø, men ikke fått feilmelding på error kø eller applikasjonskvittering må dette håndteres. Hvordan dette løses, er implementasjonsavhengig og kan variere fra virksomhet til virksomhet

2.2.2 *Prosess synkrone tjenester*

For synkron kommunikasjon er prosessen for meldingsutveksling inkludert feilhåndteringsprosessen vist i figuren under. Den største ulikheten på den asynkrone prosessen er at

- Applikasjonskvittering benyttes ikke, det forventes en synkron og når sanntid respons fra mottager. Dersom denne responsen ikke kommer vil transaksjonen time ut hos avsender
- Dead letter kø benyttes ikke, meldingen er ikke persistent og vil time ut fra kø.



Figur 7: Feilhåndtering synkron meldingsutveksling

Stegene i prosessen er kortfattet beskrevet i tabellen under.

Tabell 2: Prosesssteg synkron meldingsutveksling

#	Steg	Beskrivelse
1.	Send melding	Avsender sender melding, legges på mottagers Async kø

2.	Les melding fra kø	Mottager leser melding fra kø
3.	Valider AMQP melding	Melding valideres i henhold til beskrivelse i avsnitt 2.2.3. Dersom validering feiles skal melding sendes til avsenders Error kø
4.	Send AMQP Error	Feil oppstått som følge av validering av AMQP melding og definert i avsnitt 2.2.3 skal sendes til AMQP Error kø. Andre interne feil eller andre feilkilder skal ikke føre til melding på Error kø.
5.	Valider fagmelding	Fagmelding valideres i henhold til beskrivelse i avsnitt 2.2.3
6.	Fagsystem behandler melding	Dersom melding validerer OK behandles forespørsel og svarmelding opprettes.
7.	Commit melding	Melding commites fra kø når en av følgende er oppfylt: - Svarmelding sendt - AMQP Error sendt Hvis melding forsøkes lest 10 ganger uten at den commites vil den leggges på Dead letter kø. For synkrone meldinger er time to live 15 sekunder, så Dead letter kø vil i praksis ikke benyttes.
8.	Send svarmelding	Svarmelding sendes til avsender av melding. Svar inneholder enten svar på forespørsel eller en feilkode dersom melding ikke kunne tolkes eller håndteres.
9.	Håndter Error kø	Prosess for å håndtere og rette opp meldinger som ikke validerer OK i henhold til spesifikasjon
10.	Håndter svarmelding	Prosess for å håndtere svarmeldinger.

2.2.3 Validering av meldinger og håndtering av feil

Både AMQP-meldingen og fagmeldingen skal valideres av avsender før den sendes, og av mottaker før den prosesseres. Avsnittet beskriver minstekravene for validering av en melding og hvordan feil i validering skal håndteres.

Type	Validering	Håndtering av feil
AMQP	Verifisere verdiene for påkrevde felter. For å	AMQP-melding på Error-kø med errorCondition

melding	sikre at AMQP-meldinger inneholder påkrevde felter og verdier må det programmatisk gjøres en validering	«transport:invalid-field-value»
	Verifisere at kommunikasjonsprosessen er støttet.	AMQP-melding på Error-kø med errorCondition «transport:unsupported-message»
	Dekryptering feiler	AMQP-melding på Error-kø med errorCondtion «transport:decryption-failed»
	Avsenders sertifikat er utgått	AMQP-melding på Error-kø med errorCondition «transport:expired-certificate»
	Avsenders sertifikat er tilbaketrukket	AMQP-melding på Error-kø med errorCondition «transport:revoked-cerificate»
	Avsenders signatur kan ikke verifiseres	AMQP-melding på Error-kø med errorCondition «transport:invalid-signature»
	Duplikat AMQP MessageID. AMQP melding har blitt sendt tidligere.	Melding logges av mottager, ingen respons på error kø og ingen apprec. Opprinnelig sendt melding forventes å gi apprec og meldingen skal ikke behandles en gang til av fagsystem.
	Fagmelding header validerer ikke eller kan ikke tolkes.	AMQP-melding på Error-kø med errorCondition "transport:not-well-formed-xml"
	Replyto kø fins ikke	AMQP-melding på avsenders Error-kø med errorCondition «transport:invalid-field-value»
	Ikke samsvar AMQP Avsender HER-Id <-> fagmelding Avsender HER-Id	AMQP-melding på Error-kø med errorCondition «abuse:spoofing-attack»
Fagmelding	Ikke samsvar AMQP mottager HER-Id <-> fagmelding mottager HER-Id	Negativ AppRec med kode «E10 Ugyldig meldingsidentifikator» fra kodeverk 8221.
	Mottatt XML kan ikke tolkes	Negativ AppRec med kode «T01 – Ikke XML / ikke 'well formed' / uleselig» fra kodeverk 8221. Krever at header i melding validerer og kan tolkes.
	XSD-validering	Negativ AppRec med kode «T02 – XML validerer ikke» fra kodeverk 8221. Krever at header i melding validerer.
	Verfisering av verdier for påkrevde felter feiler	Negativ Applikasjonkvittering med kode «T02 – XML validerer ikke» fra kodeverk 8221

2.2.4 Feilsituasjoner og håndtering av disse

Tabellen under viser noen mulige feilkilder og beskrivelse av hvordan de skal håndteres.

Feilsituasjon	**Håndtering av feilsituasjon**
Avsender mottar negativ AppRec	Avsender må manuelt følge opp mottatte feilkoder i AppRec og genere ny (feilfri) fagmelding og sende den. Resending av samme fagmelding skal ikke skje da dette forventes å føre til ny negativ AppRec.

Mottaker får ikke sendt AppRec i forbindelse med feil i sentral infrastruktur	Mottakers system sender automatisk AppRec på nytt etter et egendefinert tidsrom, eller gjør brukeren oppmerksom på feilsituasjonen med sentral infrastruktur slik at brukeren kan forsøke å generere/sende meldingen på nytt.
Avsender får ikke sendt melding i forbindelse med feil i sentral infrastruktur	Avsender sender melding på nytt automatisk etter et egendefinert tidsrom eller gjør brukeren oppmerksom på feilsituasjonen med sentral kø slik at brukeren kan forsøke å generere/sende meldingen på nytt.
Mottaker mottar samme fagmelding to ganger	Forkaste duplikat meldingen og sørge for at AppRec sendes kun én gang for forespørselen med tilsvarende fagmelding sin MsgId. En duplikat melding er en melding med samme verdi i MsgHead/MsgInfo/MsgId som en tidligere mottatt melding.
Avsender av fagmelding mottar ikke AppRec innen forventet tid	Forventet tid for mottak av apprec vil variere avhengig av bruken og hvilke aktører meldingen utveksles med. Helsenorge.no kan forventes å sende applikasjonskvittering innen et fåtall timer, og normalt innen et fåtall minutter. Avsenders bruker bør manuelt sjekke at melding er ok og kan sende melding på nytt. Ikke mottatt AppRec kan være feil hos mottaker, men det kan også være feil i sendt fagmelding som gjør den ikke-prosesserbar hos mottaker. Identisk fagmelding bør ikke resendes mer enn én gang. NHN har sporbarhet på meldinger og overvåkning av køer og meldinger.

2.2.5 Resending og id-er

Følgende retningslinjer gjelder for resending av meldinger og bruk av messageId på AMQP-nivå og MsgID fagmeldingen:

Situasjon	**amqp:messageId**	**MsgHead/MsgInfo/MsgID**
Systemet resender meldingen på nytt etter å ha mottatt en feil på AMQP Error-kø og rettet feil.	Ny	OriginalId
Systemet resender en melding etter å ha mottatt negativ AppRec og rettet feil.	Ny	Ny
Systemet resender en melding pga. at man ikke fikk lagt meldingen på køen (og derfor aldri har blitt behandlet av mottaker)	OriginalId	OriginalId

ebXML rammeverket beskriver resending av melding på grunn av manglende AppRec innen 96 timer. Dette er ikke implementert for AMQP av følgende årsaker:

- Meldingsutveksling over AMQP forutsetter bruk av kommunikasjonsparametre (CPP/CPA). Avsender vet at melding støttes av mottager.
- Meldingen er skrevet til mottagers kø. Avsender vet at melding er kommet fram
- Melding skal ikke fjernes fra kø før den er behandlet og applikasjonskvittering er sendt.
- Dersom mottager behandler meldinger vil meldingen havne på avsenders Error kø, mottagers dead letter kø eller applikasjonskvittering vil sendes
- Melding timer aldri ut fra async kø, og async kø skal overvåkes av mottager

Prosess for manglende respons beskrevet i avsnitt 2.2.1 benyttes i dette tilfellet.

2.2.6 Feilrapportering på AMQP Error-kø

Feilrapporteringen fra mottakers vil skje ved at det genereres en AMQP-melding (feilmelding) som kun består av properties og application properties med referanse til den mottatte meldingen og en oversikt eller liste som angir hvilke feil som er oppdaget. En slik melding vil ikke inneholde et forretningsdokument i form av en application data.

Ved feilrapportering skal AMQP-felter settes slik beskrevet i tabellen under.

Application Property	**Beskrivelse**
amqp:messageId	Ny unik verdi
originalMessageId	Settes til opprinnelige amqp:messageId
receiverTimeStamp	Tidspunkt da meldingen ble forsøkt behandlet av mottaker
errorCondition	Lesbar og maskinlesbar kode som beskriver feilårsak. Se tabell under for detaljering.
errorDescription	Lesbar tekst som beskriver feilårsaken. Se tabell under for detaljering.
errorConditionData	Inneholder tilleggsdata i forbindelse med feilmelding. F.eks. i forbindelse med manglende påkrevde felter kan man gjengi manglende felter på en maskinlesbar måte.

Feilkoder og beskrivelser av disse er definert i tabellen under:

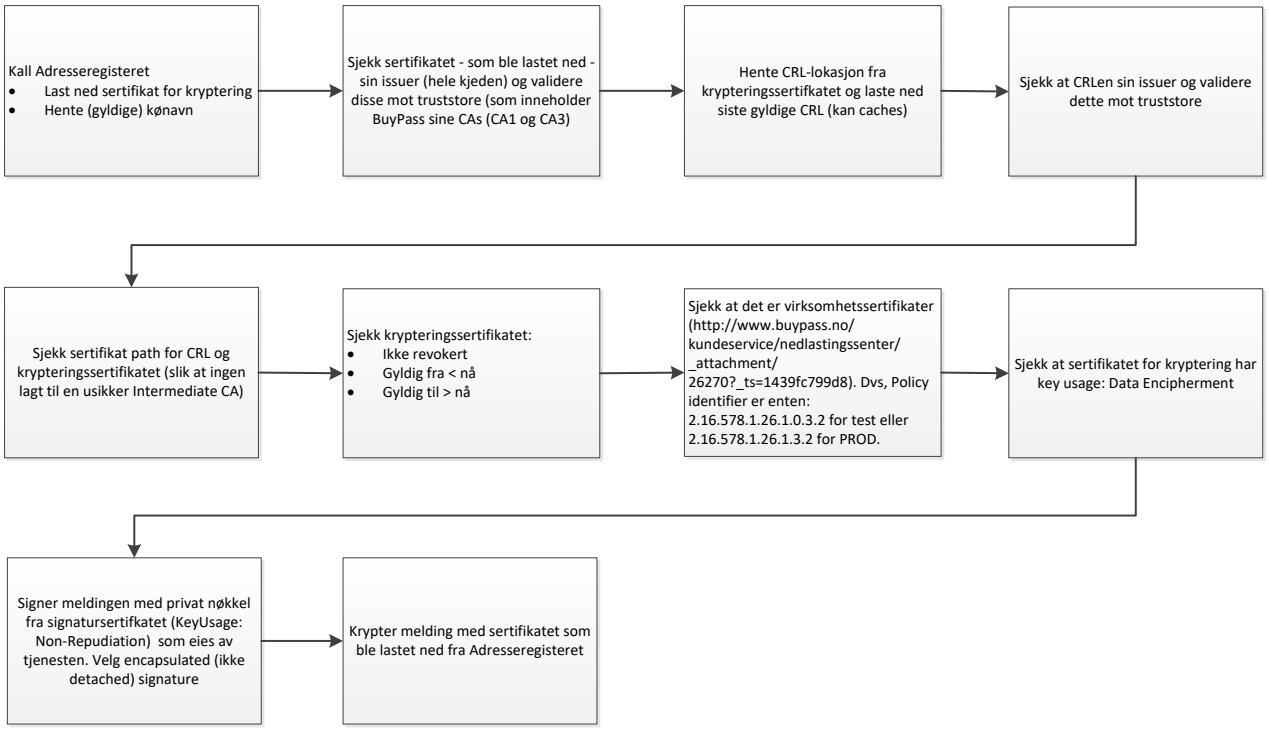
errorCondition	**errorDescription**	**errorConditionData**
transport:invalid-cms-pkcs	Could not decrypt message because of *invalid format to CMS/PKCS*.	
transport:invalid-certificate	Could not decrypt message because of *unknown/incorrect certificate*	{ "thumbprint" : { "expected": "streng", "actual": "streng" } Thumbprint til sertifikater, for å lette feilsøking
transport:expired-certificate	Could not decrypt message because of *certificate expired*.	Thumbprint til sertifikat, for å lette feilsøking
transport:revoked-certificate	Could not decrypt message because of *certificate added to CRL (Certificate Revocation List)*.	Thumbprint til sertifikat, for å lette feilsøking
transport:decryption-failed	Could not decrypt message because of *unknown reason*.	Thumbprint til sertifikat, for å lette feilsøking
transport:invalid-signature	Digital signature could not be verified.	Thumbprint til sertifikat, for å lette feilsøking
transport:required-field-missing	Missing or invalid value in field: '*AnyField*'.	Array med navn på felter som mangler
transport:invalid-field-value	Invalid value in field: '*AnyField*'.	Array med navn på felter hvor verdier mangler eller ikke er satt riktig
transport:invalid-encoding	Error occurred during decoding message. Expecting message encoded as '*Unicode*'.	En streng med IANA/MIME-navnet på encoding forventet http://www.iana.org/assignments/character-sets/character-sets.xhtml
abuse:spoofing-attack	Possible spoofing attack detected.	Array med to elementer { amqp:[herId],

		application:[herId] }
transport:xml-not-interpretable	XML cannot be interpreted	

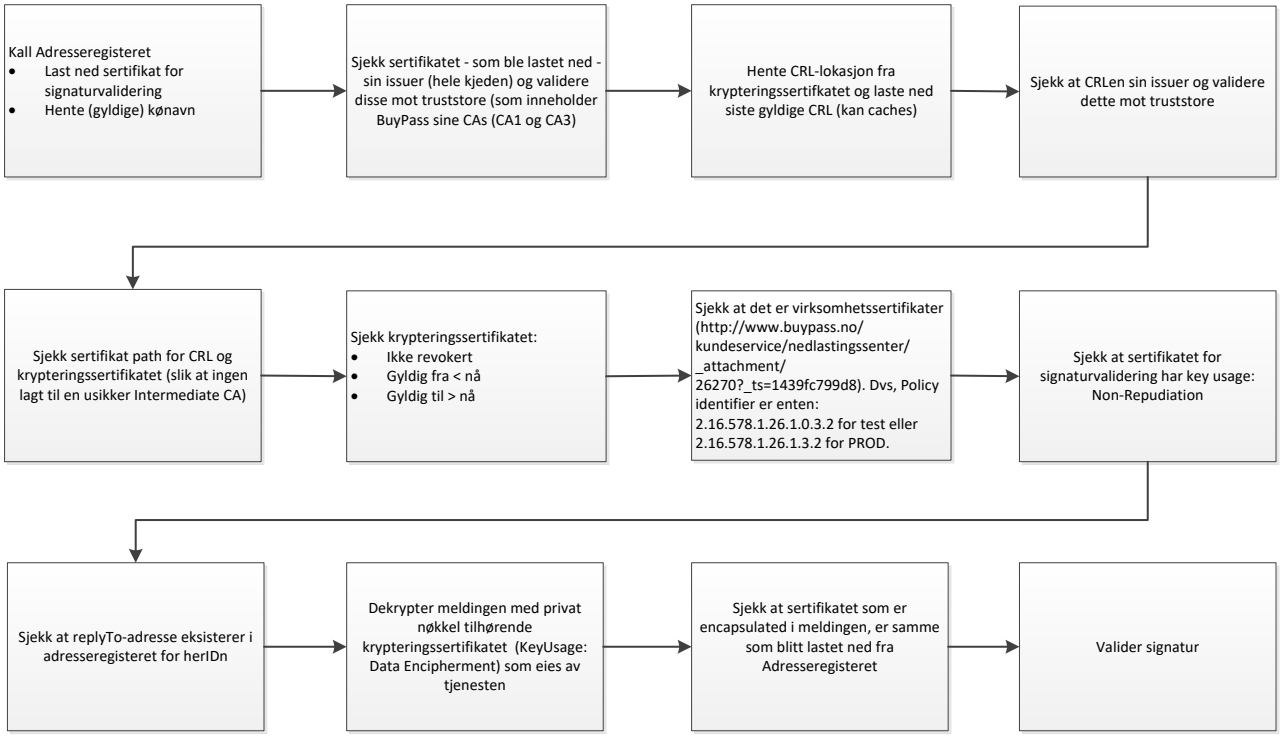
3 PKI-sjekkliste

Nedenfor er det vist sjekklister som kan brukes for PKI og sertifikathåndtering ved sending og mottak for synkrone og asynkrone tjenester

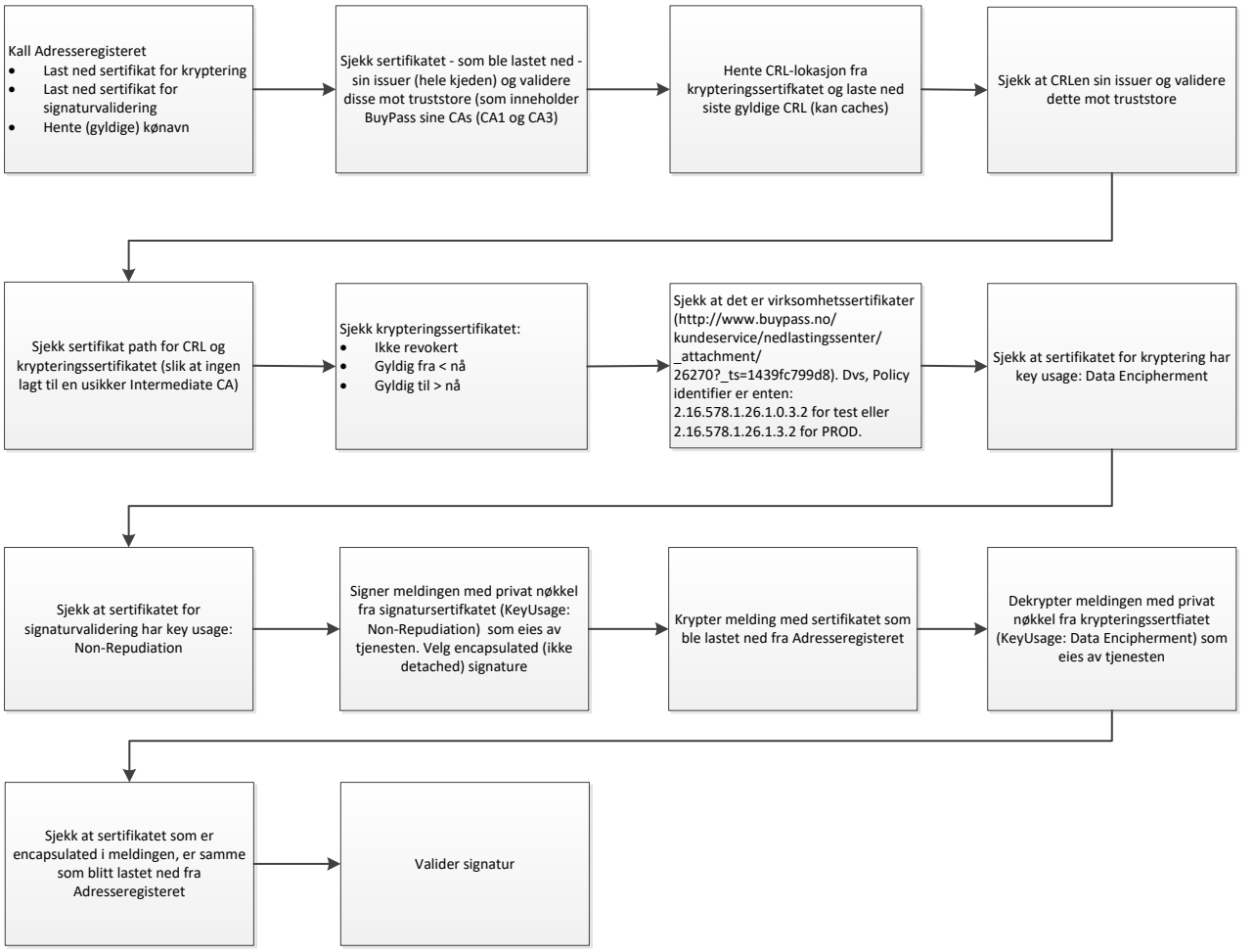
3.1 Asynkron, send melding



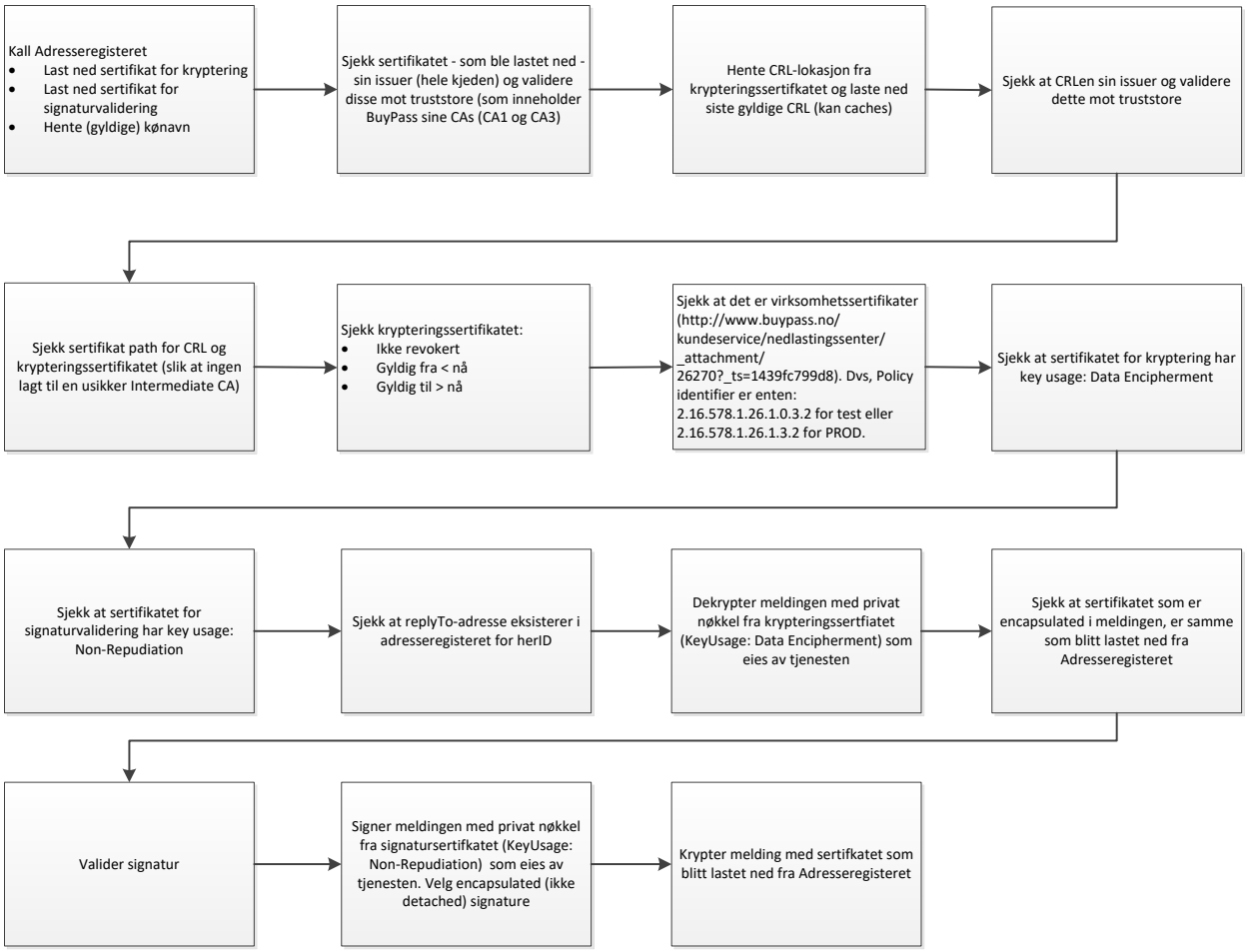
3.2 Asynkron, motta melding



3.3 Synkron, send og motta melding



3.4 Synkron, hent og send melding



3.5 Henting av meldinger fra AMQP-kø

Som en generell retningslinje bør mottaker av en melding la meldinger være på AMQP-køen til den er behandlet og respons sendt (enten som apprec eller til error kø). Dette for å forhindre at meldinger «forsvinner» dersom en fjerner meldingen fra AMQP-køen og så skjer det en feil før meldingen er levert.

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Postadresse
Postboks 6737
St. Olavs plass
0130 OSLO

postmottak@ehelse.no

ehelse.no