E-resept

Arkitektur

Versjon: 2.8
2. juni 2016

Dokumenteier: avdeling Produkt og Plan, seksjon Produkt og Veikart

Versj.	Dato	Kapittel	Endring	Produsenter
2.2	23.3.10	Alle	Dokumentet utgjør grunnlaget for v2.3.1	Jon Tysdahl
2.3	6.4.10	Alle	Innarbeidet EO51 og 52 og dokumentet utgjør grunnlaget for v2.4	Jon Tysdahl
2.4	15.04.11	Alle	Innarbeidet EO53, EO54 og diverse rettelser.	Henrik Paus
2.4	15.06.11	Alle	Innarbeidet kommentarer fra prosjektene	Henrik Paus
2.4.1	4.5.12	Kap 3.1, 4.3.2, 4.4, 5.2, 5.3, 8.5.2	Innarbeidet endringer knyttet til at M25 skal gå via Reseptformidleren	Jon-Are
2.4.2	07.05.12	Kap 3.1	Rette opp feil i skisse figur 2, figur 3, figur 4	Gustav Sletta
2.5	04.04.13	V2.5 endringer	Daglig HPR, fig 4, Søknadssvar fra Legemiddelverket på notifiseringer, Meldingsdefinisjonsendringer v2.4 og v2.5 til forankring	Gustav Sletta
2.6	16.04.13	V2.5 endr.	Er vedtatt i e-resept endringsrådsmøtet 2/5-2013, etter verifiseringsrunde.	Gustav Sletta
2.7	07.10.13	V2.5 endr	Oppdatert med nye endringer i 2.5	Ole Winnem
2.71	12.05.14	5.2, 5.3.1, 5.3.6; 5.3.5	EO 5166, Ny svarmelding M5.2; EO 5783 Fjerning av M27.3-4; EO 5526 Bruk av RefToParent i M25	Jon-Are Bækkelie
2.8	02.06.16	Hele	Feilretting. EO 6460 EO 7669.	Jon-Are Bækkelie

INNHOLDSFORTEGNELSE:

1 Innledning

1.1 Oppsummering

Dette dokumentet beskriver e-resept-arkitekturen.

Kapittel 1 beskriver dokumentets innhold, bakgrunn, formål og målgruppe.

Kapittel 2 presenterer en referansemodell for arkitektur tilpasset for e-resepts formål.

Kapittel 3 presentere løsningsarkitekturen.

Kapittel 4 presenterer løsningens overordnede sikkerhetsarkitektur.

Kapittel 5 presenterer integrasjonsarkitekturen.

Kapittel 6 gir en oversikt over informasjonsarkitekturen.

Kapittel 7 presenterer utviklings- og testmiljø.

Kapittel 8 presenterer driftsarkitekturen.

1.2 Bakgrunn

Gjennom e-reseptløsningen ble aktørene i reseptbehandlingen knyttet sammen gjennom elektronisk samhandling. Informasjon om legemidler og medisinsk forbruksmateriell og næringsmidler overføres fra Statens legemiddelverks løsning for Forskrivnings- og ekspedisjonsstøtte (FEST) til behandlende aktører og gi dem felles datagrunnlag for behandling av reseptinformasjon.

E-resept innførte en ny aktør i samhandlingen rundt resepter, Reseptformidleren, som tilgjengeliggjør resepter for utleverer og gir en rekke annen funksjonalitet. Reseptformidleren var ved etablering av e-resept forventet å formidle drøye 20 millioner resepter i året. I 2015 ble det formidlet litt over 22 millioner resepter.

Den samlede løsningen for håndtering av elektroniske resepter baseres på forskjellige systemer som er utviklet for å støtte den enkelte involverte profesjons funksjonelle behov.

Dette dokumentet inngår som en del av e-resepts dokumentasjon og bør leses i sammenheng med Overordnet funksjonell spesifikasjon (OFS), Detaljert funksjonell spesifikasjoner (DFS) og meldingsspesifikasjonene.

Disse sentrale dokumentene utgjør ikke en fullverdig beskrivelse av de løsninger som er utviklet/levert hos hver enkelt aktør, men danner et felles grunnlag for detaljspesifiseringen.

1.3 Formål

Arkitekturen i e-resept er utformet for å støtte e-resepts hovedmål:

Arkitekturdokumentet beskriver de rammer for kommunikasjon og krav til løsningen som er nødvendig for at denne skal ha tilstrekkelig sikkerhet, ytelse og tilgjengelighet slik at e-resepts hovedmål kan oppnås.

Dette dokumentet tydeliggjør samspillet mellom systemene og stiller krav til disse der dette er nødvendig for at løsningen samlet sett skal være sikker og tilby adekvat funksjonalitet.

Dokumentet er førende for implementering av systemer i det enkelte prosjekt og hos deres leverandører.

1.4 Målgruppe

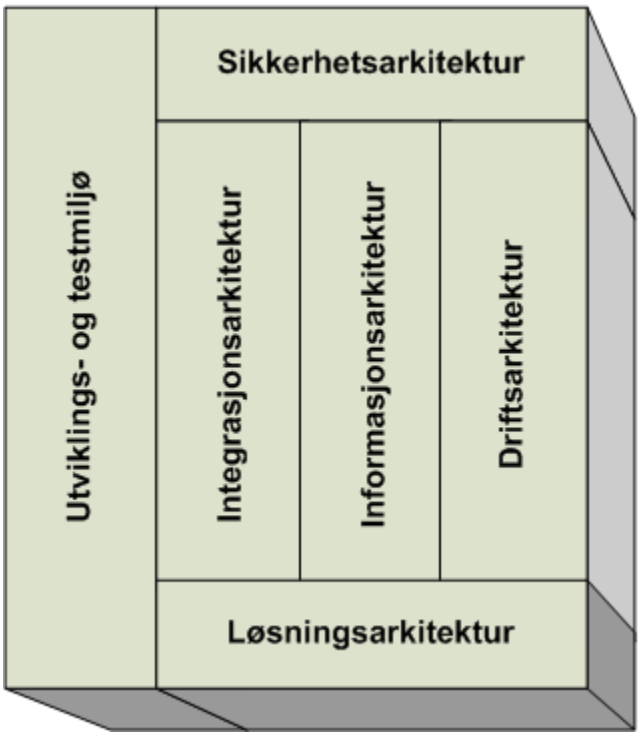
Dokumentets målgruppe er primært følgende aktører:

- e-resept aktører med deres leverandører
- Nye aktører som ønsker å sende elektronisk resept

I tillegg vil dokumentet også være relevant for eksterne instanser som ønsker informasjon om e-resepts arkitektur.

2 Begreper og referansemodell

For å strukturere den samlede arkitekturbeskrivelsen i e-resept har vi tatt utgangspunkt i en arkitekturmodell som er i bruk hos NAV og tilpasset den til e-resepts formål. Modellen er vist i figuren under:



Figur 1: Referansemodell for e-resept

Grunnen til at det er gjort tilpasninger er knyttet til ansvarsforhold for dokumentasjon som er delt mellom aktørene i e-resept. For enkelte aspekter er det nødvendig å etablere felles arkitekturstandarder for at e-reseptløsningen skal fungere. Disse felles aspektene for e-resept er beskrevet i dette dokumentet og utgjør et rammeverk for samhandlingen mellom aktørene. De felles deler som er beskrevet er følgende:

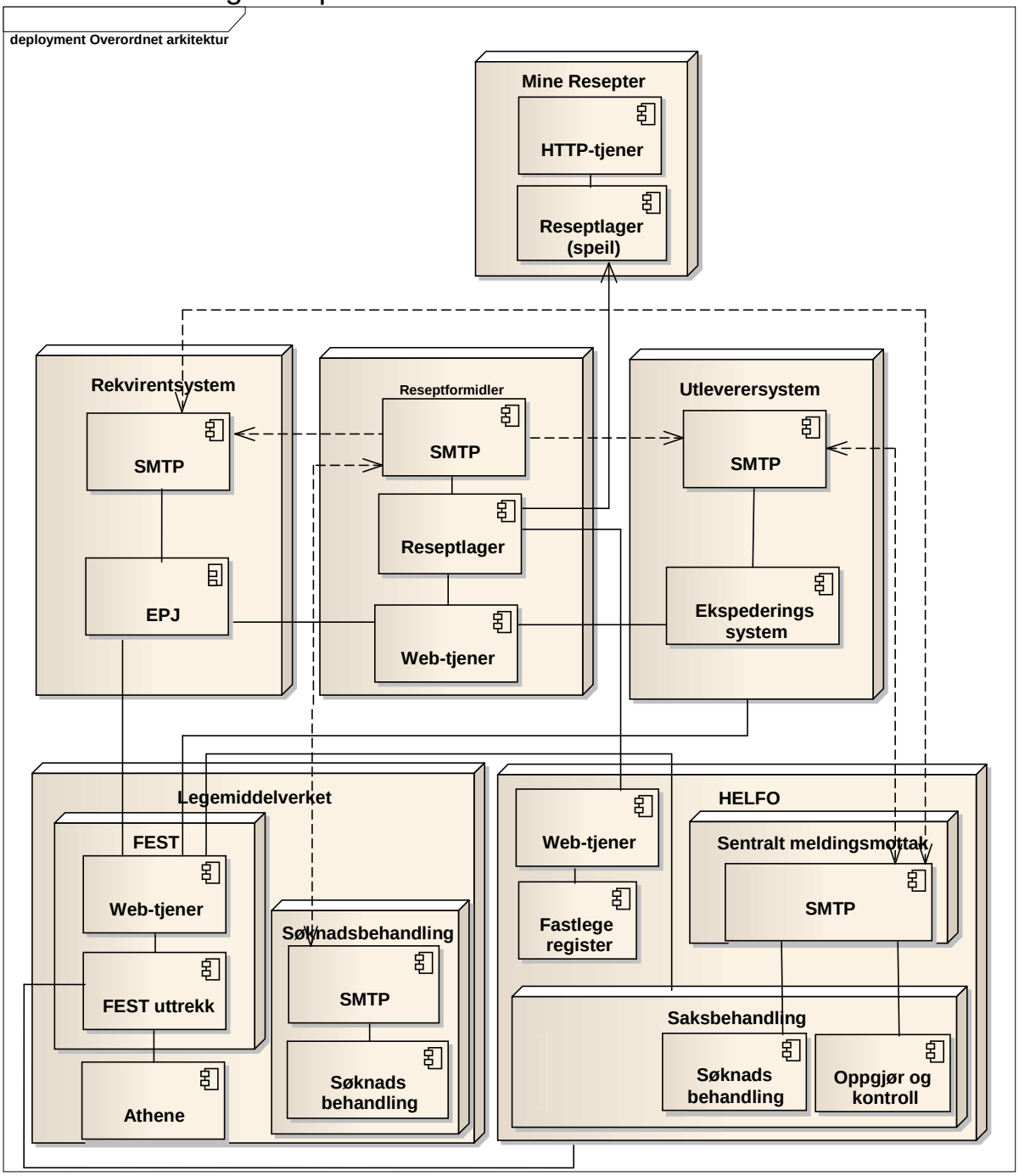
- Løsningsarkitektur (kap 3)
- Sikkerhetsarkitektur (kap 4)
- Informasjonsarkitektur (kap 5)
- Integrasjonsarkitektur (kap 6)
- Driftsarkitektur (kap 7)
- Utviklings- og testmiljø (kap 8)

Aspekter som Applikasjoner, Applikasjonsarkitektur, Prosesseringsarkitektur og Teknisk infrastruktur er ikke beskrevet, da dette anses å ligge innenfor den enkeltes aktør/leverandørs domene. Aspekter knyttet til aktører og roller er heller ikke beskrevet da disse anses å være behandlet tilstrekkelig i DFS.

3 Løsningsarkitektur

Dette kapittelet presenterer e-resept overordnede arkitektur. Først presenteres de løsningskomponenter (systemer) som inngår i meldingsutveksling knyttet direkte til behandling av elektroniske resepter og søknader. Deretter presenteres håndtering av grunndata.

3.1 Løsningskomponenter



Figur 2: Illustrasjon av systemer og meldingsflyt i e-resept.

I figuren er Web-tjener kommunikasjon illustrert med tynne linjer uten retningsangivelse. SMTP basert kommunikasjon er illustrert med stiplede linjer med retningsangivelse og overføring av reseptdata fra Reseptformidleren til Mine Resepter er illustrert ved linje med retningsangivelse. De ulike aktørsystemene, og løsningskomponentene, er presentert nedenfor. Web-tjener og SMTP er ikke presentert i eget kapittel. SMTP er identifisert hos parter som samhandler via denne teknologien. For å kunne samhandle er det nødvendig at begge parter støtter bruk av teknologien. Web-tjener er identifisert som komponent hos den aktøren som tilbyr tjenesten. Det er ikke identifisert en egen klient hos de aktørene som bruker Web-tjenere. I kapittel for integrasjonsarkitektur er det beskrevet i detalj hvordan samhandlingen skal være mellom de enkelte systemene og i kapittelet for informasjonsarkitektur er det beskrevet hvilken informasjon som formidles mellom systemene.

3.1.1 Statens legemiddelverk

3.1.1.1 FEST

FEST skal tilby en tjeneste hvor alle aktører åpent skal kunne hente ut nødvendig informasjon om relevante registrerte varer. Informasjonen om legemidler skal hentes ut av Legemiddelverkets saksbehandlingssystem Athene. Annen informasjon deriblant informasjon om medisinsk forbruksmateriell og næringsmidler blir tilgjengeliggjort av tredjepartsaktører. Statens legemiddelverk inngår avtaler med disse tredjepartsleverandørene om leveranse av informasjon som distribueres via FEST og tilrettelegger denne informasjonene uten å kvalitetssikre den. Kvalitetssikringen skjer dermed gjennom godkjenning av tredjepartsleverandør som leverandør av informasjon til tjenesten. Tredjepartsleverandørene som er inkludert i versjon 2 av FEST er HELFO, Farmalogg og Direktoratet for e-helse.

FEST skal støtte nedlasting av all informasjon og inkrementell nedlasting og er tilgjengelig i Norsk Helsenett.

3.1.1.2 Søknadsbehandling

Legemidler som ikke markedsføres i Norge kan ikke utleveres uten at legemiddelverket har godkjent utleveringen på individuell basis. Imidlertid har Legemiddelverket gjort en forenkling for alle legemidler med markedsføringstillatelse i EØS-området, USA eller land i PIC/S[1] og MRA[2]-avtale da disse kan forhåndsekspederes av apotek og hvor notifisering om utlevering sendes i ettertid.

I e-resept er søknad om godkjenningsfritak en mindre utvidelse av resepten som sendes til Reseptformidleren og hvor reseptformidleren enten sender søknaden videre til Legemiddelverket eller gjør den ekspederbar basert på informasjonen i resepten. Søknadsbehandling inneholder i så måte tre forskjellige typer søknader:

---

[1] *Består av følgende medlemsland: Australia, Østerrike, Belgia, Canada, Tsjekkia, Danmark, Finland, Frankrike, Tyskland, Hellas, Ungarn, Island, Irland, Italia, Latvia, Liechtenstein, Malaysia, Nederland, Norge, Portugal, Romania, Singapore, Slovakia, Spania, Sverige, Sveits og Storbritannia.*

[2] *Avtale med New Zealand, Australia, Canada og Sveits.*

- Søknad som er sendt fra rekvirent via Reseptformidleren til Legemiddelverket (kan ikke ekspederes før godkjenningsfritak er gitt).
- Søknad som sendes til Legemiddelverket fra apotek etter at de har funnet at de ikke kan ekspedere den før Legemiddelverket har godkjent utlevering.
- Notifisering om utlevering som sendes etter at apotek har utlevert legemiddelet.

For alle søknader som må behandles av Legemiddelverket blir det sendt svar til Reseptformidleren som videreformidler svaret til rekvirent og eventuelt apotek som har resepten under ekspedering. Kommunikasjon med Reseptformidleren skjer asynkront over Norsk Helsenett.

3.1.2 Rekvirentsystem

Rekvirentsystem skal tilby funksjonalitet som gjør det mulig for leger og andre med rekvireringsrett å rekvirere med synkron kommunikasjon mot RF fra lokalt epj-system og behandle informasjon om legemidler og andre varer som krever rekvirering på en effektiv og sikker måte. Rekvirentsystem skal støtte henting og bruk av FEST informasjon, og kommunikasjon med Reseptformidleren, HELFO og utleverere.

Nedlasting av FEST informasjon skal skje ved oppkobling mot FEST web-tjener via Norsk Helsenett. Kommunikasjon med HELFO skal skje via ebXML/SMTP over Norsk Helsenett og kommunikasjon med Reseptformidleren skal skje via Web-tjener og ebXML/SMTP over Norsk Helsenett. All kommunikasjon som initieres av Reseptformidleren sendes via ebXML/SMTP, mens kommunikasjon som initieres av rekvirentsystem skal utføres som synkrone meldinger mot RF.

3.1.3 Reseptformidleren

Reseptformidleren skal ha en sentral rolle i formidlingen av informasjon mellom aktørene i e-resept. Gjennom sin funksjon som formidler av reseptrelatert informasjon skal reseptformidleren ivareta målet om fritt valg av utleverer. Reseptformidleren skal ikke ivareta en arkivfunksjon. Informasjon om resepter skal fysisk slettes fra Reseptformidleren etter regler gitt i DFS 5.3.1.4.

Reseptformidleren skal ha en rolle som tiltrodd aktør knyttet til validering av reseptinformasjon som videreformidles til andre parter. Dette gjøres ved at Reseptformidleren knytter et objekt til resepter og dokumenterer hvilke formelle sjekker som er gjort i forhold til reseptens gyldighet i dette objektet.

Reseptformidleren skal tilby tjenester gjennom Web-tjener grensesnitt og den skal videreformidle informasjon via SMTP. Den skal kommunisere med rekvirent, utleverer, Legemiddelverket, Mine Resepter og Kjernejournal. For at Reseptformidleren skal kunne tilby adekvate tjenester, stilles det krav til kommunikasjon med flere registre. Kommunikasjon med disse registrene avhenger av hvilket grensesnitt de enkelte registrene støtter og hvilke krav til responstid og oppdatert informasjon som stilles ved bruk av tjenesten.

3.1.4 Utleverersystemer

Utleverersystemer (apotek- og bandasjistsystemer) skal støtte ekspedering av elektroniske resepter, rapportering av utlevering og oppgjør. Apotek skal i tillegg støtte søknad om godkjenningsfritak. Apotek som tilbyr multidosepakking skal støtte kommunikasjon av multidoseinformasjon, men dette kan være implementert i et eget pakkesentralsystem med en egen HER-id knyttet til apotekets HER-id .

Kommunikasjon med Reseptformidleren som initieres av utleverersystem skal bruke Web-tjener funksjonaliteten i Reseptformidleren, mens all annen kommunikasjon skal bruke SMTP.

3.1.5 Oppgjør- og kontrollsystem

HELFO skal kunne avgi informasjon som inneholder refusjonsberettigede handelsvarer til FEST. De skal også kunne motta FEST informasjon til sin oppgjørsløsning. Både avgivelse og mottak skal skje via ebXML/SMTP over internett.

3.1.5.1 Oppgjør og kontroll

Oppgjør og kontroll skal gi funksjonalitet for behandling av oppgjørskrav fra utleverer basert på innsendte krav og tilhørende resepter og utleveringsinformasjon. I tillegg skal funksjonalitet for kontroll av legers forskrivning kunne gjennomføres basert på utlevering og tilhørende resepter.

Kommunikasjon av oppgjørsinformasjon skal sendes via ebXML/SMTP over internett eller NHN.

3.1.5.2 Søknadsbehandling

HELFO skal kunne støtte behandling av elektronisk søknad om individuell refusjon. Kommunikasjon av søknadsinformasjon skal mottas via sentralt meldingsmottak via ebXML/SMTP over internett eller NHN.

3.1.5.3 Oppslag i Fastlegeregister

HELFO skal støtte funksjonalitet for oppslag i Fastlegeregisteret. HELFO skal tilgjengeliggjøre et slikt oppslag via en Web-tjener over internett og over Norsk Helsenett.

3.1.6 Mine resepter

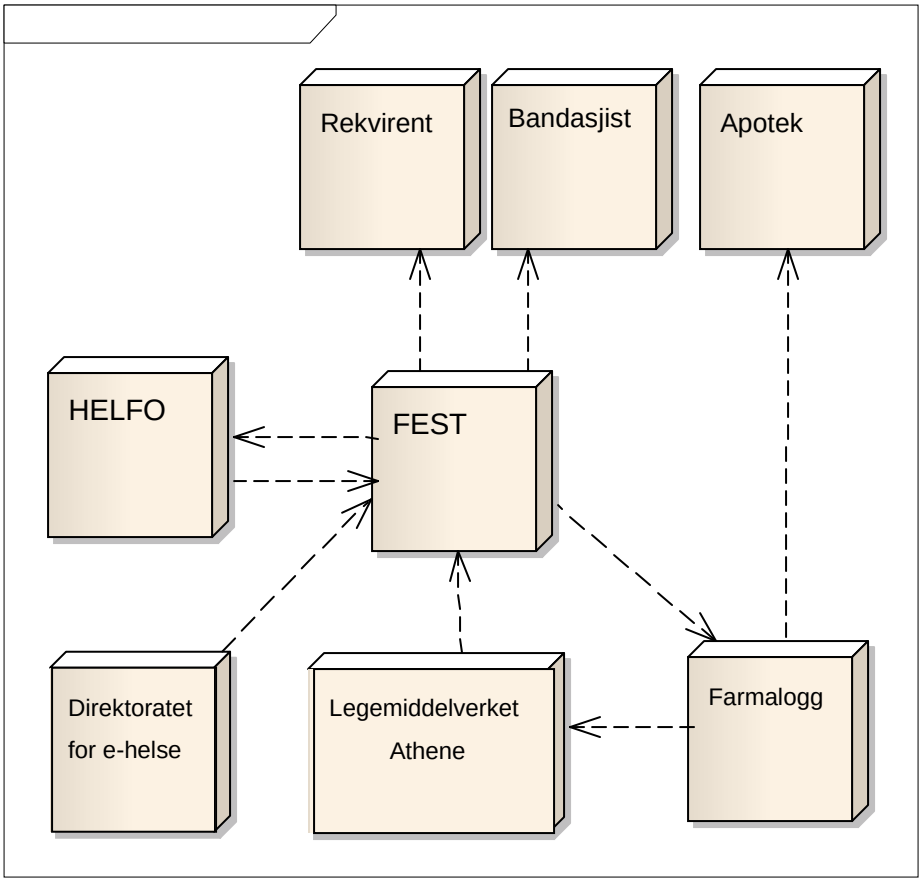
Mine resepter skal støtte funksjonalitet for sikkert oppslag i pasientens egne resepter via internett. Mine resepter er en adskilt tjeneste som skal speile informasjonen i Reseptformidleren slik at pasienter alltid kan få oppdatert oversikt over hvilke resepter som er tilgjengelig. Oppslag i Mine resepter skal skje via HTTPS og ved bruk av nettleser og nivå 4 autentisering.

3.2 Grunndata

Dette kapittelet beskriver grunndata som inngår i e-resept. I kapittel 3.2.1 beskrives faglig grunndataflyt og i kapittel 3.2.2 beskrives grunndataflyt om enheter.

3.2.1 Faglig grunndata

Faglig grunndata omfatter data om legemidler, næringsmidler, brystproteser og medisinsk forbruksmateriell. Illustrasjonen under viser utveksling av data mellom aktører i e-resept og aktører som bidrar med informasjon til FEST.

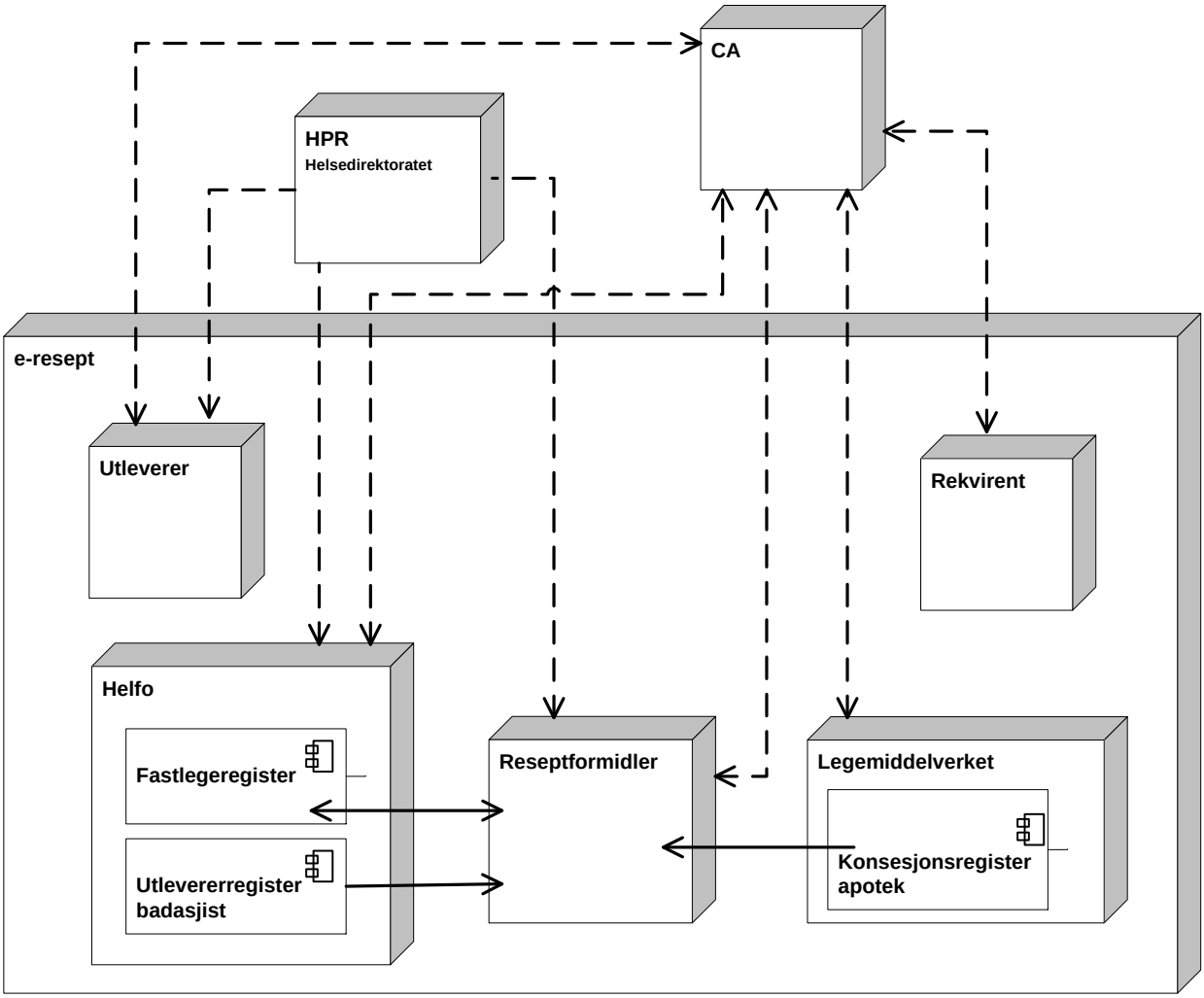


Figur 3: Overføring av faglig grunndata

Faglige grunndata til bruk i e-resept skal leveres av Legemiddelverket gjennom deres FEST tjeneste. Grunndata levert fra FEST skal kunne kombineres med andre grunndata i mottakersystemene. FEST skal innhente data fra tiltrodde relevante kilder som gjør FEST informasjon adekvat for den enkelte aktør. Informasjon om Legemidler skal baseres på informasjon fra Athene og kombineres med informasjon fra Farmalogg. Informasjon om Legemidler skal omfatte alle legemidler som har fått utdelt varenummer fra Farmalogg og finnes tilgjengelig i apotek. Legemiddelverket skal levere interaksjonsdata i FEST. Informasjon om handelsvarer blir hentet fra to kilder, Farmalogg skal levere alle handelsvarer som er relevant for multidosepakking og HELFO skal levere oversikt over pris og produkter som er refusjonsberettiget på blåresept (handelsvarer).

3.2.2 Grunndata om enheter

Grunndata om enheter er grunndata som brukes i verifisering av kommunikasjonsparter og meldinger. Disse dataene hentes ut fra ulike registre. Figuren under viser dataflyten mellom disse aktører og registre.



Figur 4: Flyt av grunndata om enhetsopplysninger i e-resept

Tabellen beskriver figuren over:

Fra	Til	Data	Frekvens
Adresseregisteret (HER)	Utleverer HELFO Rekvirent Legemiddelverket	Elektroniske adresser og pekere til sertifikater	Ved behov
Katalogtjeneste for PKI (CA)	Reseptformidleren Utleverer HELFO Rekvirent Legemiddelverket	CRL, fødselsnummer, sertifikater	Ved behov
HPR	Reseptformidleren, Utleverer HELFO	Uttrekk fra Helsepersonellregisteret: Rekvirentautorisasjon inkl. Rekvisisjons-/forskrivningsrett	Daglig oppdatering
Legemiddelverket (Konsesjonsregister)	Reseptformidleren	Konsesjonsregister apotek	En gang pr. døgn
HELFO (Fastlegeregister)	Reseptformidleren	Pasientens fastlege	Oppslag ved behov
HELFO (Utlevererregister)	Reseptformidleren	Liste over bandasjister med oppgjørsavtale med HELFO	Ved hver endring i avtaleinngåelsen mellom en bandasjist og HELFO

Tabell 1: Beskrivelse av Figur 4

Kommunikasjon av informasjon til registrene er ikke en del av e-resept og derfor ikke beskrevet.

3.2.2.1 Adresseregisteret

Adresseregisteret (HER) er en tjeneste i Norsk Helsenett som inneholder elektroniske adresser og/eller postadresser for alle brukere av Norsk Helsenett. Alle brukere skal være registrerte i Adresseregisteret og har selv ansvar for å holde egne opplysninger oppdatert. HER kan også inneholde adresser til parter som ikke er kunder av Norsk Helsenett AS. Adresseregisteret benyttes som grunnlag for meldingsutveksling i e-resept, og alle meldingsparter som inngår i e-resept skal være registrerte i Adresseregisteret.

Adresseregisteret skal i e-resept fungere for flere bruksområder eksempelvis

- Entydig å identifisere kommunikasjonspart
- Gi opplysninger om kommunikasjonsparametere som edi-adresser og sertifikater
- Identifisering av 3 part som skal refereres i fagmeldinger.

Når en rekvirent slutter, skal det meldes til Adresseregisteret. Tilhørende HER-Id vil da markeres som utgått.

Adresseregisteret er beskrevet mer fullstendig i www.nhn.no/hjelp-og-brukerstotte/adresseregisteret/veiledningerpdf/Om-Adresseregisteret.pdf.

3.2.2.2 Katalogtjeneste for PKI (CA[3])

Bruken av PKI (Public Key Infrastructure) i e-resept er basert på at de aktuelle PKI-leverandører har nødvendige katalogtjenester tilgjengelig i Norsk Helsenett. Disse tjenestene omfatter:

- Fødselsnummeroppslag
- Tilgang til revokeringslister (CRL)
- Sertifikatstatus i sanntid (OCSP)
- Nedlasting av meldingsparters sertifikater

3.2.2.3 Helsepersonellregisteret

Helsepersonellregisteret (HPR) vedlikeholdes av Helsedirektoratet.

HPR er et register over alt helsepersonell i Norge. Reseptformidleren, Legemiddelverket, utleverer og HELFO skal benytte et uttrekk av dette registeret for å autorisere rekvirenter. Oppslag i HPR basert på fødselsnummeret/D-nummeret til rekvirenten skal brukes for å knytte rekvirentens sertifikat til et HPR-nummer og for å bekrefte autorisasjon og rekvireringsrett.

Daglig oppdatering skal utføres.

3.2.2.4 Konsesjonsregister apotek

Konsesjonsregisteret er et register over alle de apotek som har gyldig konsesjon. Det er Statens legemiddelverk som gir og forvalter konsesjoner for apotekene. Registeret leveres av Statens legemiddelverk og vil inneholde apotekeiers organisasjonsnummer og apotekets konsesjonsnummer. Konsesjonsnummer blir gitt av legemiddelverket.

3.2.2.5 Fastlegeregister

Fastlegeregisteret inneholder koblingen mellom borgere og deres fastlege. Oppslag i Fastlegeregisteret skal gjøres ved bruk av Web-tjener hvor Reseptformidleren sender legens og valgt pasients fødselsnummer. Web-tjenesten returnerer ja/nei og en status.

Det er ett spesielt forhold rundt oppslag mot fastlegeregisteret for personer med fortrolig adresse, såkalt kode 6 eller 7 personer. Her vil oppslaget gi negativ tilbakemelding og det vil ikke være mulig å registrere samtykke til utleveringsrapport til fastlege for pasienter med fortrolig adresse.

---

[3] CA - Certificate Authority. En instans som publiserer sertifikater, revokeringslister og tilbyr fødselsnummeroppslag,

3.2.2.6 Utleverérregister

Registeret inneholder en oversikt over alle bandasjister som har oppgjørsavtale med HELFO.

3.3 Lover og forskrifter

De enkelte aktørene i e-resept forvalter en rekke sensitive personopplysninger, og forholder seg til aktuelt lovverk og forskrifter. Dette ansvaret endres ikke grunnleggende ved innføring av e-resept.

”Norm for informasjonssikkerhet i helsesektoren” inneholder en sammenstilling og operasjonalisering av krav og pålegg i gjeldende lovverk, og skal ligge til grunn for alle parters sikkerhetsarbeid i e-resept. Normen er en sektornorm, og alle virksomheter med tilkoblingsavtale til Norsk Helsenett forplikter seg juridisk til å overholde denne gjennom tilgangsavtalen.

4 Sikkerhetsarkitektur

4.1 Innledning

Sikkerhetsarkitektur brukes i dette dokumentet om forhold som er nødvendige for å oppfylle krav til informasjonssikkerhet: konfidensialitet, integritet, tilgjengelighet, kvalitet og sporbarhet.

Sikkerheten i e-resept skal ivaretas i en kjede som involverer mange selvstendige virksomheter med ulike IT-løsninger. Felles for disse aktørene er at de i dag eksisterer som virksomheter, er underlagt lovverk som regulerer krav til informasjonssikkerhet, og har etablerte rutiner for behandling av helse og personopplysninger. For Reseptformidleren er det i så måte etablert en egen forskrift (Reseptformidlerforskriften) som skal regulere dens behandling av informasjon.

4.2 PKI i e-resept

Bruken av PKI skal følge [KITH 1304] og [HIS 1037:2011], samt ”Kravspesifikasjon for PKI i offentlig sektor”.

En beskrivelse av PKI i e-resept er dokumentert i Vedlegg E.

4.3 Informasjonssikkerhet i e-resept

Fire av aspektene som er identifisert i sikkerhetsarkitekturen er definert i Norm for informasjonssikkerhet i helsesektoren. I tillegg stiller e-resept krav til sporbarhet. Med sporbarhet menes mulighet for å følge informasjon gjennom hele levetiden og mulighet for å finne logget informasjon som gjør det mulig å rekonstruere informasjonsflyten.

4.3.1 Konfidensialitet

I e-resept skal **konfidensialitet** under overførsel mellom aktørene sikres ved bruk av PKI-basert kryptering basert på mottagers virksomhetssertifikat.

Kryptering skal minst benytte ”3DES”, men partene må være i stand til å håndtere meldinger med nyere og sterke algoritmer.

4.3.2 Integritet

I e-resept skal **integritet** under overførsel mellom aktører sikres ved bruk av signering med avsenders virksomhetssertifikat.

Signering skal minst benytte ”SHA256” som hash-algoritme.

4.3.2.1 Meldinger med signatur på innholdsnivå

Meldinger fra rekvirent som skal påføres digital signatur på innholdsnivå med bruk av personlig sertifikat på nivå høyt, er:

- M1 Resept
- M2 Søknad om individuell refusjon
- M5 Tilbakekalling av resept
- M9.5 Forespørsel om resepter på pasient
- M9.11 Forespørsel om Legemidler i bruk
- M24.1 Samtykkeregistrering
- M24.3 Flytting av samtykker
- M25.1 Legemidler i bruk
- M27.1 Registrering av LIB-ansvarlig lege

Videre skal M18 signeres på innholdsnivå med utleverers virksomhetssertifikat.

M25.2 og M25.3 skal signeres på innholdsnivå med avsenders (utleverers) virksomhetssertifikat.

SKO, se kap 4.3.5.2, signeres på innholdsnivå med Reseptformidlerens virksomhetssertifikat. Tidsstempelet i SKO er signert med Reseptformidlerens tidsstemplingssertifikat.

4.3.2.2 Håndtering av nedetid hos CA

Reseptformidleren skal kontrollere at sertifikatet er gyldig og også slå opp hos CA og hente rekvirents personnummer for kontroll mot HPR. Gyldig sertifikat sjekkes mot CRL (sperreliste), mens personnummer hentes ved OCSP-oppslag online mot CA. For å sikre oppetid aksepteres at resultatet av OCSP-oppslaget caches i Reseptformidleren i inntil 24 timer. Dersom CA ikke er tilgjengelig er det mulig å benytte cachet verdi i inntil 24 timer til før Resepthåndteringen stanses opp. For CRL aksepteres at gammel CRL benyttes i maksimalt 12 timer etter at ny CRL skulle vært mottatt.

4.3.3 Tilgjengelighet

Pasientsikkerhet forutsetter at elektroniske resepter ikke bare er sikret mot innsyn og misbruk, men at de er tilgjengelige. Reseptinformasjon må være tilgjengelige når utlevereren eller rekvirenten har behov for innsyn. Dette stiller krav til rekvirent og utleverer system i tråd med gjeldende praksis, men viktigere er kravene til Reseptformidleren og Norsk Helsenett.

Reseptformidlerens skal driftes med krav om oppetid på 99,99 % målt på månedlig basis. Dette svarer til 4 minutters nedetid per måned. Reseptformidleren skal driftes fullt redundant, med doble nett-tilkoblinger til det nasjonale hovednettet i Norsk Helsenett. Det stilles også krav til at Norsk Helsenett driftes med 99,99 % tilgjengelighet på sine sentrale løsninger målt på månedlig basis.

4.3.4 Kvalitet

I e-resept skal kvalitet sikres ved felles datagrunnlag i FEST, strukturerte meldinger, bruk av hodemelding og bruk av kodeverk. Det stilles krav om at alle aktører i e-resept skal bruke FEST som

datagrunnlag og at faglig informasjon som finnes i FEST brukes som basis for meldingene der hvor dette er mulig.

Det stilles krav om at alle aktører i e-resept kvalitetssikrer informasjonen som er brukerdefinert og at det ikke skal være mulig å legge inn informasjon som fører til feil, eller at bruker unngår å legge inn informasjon i nødvendige felt. Til rekvirent stilles det krav om at reseptID IKKE skal endres ved resending av melding..

Videre stilles det krav til at alle aktører som skal kommunisere i e-resept skal godkjennes av NHN for sending og mottak av alle relevante meldinger, samt at det stilles krav til at alle aktører har vært gjennom e-resepts testregime.

4.3.4.1 Kontroll av signeringstidspunkt

Når dokumenter signeres av rekvirenten skjer dette uten at en tiltrodd tredjepart går god for at signeringen faktisk skjer på den dato som er angitt som forskrivningsdato. For å sikre at det ikke skrives resepter frem eller tilbake i tid skal Reseptformidleren sikre at differansen mellom reseptens forskrivningsdato og Reseptformidlerens systemklokke ved mottakstidspunktet ligger innenfor +/- 7 dager. Reseptformidleren skal avvise Resepter som den mottar, dersom avviket er større.

Reseptformidleren skal oppdatere sin systemklokke slik at den aldri er mer enn 1 sekund fra referansetiden (ntp.uio.no) og dokumentere tidspunkt for mottak av resept i SKO (se kapittel 4.3.5.2).

Denne datoen danner utgangspunktet for vurdering av reseptens gyldighet. Ved avvik mellom forskrivningsdato og reseptformidlerens systemklokke skal tiden angitt i SKO benyttes som utgangspunkt for beregning av siste tidspunkt for mulig utlevering.

4.3.5 Sporbarhet

Sporbarhet skal sikres med en kombinasjon av tre forskjellige mekanismer som samlet gjør det mulig å rekonstruere et forløp. Disse mekanismene er:

- Logging
- Opprettelse av SKO
- Lagring av dokumenter

4.3.5.1 Logging

Alle parter skal gjennomføre logging som er nødvendig for å overholde de regler for informasjonssikkerhet som normen for informasjonssikkerhet i Helsesektoren fastsetter.

Alle aktører skal logge alle inn- og utgående meldinger for å sikre sporbarhet av transaksjoner. Minimum skal alle aktører i forbindelse med meldingsmottak og forsendelse logge (eller på annen måte ta vare på):

- meldings-ID
- meldingspart (avsender/mottaker)
- tidspunkt

Logging i systemene skal videre sikre at eventuelt misbruk av opplysninger fra Reseptformidleren kan avdekkes. Dette stiller krav til at avsender av meldingene M9.1, M9.3, M9.11 og M10 logger hvilken bruker som sender meldingen.

I tillegg til krav om logging av meldinger og interaksjon med andre aktører er det også krav om logging av all systembruk utført av autorisert administrativt personale. Forsøk på uautorisert bruk skal også logges.

Krav til logging er ytterligere detaljert i e-resept detaljert funksjonell spesifikasjon (DFS).

I tillegg til loggingen vil signaturkontrollobjektet (SKO) overføre viktig informasjon om reseptens signering og gyldighet.

4.3.5.2 Opprettelse av SKO

Reseptformidleren skal for alle innkomne resepter opprette et Signaturkontrollobjekt (SKO) hvor Reseptformidleren dokumenterer hvilke tester som er gjennomført ved mottakelse av meldingen. Dette objektet skal så følge resepten i alle meldinger hvor resepten blir formidlet med unntak av M9.6 til rekvirent. Nærmere beskrivelse av SKO finnes i vedlegg G.

4.3.5.3 Lagring av dokumenter

Det er for partene i e-resept krav om dokumentasjonsplikt knyttet til flere lover og forskrifter. Hver part skal overholde dokumentasjonsplikter som er relevante for deres virksomhet og på den måten sikre sporbarhet for dokumenter i tidsrommet lover og forskrifter krever.

4.4 Utlevering av reseptopplysninger fra Reseptformidleren

Reseptformidleren er hjemlet i pasientjournalloven § 12 og tilhørende forskrift. Reseptformidleren forholder seg dessuten til gjeldende regelverk knyttet til behandling av sensitive personopplysninger.

Resepter og reseptopplysninger utleveres fra Reseptformidleren som resultat av forespørsler fra autoriserte avsendere etter regler som Reseptformidleren implementerer i tråd med lovhjemmel og forskrifter. De som kan få utlevert reseptopplysninger fra Reseptformidleren er rekvirent, utleverer, Legemiddelverket, Kjernejournal og pasient. Rutiner for tilgangskontroll i systemene disse aktørene bruker må utformes med tanke på å hindre urettmessig tilgang til informasjon utlevert fra Reseptformidleren. Det gjelder spesielt hos utleverer og Legemiddelverket der autentisering overfor Reseptformidleren med personlig PKI ikke benyttes. Brukerapplikasjon må implementere mekanismer som sørger for sikker knytning til et gitt individ og logging av dette når det sendes meldinger til Reseptformidleren.

4.4.1 Rekvirenter

Utlevering fra Reseptformidleren til rekvirent skal skje på grunnlag av pasientens fødselsnummer og/eller referansenummer. Rekvirent må signere med personlig signatur ved forespørsel om å få utlevert informasjon fra Reseptformidleren.

Rekvirent vil motta utleveringsrapporter fra Reseptformidleren og fastlege vil, basert på pasientens samtykke registrert i Reseptformidleren, kunne motta utleveringsrapport fra Reseptformidleren.

4.4.2 Utleverer

For å ekspedere en elektronisk resept må ansatte hos utleverer få utlevert resepten fra Reseptformidleren. Utlevering fra Reseptformidleren til utleverer skal bare skje etter at utleverer har etterspurt informasjon på en gitt pasient. Utleverer kan etterspørre informasjon på grunnlag av:

- Kundens fødselsnummer
- Kundens navn og fødselsdato
- Kundens referansenummer
- Fonetisk søk på kundens navn og fødselsdato

Dersom pasienten har bedt om låst resept hos rekvirent, skal ikke resepten utleveres fra Reseptformidleren uten at utleverer har oppgitt referansenummeret i sin forespørsel til Reseptformidleren.

4.4.3 Legemiddelverket

Reseptformidleren sender søknader og notifiseringer om unntak fra markedsføringstillatelse til Legemiddelverket. Legemiddelverket har ansvaret for å sikre at bare autentiserte og autoriserte brukere med tjenestelig behov for å behandle disse opplysningene får tilgang.

4.4.4 Innsyn fra pasienten

Pasienten har rett til innsyn i egne resepter som er lagret i Reseptformidleren. Dette skal bare skje gjennom oppslag med høyt personlig sikkerhetsnivå i Mine resepter og ved henvendelse til utleverer eller rekvirent.

4.4.5 Annet personell

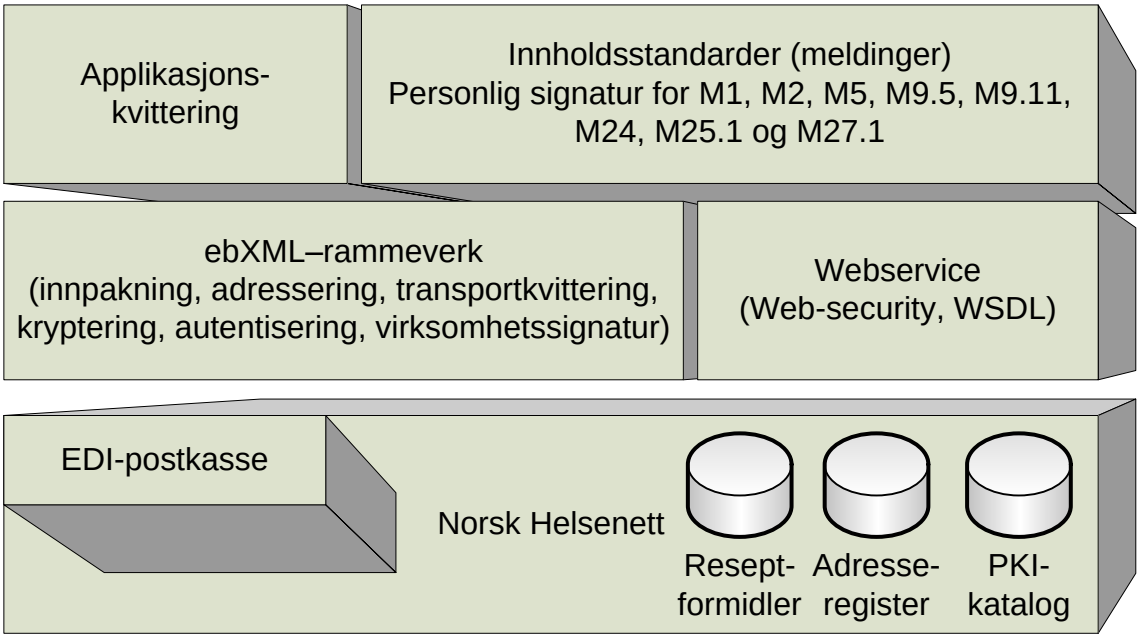
Annet personell kan ikke få utlevert informasjon fra Reseptformidleren.

Teknisk personell som arbeider med forvaltning og drift av Reseptformidleren kan få tilgang til data i Reseptformidleren. Slik tilgang skal reguleres gjennom databehandlingsavtaler.

5 Integrasjonsarkitektur

5.1 Standardisert meldingsutveksling

Det grunnleggende prinsippet i e-resept er at det overføres meldinger mellom partene. Mottaker behandler en melding basert på avsenders identitet, innholdet i meldingen og gjeldende forretningsregler. Etter endt behandling sendes svar tilbake til avsender. Prinsippet om meldingsbasert integrasjon gjelder uavhengig av transportprotokoll. Noe som medfører at forretningsmessig innhold ikke endres basert på transportprotokoll. e-resept benytter to metoder for transport; ebXML over SMTP (asynkron) og Webservices over HTTP (synkron).



Figur 5: Referansemodell for meldingsutveksling

5.2 Meldinger og samhandlingsprotokoller

Dette kapittelet inneholder en oversikt over hvilke meldinger som kan sendes over hvilke samhandlingsprotokoller.

Tabellen viser hvilke transportprotokoller som tilbys for de ulike meldingene.

Meldinger og transportprotokoller		
asynkron	**synkron**	**Beskrivelse**
	M1	Resept fra rekvirent til Reseptformidler
M2		Søknad om individuell refusjon
	M3	Anmodning om søknad til Legemiddelverket. Sendes fra apotek til Reseptformidler
	M4.1, M4.2	Sekvens for å hente referansenummer, mellom rekvirent og Reseptformidler
	M5, - M5.2	Tilbakekalling av resept, fra rekvirent til Reseptformidler Kvittering på tilbakekalling resept, fra Reseptformidler til rekvirent
M7		Informasjon fra Reseptformidler til rekvirent om slettet resept
M6, M8		Utleveringsrapport fra Reseptformidler til rekvirent/fastlege
	M9.1-M9.4	Utleverers forespørsel om og nedlasting av resepter, sekvens mellom Utleverer og Reseptformidler
	M9.5-M9.6	Leges forespørsel om resepter, sekvens mellom rekvirent og Reseptformidler
	M.9.11-M9.12	Forespørsel om Legemidler i bruk, sekvens mellom apotek/rekvirent og Reseptformidler
	M9.21-M9.22	Forespørsel om endrede multidosepasienter mellom apotek og reseptformidler
	M10	Utleveringsrapport, fra utleverer til Reseptformidler
M12		Søknadssvar individuell refusjon
M14		Søknad om godkjenningsfritak til Legemiddelverket. Sendes fra Reseptformidler til Legemiddelverket.
M15		Søknadssvar fra Legemiddelverket. Sendes fra Legemiddelverket til Reseptformidler. Samme melding sendes også fra Reseptformidler til rekvirent/utleverer.

M18		Oppgjørskrav, fra utleverer til HELFO. Denne meldingen skal være komprimert.
M20		Notifisering Sendes fra Reseptformidler til Legemiddelverket
M21		Ekspederingsanmodning. Baseres på informasjon i M1 og sendes fra Reseptformidler til utleverer
M22		Oppgjørsresultat, fra HELFO til utleverer
M23		Utbetalingsmelding, Fra HELFO til utleverer
	M24.1 – M24.2	Samtykkeregistering fra rekvirent til Reseptformidleren Svar samtykkeregistering fra Reseptformidleren til rekvirent.
	M24.3	Flytting av samtykker til ny organisasjon. Fra rekvirent til reseptformidleren.
M24.4 og M24.5		Flyttede samtykker, sendes fra reseptformidler til rekvirents nye og gamle organisasjon.
	M25.1	Legemidler i bruk, melding fra rekvirent til Reseptformidleren.
M25.2 og M25.3		Legemidler i bruk, melding fra Reseptformidleren til rekvirent
	M25.2 og M25.3	Legemidler i bruk, melding fra apotek til Reseptformidleren
	M27.1-M27.2	Registrering av multidoseapotek/LIB-ansvarlig lege. Melding fra rekvirent og apotek til Reseptformidleren. Svar, sendes fra Reseptformidleren til rekvirent og apotek
M28		Endring av LIB-ansvarlig lege. Melding fra Reseptformidleren til rekvirent.
	M30	FEST-meldingen fra FEST til HELFO, rekvirenter, bandasjister og Farmalogg. Meldingen brukes også til å overføre produkt- og prisliste fra HELFO til FEST.
	MV	Verifiseringsmelding for å sjekke kobling mot RF. Kan brukes av alle aktører.

Tabell 2: Protokoller for ulike meldinger.

5.3 Forsendelse av en melding

Samtlige meldinger i e-reseptløsningen skal besvares enten med en applikasjonskvittering (AppRec) eller med en direkte svarmelding (fagmelding). Applikasjonskvittering slik den er definert i vedlegg B, referanser skal benyttes.

5.3.1 Bruk av applikasjonskvittering

Tabellen under viser en oversikt over hvilke meldinger som skal benytte applikasjonskvittering, og hvem som er avsender og mottager. I tillegg er det en oversikt over hvilke kodeverk som skal benyttes i applikasjonskvitteringen. I tabellen er Reseptformidler forkortet RF.

Meldingstype		Avsender melding	Mottaker melding	AppRec	Kodeverk
Nr.	**Navn**				
M1	Resept	Rekvirent	RF	AppRec	8221 og 7419
M2	Søknad om individuell refusjon	Rekvirent	HELFO	AppRec	8221
M3	Anmodning om søknad til Legemiddelverket	Apotek	RF	AppRec	8221 og 7419
M4.1	Forespørsel om referansenummer	Rekvirent	RF	AppRec (kun hvis negativ, ellers M4.2)	8221 og 7419
M5	Tilbakekalling av resept	Rekvirent	RF	AppRec (kun hvis negativ, ellers M5.2)	8221 og 7419
M6	Utleveringsrapport Rekvirent	RF	Rekvirent	AppRec	8221
M7	Slettet resept i Reseptformidleren	RF	Rekvirent	AppRec	8221
M8	Utleveringsrapport Fastlege	RF	Fastlege	AppRec	8221
M9.1	Forespørsel om resepter på pasient	Utleverer	RF	AppRec (kun hvis negativ, ellers M9.2)	8221 og 7419
M9.3	Forespørsel om nedlasting av resept	Utleverer	RF	AppRec (kun hvis negativ, ellers M9.4)	8221 og 7419
M9.5	Forespørsel om resepter på pasient	Rekvirent	RF	AppRec (kun hvis negativ, ellers M9.6)	8221 og 7419
M9.11	Forespørsel om Legemidler i bruk	Rekvirent/ Apotek	RF	AppRec (kun hvis negativ, ellers M9.12)	8221 og 7419
M9.21	Hent endrede multidosepasienter	Apotek	RF	AppRec (kun hvis negativ, ellers M9.22)	8221 og 7419
M10	Utleveringsrapport	Utleverer	RF	AppRec	8221 og 7419
M12	Søknadssvar individuell refusjon	HELFO	Rekvirent	AppRec	8221
M14	Søknad om godkjenningsfritak til Legemiddelverket	RF	Legemiddel-verket	AppRec	8221 og 7419
M15	Søknadssvar fra Legemiddelverket	Legemiddel-verket RF RF	RF Rekvirent Apotek	AppRec AppRec AppRec	8221 og 7419
M18	Oppgjørskrav	Utleverer	HELFO	AppRec	8221

M20	Notifisering	RF	Legemiddel-verket	AppRec	8221
M21	Ekspederingsanmodning	RF	Utleverer	AppRec	8221
M22	Oppgjørsresultat	HELFO	Utleverer	AppRec	8221
M23	Utbetalingsmelding	HELFO	Utleverer	AppRec	8221
M24.1	Samtykkeregistrering	Rekvirent	RF	AppRec (kun hvis negativ, ellers M24.2)	8221 og 7419
M24.3	Flytting av samtykker	Rekvirent	RF	AppRec	8221 og 7419
M24.4	Endringer av samtykke i RF	RF	Rekvirent	AppRec	8221
M24.5	Informasjon om flyttede samtykker	RF	Rekvirent	AppRec	8221
M25.1	Legemidler i bruk (LIB)	Rekvirent	RF	AppRec	8221 og 7419
M25.2	Legemidler i bruk (LIB)	Apotek RF	RF Rekvirent	AppRec AppRec	8221 og 7419
M25.3	Legemidler i bruk (LIB)	Apotek RF	RF Rekvirent	AppRec AppRec	8221 og 7419
M27.1	Registrering av multidoseapotek/LIB-ansvarlig lege	Rekvirent Apotek	RF RF	AppRec (kun hvis negativ, ellers M27.2)	8221 og 7419
M28	Endring av LIB-ansvarlig lege	RF	Rekvirent	AppRec	8221
MV	Verify	Alle aktører	RF	AppRec	8221 og 7419

Tabell 3: Oversikt over AppRec knyttet til meldinger

Mottak og sending av applikasjonskvitteringen skal alltid logges. Applikasjonskvitteringer som inneholder avvik skal gi varsel i sluttbrukerapplikasjonen (feilmelding). System som skal motta AppRec må ha rutiner for hva som skjer når den uteblir, rutinene skal være i tråd med standard for meldingsutveksling i helsesektoren.

For meldinger som har svarmelding brukes svarmeldingen, ved applikasjonsfeil sendes en AppRec og ved kommunikasjonsfeil sendes en fault melding på transportnivå. Ved M1, M3, M10, M24.3, M25.1, M25.2, M25.3 og MV som er synkrone meldinger, sendes likevel alltid AppRec.

5.3.2 Kodeverk for AppRec

Det skal benyttes kodeverk i AppRec. Disse skal brukes både for applikasjonkvittering over SMTP og over HTTP. Følgende kodeverk skal benyttes i e-resept:

- Standard statuskodene i AppRec
- Kodeverk 8221, Generelle feilmeldingskoder
- Kodeverk 7419, Feilmeldingskodeverk for e-resept

Alle som skal motta en AppRec må således kunne støtte standard-statuskodene i AppRec.

- Ok
- Ok, men med melding om avvik
- Avvist, med melding om avvik

Ved feilmelding kan det også oppgis tilleggsinformasjon ved bruk av XML-attributtet OT, men det skal ikke sende tekniske feilmeldinger i OT-feltet. RF benytter seg bare av første og siste kode.

Eksempel på feilmelding med tilleggsinformasjon:

<Error S='2.16.578.1.12.4.1.1.8221» V=»E20» DN=»Lege finnes ikke» OT=»Legen har sluttet»/>

5.3.3 Håndtering av manglende AppRec eller transportkvittering

Hvis (positiv eller negativ) AppRec er mottatt på applikasjonsnivå, skal videre manglende transportkvitteringer ignoreres. På transportnivå vil det fortsatt etterspørres transportkvitteringer, men dette dør ut av seg selv

Hvis negativ AppRec er mottatt, må avsender lage ny melding med ny meldingsid (med bedre innhold) og sende den. Å sende samme melding på nytt vil ikke gi bedre resultat.

Hvis AppRec ikke er mottatt må det sees på om transport er OK eller ikke. Å sende samme meldingen på nytt bør unngås, med mindre det gjøres tiltak for å løse kommunikasjonsproblem i mellomtiden.

Hvis ingen AppRec og ingen transportkvittering foreligger etter resendinger, kan det konstateres et kommunikasjonsproblem som må håndteres (manuell inngripen). Om det skal resendes med gammel eller ny melding må avklares mellom partene. Hvis meldingen aldri har kommet frem, kan meldingen sendes på nytt med samme ID.

Dersom avsender av en AppRec ikke har fått transportkvittering på denne, så anses dette å være mottagers (av AppRec) sitt problem og avsender gjør ikke noe mer med dette, utover å vente på trensportkvittering.

For M21 ekspederingsanmodning er det spesielle rutiner ved manglende AppRec eller transportkvittering. Dette er beskrevet i vedlegg H.

5.3.4 Adressering

HER-id brukes som gjennomgående identifikator i meldingsutveksling i e-resept. HER-id kan slås opp i Adresseregisteret for å finne/verifisere oppdatert adresseinformasjon for mottager, peker til sertifikater og for å verifisere at HER-id fortsatt er gyldig. Ved sending med ebXML skal avsender sjekke at den har gyldig CPA med mottaker.

Alle meldinger skal inneholde organisasjonens HER-id.

5.3.5 Referanser mellom meldinger i en dialog/sekvens

Det benyttes flere ulike mekanismer for å referere mellom meldinger, iht. krav fra Avdeling Standardisering i Direktorat for e-helse, (Standardisering) og ebXML standarden.

ConversationRef

Klassen ConversationRef sendes ikke med i første melding i en dialog. For alle meldinger som etterfølger en annen melding, er denne klassen obligatorisk.

I tilfeller hvor det er dialoger av meldinger skal det refereres til første melding i dialogen og forrige melding i dialogen. Til dette benyttes henholdsvis feltene ”RefToConversation” og ”RefToParent” i klassen ConversationRef i hodemeldingen.

I feltet «RefToParent» skal MsgId til den forrige meldingen i dialogen stå. Eksempelvis:

M9.2: referanse til M9.1

M9.3: referanse til M9.2

M9.4: referanse til M9.3

M10: referanse til M9.4 (gjelder for ALLE M10 i en dialog)

I feltet «RefToConversation» skal alltid MsgId til den første meldingen stå. Eksempelvis:

M9.2: referanse til M9.1

M9.3: referanse til M9.1

M9.4: referanse til M9.1

M10: referanse til M9.1

RefToParent

Når det ikke velges noen resepter så skal det sendes en M9.3 (kansellering) for hver reseptliste i M9.2. M9.3 skal da inneholde en referanse til M9.2 listen: RefToParent (M9.2) i hodemeldingen, pluss kanselleringskoden. Det er dermed RefToParent som blir benyttet som referanse i meldingen (ikke reseptid eller referansenummer)

RefToParent og RefToConversation fylles ut i alle M10, ved ekspedering på samme resept.

Ved reekspederinger hvor apotek starter å sende en M9.3 kan dette

løses med følgende:

RefToParent:

M9.4: referanse til M9.3

M10: referanse til M9.4

RefToConversation:

M9.4: referanse til M9.3

M10: referanse til M9.3

For M25 meldingene gjelder følgende.

RefToParent skal inneholde referanse til siste M25.1/2/3 som Reseptformidleren mottok. M9.12 kan inneholde både M25.1, M25.2 og M25.3, og mottagersystemet kan da finne hvilken av disse som Reseptformidleren mottok sist ut i fra RefMsgId i M9.12. Denne skal benyttes som RefToParent når M25 meldinger sendes inn.

Når RF videresender M25.2 og M25.3 til LIB ansvarlig, så endres RefToParent til å referere til meldingen som ble mottatt fra apotek. RefToConversation beholdes uendret og peker på forrige M25 som ble levert til RF.

5.3.6 Avgrensning av en meldingskonversasjon

Omfanget av en meldingskonversasjon i ebXML er bestemmende for bruk av flere kommunikasjonsparametere i en meldingsutveksling.

Spørsmålet om hvor lang dialog en ConversationID kan dekke besvares ikke entydig hverken i Rammeverket til Standardisering eller i OASIS ebXML-standarden. Begge steder åpnes det for at en dialog kan inneholde flere meldinger.

Det benyttes følgende utstrekning av konversasjoner i e-resept i betydning lik ConversationID på ebXML-nivå: Asynkrone meldinger og den tilhørende AppRec skal ha samme ConversationID.
For referanser internt i fagmeldinger til tidligere meldinger i samme konversasjon (RefToConversation) benyttes følgende utstrekning av referanser.

Konver-sasjon	Melding 1	Melding 2	Melding 3	Melding 4	Melding 5	Melding 6	Melding 7	Melding 8
M1	M1	AppRec M1						
M1/M21	M1	AppRec M1	M21	AppRec M21	M9.3	M94/AppRec M9.3		
M1/M15	M1	AppRec M1	M14	AppRec M14	M15	AppRec M15	M15 Rek/Utl	AppRec M15
M5	M5	M5.2/AppRec M5	M7	AppRec M7				
M4.1	M4.1	M4.2 / AppRec M4.2						
M24.1	M24.1	M24.2 / AppRec M24.2						
M24.4	M24.3	AppRec	M24.4	AppRec				
M24.5	M24.3	AppRec	M24.5	AppRec				
M9.5	M9.5	M9.6 / AppRec M9.6						
M91/M3	M9.1	M9.2 / AppRec M91	M9.3	M9.4 / AppRec M93	M3	AppRec M3	Forts. i Melding 3 for M1/M15	
M9.1/M6	M9.1	M9.2 / AppRec M91	M9.3	M9.4 / AppRec M93	M10	AppRec M10	M6	AppRec M6
M9.1/M8	M9.1	M9.2 / AppRec M9.1	M9.3	M9.4 / AppRec M93	M10	AppRec M10	M8	AppRec M8
M9.1/M20	M9.1	M9.2 / AppRec M9.1	M9.3	M9.4 / AppRec M9.3	M10	AppRec M10	M20	AppRec M20
M9.11	M9.11	M9.12/ AppRec M9.11	M9.3	M9.4 / AppRec	M10	AppRec M10	Som M9.1 alternativer	

M9.21	M9.21	M9.22/ AppRec						
M2	M2	AppRec M2	M12	AppRec M12				
M18	M18	M22	M23					
M25.1	M25.1	AppRec M25.1	Se regler i meldingsdokument					
M25.2	M25.2 Apotek-RF	AppRec M25.2	M25.2 RF-rekvirent	AppRec M25.2	Se regler i meldingsdokument			
M25.3	M25.3 Apotek-RF	AppRec M25.3	M25.3 RF-rekvirent	AppRec M25.3	Se regler i meldingsdokument			
M27.1	M27.1	M27.2	M28	AppRec M28				
MV	MV	AppRec						

Tabell 4: Utstrekning av referanser – RefToConversation

5.3.7 ebXML over SMTP - asynkron

Bruken av ebXML baseres på “Rammeverk for elektronisk meldingsutveksling i helsevesenet, HIS 1037:2011”

5.3.7.1 Sikker leveranse

Leveringssikkerhet baseres på rammeverket ebXML. Det innebærer at partene automatisk sender transportkvitteringer for mottatte meldinger mellom sine respektive meldingssentraler.

Ved uteblitt transportkvittering på forsendelse skal meldingen flyttes til en feilhåndteringsmekanisme hos avsender. Det er avsender som er ansvarlig for å sørge for at mottaker får en melding og for å iverksette manuell avvikshåndtering ved manglende transportkvittering. Når det er konstatert at opprinnelig melding er gått tapt i kommunikasjonen, skal det skje en manuell eskalering (etter et antall timer). Opprinnelig melding må da kunne resendes (manuelt).

For å sikre mottak av komplett melding skal mottaker kontrollere at mottatt XML er velformet. Dette gjelder også for meldinger mottatt som vedlegg.

5.3.7.2 Resending

Frekvensen for resending på transportnivå settes for den enkelte mottaker. Dette bestemmes ved å sette tre ebXML parametre;

- Retry interval = Tid mellom hvert forøk på resending.
- Retry count = Antall resendingsforsøk
- Eskaleringstid = Tiden frem til avsender eskalerer overfor mottaker.

Parametrene settes i henhold til tabellen under for kommunikasjon fra en hvilken som helst part til hver av partene:

	Apotek	**Rekvirent**	**Bandasjist**	**SLV**	**RF**	**HELFO**
Retry interval	1 time	4 timer	4 timer	1 time	1 time	3 timer
Retry count	4 ganger	4 ganger	4 ganger	4 ganger	4 ganger	4 ganger
Esk. Tid	24 timer	100 timer	100 timer	24 timer	6 timer	24 timer

For M21 ekspederingsanmodning gjelder egne rutiner som beskrevet i vedlegg H.

5.3.8 Kommunikasjonsavtaler (CPA)

I kommunikasjon mot Reseptformidleren, jobbes det per dags dato på følgende måte i stedet for CPP/CPA: Dersom en aktør ønsker å kommunisere mot Reseptformidleren, må dette initieres manuelt overfor Reseptformidleren. Det er nødvendig å etablere en kommunikasjonsavtale(CPA) i Reseptformidleren for kommunikasjonsmotparten. Kommunikasjonsavtalen identifiseres ved hjelp av en unik ID, CPAid. CPAid i Reseptformidleren spesifiseres på følgende måte: CPAid :== <laveste_herid>'_'<høyeste_herid>'_'<løpenr>.

For å kunne opprette en kommunikasjonsavtale i Reseptformidleren for kommunikasjonsmotparten, må følgende informasjon om kommunikasjonsmotparten registreres og eventuelt oppdateres i Adresseregisteret:

- Virksomhetens navn
- Virksomhetens HER-id
- Virksomhetens EDI-adresse
- Virksomhetens sertifikat

Reseptformidleren henter denne informasjonen fra adresseregisteret, lagrer denne i RF sin aktørtabell og tildeler deretter en CPAid. Kommunikasjonsmotparten aktiveres deretter som en gyldig aktør i e-resept.

5.3.9 Webservice over HTTP - synkron

Generell meldingsstruktur for alle synkrone meldinger er.

```
<complexType name="Mx">
  <sequence>
    <element name="dokument" type="anyType" minOccurs="1" maxOccurs="1"/>
  </sequence>
</complexType>
```

Meldingen inneholder kun elementet dokument som inneholder melding Mx i sin helhet (fagmeldingen) som beskrevet xsd'er. Encoding er alltid UTF-8 og meldingsversjonen leses ut av namespace.

Web-services i e-resept baseres på SOAP v1.1.

Web-services tilbys som beskrevet i WSDL for den enkelte aktør. Webservices for overføring av meldinger med sensitive personopplysninger baseres på WS-security (WS-SEC).

5.4 Nettverk

Kommunikasjon av helseopplysninger skal som hovedregel finne sted over nett som er sikret med egne tiltak, slik som lukkede bransjenett. Ved meldingsutveksling har den enkelte involverte aktør ansvar for at løsningen oppfyller Norm for informasjonssikkerhet i helsesektoren.

5.4.1 Norsk Helsenett

Norsk Helsenett er et lukket bransjenett og leverer nettjenester til alle aktører i helsesektoren. Helseforetak og legekontorer skal bruke Norsk Helsenett for kommunikasjon i e-resept. FEST, Reseptformidleren og Legemiddelverkets søknadsmottak skal være tilgjengelig i Norsk Helsenett.

5.4.2 Andre bransjenett

Alle apotek og noen få bandasjister er knyttet sammen i Norsk Apoteknett og skal bruke dette nettet som sin primære nettforbindelse mot Espire. Fra Espire til Reseptformidleren skal det kommuniseres via Norsk Helsenett.

Bandasjistene knyttes til Reseptformidleren ved at hver bandasjist knyttes direkte til Norsk helsenett.

5.4.3 Reseptformidlerens nettforbindelse

Reseptformidleren vil være knyttet til Norsk Helsenett. Av sikkerhetsgrunner vil Reseptformidleren ikke ha en kobling til Internett.

”Mine resepter” skal gjøre det mulig for en pasient å be om utlevering av egne opplysninger som finnes i Reseptformidleren via en Internettforbindelse. Sikkerheten ved bruk av Mine resepter er ivaretatt ved at brukeren må benytte personlig sertfikat på nivå 4.

5.4.4 HELFO

HELFO vil utveksle meldingene M18, M22, og M23 over Internett og Norsk Helsenett. Når HELFO mottar M18, vil svarene M22 og M23 sendes til avsender på samme nett som ble benyttet for meldingen de mottok.

6 Informasjonsarkitektur

6.1 Innledning

I e-resept er det lagt vekt på at informasjon og modellelementer skal kunne gjenbrukes. FEST modellen danner i så måte grunnlaget for store deler av informasjonen i andre meldinger. Videre er det lagt vekt på å samordne modeller i e-resept med nasjonale modeller utviklet av Standardisering. Det er også lagt vekt på bruk av kodeverk der hvor dette er mulig.

I alle meldinger er Hodemeldingen en integrert del i den spesifikke meldingen, og denne benyttes som en felles byggekloss med basisinformasjon. Hvilke deler av Hodemeldingen som skal benyttes for de enkelte meldingene er beskrevet i 6.2.1 og dokumentert i meldingsdokumentasjonen for e-resept.

Følgende gjelder generelt for implementering av meldingene i e-resept:

- Det skal ikke brukes norske tegn i tagger i XML (XSD)
- Vedlegg kodes med base64.
- ISO/IEC 10646/Unicode tegnsett med UTF-8 koding skal brukes
- Ved bruk av kodeverk skal kodeverdien være med i meldingen
- GUID genereres etter RFC4122, brukes som meldings-ID og resept-ID (M1s meldings-id = resept-ID)

I delkapitlene under er overordnede modeller og prinsipper beskrevet, men detaljerte informasjonsmodeller er utelatt i dette dokumentet og beskrevet i de enkelte meldingsbeskrivelsene.

6.2 Meldingsoppbygging

Alle fagmeldinger i e-resept benytter seg av et standardisert meldingshode, beskrevet i Standard for hodemelding [HIS 1037:2011]. En melding skal bestå av en Hodemeldingsdel, en fagmeldingsdel og en signatur og sertifikatdel som vist i Figur 6.

Figur 6: Meldingsinnhold i e-resept

6.2.1 Krav til utfylling av hodemelding i e-resept.

Tabellene nedenfor viser hvilke attributter i hodemeldingen som skal være utfylt.
M angir at feltet alltid må være utfylt. S angir at feltet skal være utfylt dersom feltet er tilgjengelig i avsendersystemet. K Angir at feltet kan være utfylt. Det skal være oppgitt maksimalt en ident av hver type på hver enhet i hodemeldingen.
Hodemeldingen skal alltid inneholde avsender og mottaker av meldingen. Tabellen nedenfor viser hvordan Organisasjon skal være utfylt i Avsender og Mottaker elementet.

Attributt i hodemeldingen	**Rekv. Lege-kontor**	**Rekv. HF**	**Apotek**	**Multi-dose Apotek**	**Banda-sjisjt**	**Resept-formidleren**
Organisasjon (nivå 1)						
OrganisationName (nivå 1)	M	M	M	M	M	M
Ident: HER (nivå 1)	M	M	M (resept-mottak)	M (e-dose-mottak)	M	M
Ident: RESH (nivå 1)		M				
Ident: ENH (nivå 1)	M	M	M	M	M	
Ident: AKO (nivå 1)			M (konse-sjonsnr)	M (konse-sjonsnr)	M (løpe-nr)	
Address (nivå 1)	M	M	M	M	M	
TeleCom (nivå 1)	M	M	M	M	M	
Organisasjon (nivå 2)						
OrganisationName (nivå 2)		K				
Ident: RESH (nivå 2)		K				

Alle meldinger som sendes fra EPJ (rekvirentsystem) skal i avsender, og alle meldinger som sendes til et EPJ (rekvirentsystem) skal i mottaker, inneholde helsepersonell med ett og bare ett HPR-nummer. Meldingene MV og M4.1-2 skal likevel ikke inneholde helsepersonell. Fødselsnummer/D-nummer for rekvirent skal bare oppgis i M2 og M12.

Attributt i hodemeldingen	
HealthcareProfessional	
FamilyName	M
MiddleName	S
GivenName	M
Ident: HPR	M

Pasient skal være med i alle meldinger med unntak av: M4.1-2, M9.1-2, M9.3-4, M9.21-22, M18, M22, M23 og MV.

Attributt i hodemeldingen	
Patient	
FamilyName	M
MiddleName	S
GivenName	M
Ident: FNR/DNR	S
DateOfBirth	Skal være utfylt hvis FNR/DNR mangler eller DateOfBirth ikke kan avledes derav.
Sex	Skal være utfylt hvis FNR/DNR mangler.
Address	M
TeleCom	S

6.2.2 Identifikatorer i meldinger og kobling mot virksomhetssertifikat

For utleverer stilles det krav om at en enhet skal kunne identifiseres entydig og at avsenderID i hodemeldingen fylles ut adekvat. Det må være samsvar mellom hva som er fylt ut i meldingen og i virksomhetssertifikatet. Dette fører til følgende alternative utfyllinger:

- Apotek
    - ENH fylles ut med det organisasjonsnummer som finnes i SERIAL NUMBER fra virksomhetssertifikats emne/subject felt.
    - HER fylles ut med virksomhetens HER-id i Adresseregisteret
    - AKO fylles ut med Konsesjonsnummer
    - LOK fylles ut med OU[4] fra virksomhetssertifikat i meldinger til Helfo hvis dette er fylt ut i virksomhetssertifikatets emne/subject felt.
- Bandasjist
    - ENH fylles ut med det organisasjonsnummer som finnes i SERIAL NUMBER fra virksomhetssertifikats emne/subject felt.
    - HER fylles ut med virksomhetens HER-id i Adresseregisteret
    - AKO fylles ut med bandasjist løpenummer
    - LOK fylles ut med OU[5] fra virksomhetssertifikat i meldinger til Helfo hvis dette er fylt ut i virksomhetssertifikatets emne/subject felt.

[4] OU: Organisation Unit – et attributt i virksomhetssertifikatet

[5] OU: Organisation Unit – et attributt i virksomhetssertifikatet

Bandasjister må være registrert i utleverérregisteret på angitt organisasjonsnummer. Apotek må være registrert i konsesjonsregisteret på angitt organisasjonsnummer og konsesjonsnummer. Organisasjonsnummeret til apoteket i konsesjonsregisteret tilhører apotekkonsesjonær.

For virksomheter som er del av en kjede skal kjedens organisasjonsnummer fylles ut i Serial number og utleverers (apoteket eller bandasjist) organisasjonsnummer fylles ut i OU-feltet i virksomhetssertifikatet. Ellers fylles kun Serial number ut med organisasjonsnummer og LOK utelates.

6.2.3 Vedlegg i meldinger

Vedlegg i meldinger håndteres i henhold til dokumentet Vedlegg til meldinger, www.kith.no/upload/6348/1036-2011-VedleggTilMeldinger.pdf

Vedlegg skal videre base64 enkodes for å sikre en korrekt behandling. Dette gjelder også for vedlegg av typen kundens signatur eller andre på spesielle formater. Eksempel på dette finnes sammen med meldingsdefinisjonene.

I tillegg skal det i meldingen M18 oppgjørskrav til Helfo på kundens signatur benyttes compression mode 1.

6.2.4 Krav til meldingsinnhold i e-resept

Krav som gjelder for alle meldinger:

- Det skal generellt ikke være tomme elementer i en melding. Spesielt gjelder det for:
  - Alle elementer av type PQ skal inneholde både V og U attributter med innhold
  - Alle elementer av type CV skal inneholde både DN, V og S attributter med innhold
  - Alle elementer av type CS skal inneholde både V og DN attributter med innhold
- Det skal ikke brukes verdier som overstiger krav til maksimalt feltlengde

Til M1 stilles det i tillegg følgende krav:

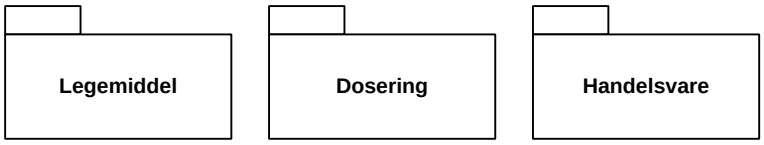
- Det kan bare benyttes paragraf 2, 3 og 4 og H-resept hjemmel 905 på legemidler
- Det kan bare benyttes paragraf 5 på medisinsk forbruksmateriell
- Det kan bare benyttes paragraf 6 på næringsmilder
- Det kan ikke sendes resept på kosttilskudd
- Det kan ikke sendes resept på brystprotese

- I en legemiddelresept skal minimum følgende felter være oppgitt
    - Alle felt som er obligatorisk i meldingen
    - Antall eller Mengde
    - DosVeiledEnkel og/eller Dosering
    - Bruk
    - PakningsinfoResept (gjelder legemiddelpakning)
- I en legemiddelresept skal følgende felter fra FEST IKKE være med
    - Preparatomtaleavsnitt
    - Hjelpestoff
    - Reseptgyldighet
    - ProduktInfo
    - RefVirkestoff
    - SortertVirkestoffMedStryke
    - AdministreringLegemiddel
    - PakningsByttegruppe
    - Refusjon
    - Opioidsoknad
    - TypeSoknadSlv
    - RefVilkar
    - Ean
    - IkkeKonservering
    - Pakningsinfo
    - PrisVare
    - Markedsforingsinfo
- I en resept på næringsmidler skal minimum følgende være oppgitt:
    - Varegruppekode
    - RefHjemmel (§6)
    - ProdGruppe
- I en resept på medisinsk forbruksmateriell skal minimum følgende være oppgitt:
    - Varegruppekode
    - RefHjemmel (§5)
    - ProdGruppe
- I ReseptDokHandelsvare skal det ikke oppgis vare hvis ikke dette er eksplisitt oppgitt i strukturerte refusjonsvilkår i FEST

6.3 Sentrale informasjonsmodeller

6.3.1 Generell forskrivningsmodell

For å sikre konsistens mellom meldinger som helt eller delvis inneholder det samme, er det laget en generell modell for forskrivning, som gjenbrukes i alle meldinger hvor det er behov for å beskrive en forskrivning. Dette gjelder meldingene M30, M1, M2, M6, M8, M10, M20 og M25. I tillegg er M1 et vedlegg i meldingene M15 og M18 slik at forskrivningsmodellen må kunne tolkes av alle parter i e-resept.



Figur 7: Forskrivning

Legemiddel er en modell som inneholder relevante klasser som skal være med i forskrivning av legemiddel. Ved forskrivning av legemiddel kan også modellen for Dosering inkluderes. Denne inneholder detaljert informasjon om dosering av det enkelte legemiddel. Alternativ til å forskrive Legemiddel er å forskrive Handelsvare og modellen for Handelsvare inneholder informasjonen som skal være med i en forskrivning av handelsvare. Rekvirent skal bare foreskrive handelsvarer som er refusjonsberettiget.

6.4 Kodeverk

Alle kodeverk som benyttes i e-resept har en egen OID (Object IDentifier) og er registrert på Volven. Disse er referert til med et firesifret OID-nummer. Dette er kun de fire siste sifrene i det komplette OID-nummeret. Mer utfyllende beskrivelse av kodeverkene som benyttes i e-resept finnes i dokumentet ”Kodeverk i e-resept”.

7 Utviklings- og testmiljø

Utviklings- og testmiljøet vil være spesifikt for den enkelte virksomhet. Disse skal være i henhold til de øvrige arkitekturbestemmelsene i dette dokumentet. Noen krav til utviklings- og testmiljø følger av at Direktoratet skal gjennomføre akseptansetest av nye versjoner av systemene i e-reseptkjeden der det er utført endringer i e-reseptfunksjonalitet samt i avtaler med den enkelte leverandør.

7.1 Test- og godkjenningsordningen

Test- og godkjenningsordningen skal avvikles og erstattes av nye tjenester hos NHN. Nettadressen og epostadressen til NHN validering er oppdatert. Kapitlet vil ellers oppdateres når de nye tjenestene blir publisert.

7.1.1 Bakgrunn

Test- og godkjenningsordningen er etablert i regi av Standardiserings- og samordningsprogrammet og Nasjonal IKT. NHN står som ansvarlig for utvikling og drift av ordningen.

Test- og godkjenningsordningen skal hjelpe leverandører og brukere å implementere nasjonale standarder for meldingsutveksling. Målet er å sikre at meldinger kan sendes på standardisert format fra avsendersystem til mottakersystem uavhengig av hvem som har levert de forskjellige systemene.

7.1.2 Tjenestene som i dag tilbys gjennom Test- og godkjenningsordningen

Test- og godkjenningsordningen består av en test- og en godkjenningsdel.

Alle e-resept meldinger inngår i ordningen og EISI skal utvikle en valideringsfil og én akseptansetest for disse. Valideringsfilen brukes for at leverandørene skal kunne kjøre en automatisert test av sin implementering av meldingen ved hjelp av en testserver som driftes av EISI. Mer informasjon om de automatiserte testene finnes på nettsidene til EISI.

I forbindelse med implementering besvarer EISI spørsmål fra leverandørene knyttet til implementering av meldingene og bruk av Test- og godkjenningsordningen.

Godkjenning av en meldingsimplementering gjennomføres ved at EISI går igjennom en egenerklæring og mottatte eksempelfiler i henhold til casebeskrivelsen fra akseptansetesten, og verifiserer at eksempler fra leverandøren er riktig implementert. Denne prosessen gjentas inntil innsendt materiale fra leverandøren har tilfredsstillende kvalitet.

Når en leverandør er godkjent oppdateres statussiden for Test- og godkjenningsordningen på EISI sin hjemmeside.

7.1.3 Ressurser

Under er relevante lenker til resurser i Test- og godkjenningsordningen:

Testmateriale	På denne siden ligger informasjon om akseptansetestene som skal brukes i forbindelse med e-resept
NHN validering testsenter@nhn.no	NHN validering brukes for å teste e-reseptmeldingene som utvikles Dersom leverandør har spørsmål angående enhetlig bruk og korrekt implementering av nasjonale standarder for meldingsutveksling brukes denne linken
Godkjenninger	Her finnes en oversikt over godkjente meldinger og meldinger som er under testing
Bruk av akseptansetester	Her forklares hvordan man skal bruke akseptansetestene.
Krav til godkjenning av akseptansetester	Her forklares prosessen med godkjenning av akseptansetester
Hva er meldingshjelp	Her forklares hvordan man bruker meldingshjelp, samt gjennomgang av vanlige spørsmål til meldingshjelp.
Om testserver	Her forklares bruken av testserveren

8 Driftsarkitektur

Dette kapittelet beskriver hovedtrekk ved drift og forvaltning av e-reseptløsningen.

8.1 Generelle krav knyttet til drift

8.1.1 Ansvar

Den enkelte part har selv ansvaret for å etablere og drifte sin del av e-reseptløsningen.

For rekvirenter og utleverere finnes det flere ulike systemer som kan anvendes og ulike leverandører. Det er opp til den enkelte aktør å velge system og avtale driftspartner.

8.1.2 Meldingsversjoner

Oversikt over hvilke versjoner av meldinger som til enhver tid er tillatt brukt skal utarbeides og vedlikeholdes. Reseptformidleren spiller en nøkkelrolle i verdikjeden i e-resept og forvaltning av denne skal sees i sammenheng med forvaltning av meldingene. Standardisering skal ivareta en sentral funksjon i forhold til å etablere nye meldingsstandarder.

Hvis en avsendende part prøver å sende melding med utgått versjon så skal mottaker avvise meldingen.

Partene plikter å avstemme endringer med de andre aktørene i så god tid i forkant av endringer, at alle aktører kan gjennomføre forutgående tester, før endringer settes i produksjon. De eksakte kravene til forvaltningsregime vil avtales mellom partene som en del av det videre arbeidet. Se også punkt 8.3.

8.1.3 Protokollversjoner

Over tid vil aktuelle versjoner av standarder og protokoller for meldingsoverføring og PKI måtte forventes å endre seg. Overgang til nye standarder vil være underlagt sentral kontroll i samarbeid mellom partene.

8.2 Drift av sentrale komponenter

8.2.1 Reseptformidleren

Oppetid på Reseptformidleren er 24/365. Reseptformidleren var ved etablering av e-resept beregnet å skulle kunne behandle 300 millioner transaksjoner pr år. Responstidskravet for enkelte av meldingene er så lavt som mindre enn 1 sekund for 90 % av transaksjonene.

8.2.2 FEST

Legemiddelverket skal sikre drift i henhold til kravene i DFS herunder tilkobling til Norsk Helsenett.

8.2.3 Meldingsmottak Legemiddelverket

Legemiddelverket vil sikre drift innenfor vanlig kontortid, og håndtering av meldingsmottak hele døgnet. Det vil være oppetid 24/7 på teknisk nivå, men det garanteres kun kl. 8-16 på applikasjonsmessig nivå (og dermed AppRec).

8.2.4 Meldingsmottak NAV

Meldingsmottaket hos NAV skal ha 24/7 oppetid

8.2.5 Meldingsmottak apotek

Sentralt meldingsmottak (Transportkvitteringer) med oppetid på 24/7. AppRec kommer fra det enkelte apotek hele døgnet, men kan ha litt nedetid pga feil.

8.2.6 Meldingsmottak bandasjist

Bandasjist har i sin løsning meldingsmottak koblet til manuell håndtering av innkommende meldinger. Ardis vil gi transportkvittering så lenge maskinen er på, men det å skru av maskinen kan medføre at de ikke får meldinger.

8.2.7 Meldingsmottak rekvirent

Rekvirentsystemene vil ha meldingsmottak som er tilnærmet 24/7, men det kan være unntak og nedetid.

8.3 Vedlikehold av meldinger

Dette kapittelet er ment som en oppsummering av viktige forhold knyttet til versjonshåndtering av meldinger innen e-resept.

8.3.1 Generell endringshåndtering av meldinger

Direktoratet for e-helse ivaretar endringshåndtering i e-resept. Standardisering vil spille en rolle knyttet til ajourhold og publisering av meldinger.

Endringer i meldinger faller inn som en del av en generell endringshåndtering. Endringer av e-resept skal styres av Direktoratet for e-helse-. En versjon vil omfatte et sett med sammenhengende dokumentasjon av løsningen, både arkitekturmessig, funksjonelt og meldingsmessig. På den måten er det enkelt for aktørene å se helheten i en endring.

Endringer håndteres gjennom rutine for endringshåndtering som Direktoratet for e-helse er ansvarlig for. Beskrivelse av endringsrutinen foreligger i eget dokument.

8.4 Dokumentasjon av endringer i dokumentasjon

Alle endringer i dokumentasjonen publiseres påehelse.no. I tillegg vil hver part informeres særskilt om endringen som en del av endringsregimet. Dette gjelder alle endringer i dokumenter som:

- OFS
- DFS
- Arkitekturdokumentet
- Meldingsdokumentasjon
- Kodeverk

Innføring av endringer i e-resept må sees i sammenheng med regelendringer og andre absolutte krav til endringer.

8.4.1 Spesielt om meldingsdokumentasjon

Følgende gjelder for publisering av nye versjoner av meldingsdokumentasjon.

Logisk versjonsnummer
Logisk versjonsnummer er det nummeret som endringen er publisert under. Dette nummeret økes med 0.1 ved hver versjon.

Publisering
På området som tilhører det logiske versjonsnummeret plasseres innholdet i en zip-fil med samtlige meldingsdokumentasjonsdokumenter i gjeldende versjon. Zip-filen er merket med en oppdatert dato. Mens meldingsversjonen er under utvikling kan det publiseres forskjellige zip-filer med samme versjonsnummer men forskjellig dato. Både de dokumenter som ikke er endret og de som er endret publiseres. Endrede dokumenter får ny dato og dermed nytt namespace. Namespace skal alltid endres ved den minste endring i en meldingsdefinisjon. Både word-fil, pdf-fil, xsd og eksempelmelding skal publiseres. De enkelte meldingsdokumenter kan ha andre versjoner enn det logiske versjonsnummeret for denne versjonen.

Spesielle forhold
Ved enhver endring som påvirker xsd-fil skal ny xsd-fil med nytt NameSpace publiseres. For meldinger som er vedlegg til andre meldinger vil det refereres til NameSpace som entydig referanse til meldingens versjon.

For hver melding skal det entydig angis hvilken versjon av MsgHead som benyttes.

8.4.2 Spesielt om vedlikehold av kodeverk

e-resept benytter tre hovedtyper av kodeverk:

1. Kodeverk utviklet av e-resept
2. Bransjekodeverk forvaltet av Standardisering
3. Bransjekodeverk ikke forvaltet av Standardisering

Kodeverkene av type 1 og 2 er publisert på www.volven.no. Kodeverk av type 3 er referert til på Volven.

Kodeverkene av type 1 og 2 er lagret i en database og et nedlastingssystem foreligger på http://testserver.kith.no/tool/.

Det er viktig å være klar over at noen kodeverk er enkle, og har lite logikk i løsningene knyttet til seg, mens andre kodeverk innebærer mye logikk hos partene.

Kodeverk vil i en driftssituasjon normalt være statiske. Det hender dog at man utvider eksisterende kodeverk med nye koder.Kodeverk av type 1 kan distribueres gjennom M30. Dersom utvidelsen innebærer funksjonelle endringer, må annen dokumentasjon også endres i samsvar med endringsrutinen.

Forvaltning av kodeverk i e-resept følger til enhver tid gjeldende endringsrutine og beskrivelser i dokumentet kodeverk i e-resept.

8.5 Håndtering av flere meldingsversjoner i parallell

8.5.1 Behov

I e-resept er det forventet at meldingene over tid vil måtte endres noe. Det er to grunnleggende forhold knyttet til versjonshåndtering av meldinger i e-resept, som må tas hensyn til:

- **Resepten varer lenge**
  - Den grunnleggende meldingen i e-resept er resepten (M1), som også inngår som vedlegg i flere meldinger. Denne meldingen har gyldighet på opp til tre år, hvilket innebærer at endring av M1 innebærer at e-resept i lang tid må kunne håndtere både gammel og ny versjon av M1, også som vedlegg i flere andre meldinger og i alle berørte systemer.
  - Utleveringsrapporten M10 har også en levetid og gjentas som vedlegg i nye meldinger (bl.a. M9.4 og M9.6), som gir tilsvarende argumentasjon.

- **Aktørene bytter ikke systemversjoner helt samtidig**
    - For rekvirentene og for utleverernе vil det ikke kunne sikres fullstendig samtidig overgang til nye systemversjoner for alle aktører. For utleverere forventes at alle i løpet av en forholds vis kort periode kan bytte systemversjon. For rekvirentene vil en slik periode være lenger, både på grunn av antallet leger og antallet involverte systemer. Vi kan derfor ikke forvente at alle aktørene kan bytte systemversjon samtidig, og vil derfor ved innføring av nye meldinger, måtte håndtere overgang mellom nye og gamle meldingsversjoner i en kombinasjon mellom manuelle rutiner og systemstøtte.

8.5.2 Løsning

Følgende prinsipper knyttet til håndtering av nye endringsversjoner gjelder.
Rutiner og prosedyrer:

1 Det skal vedlikeholdes en oversikt over hvilke meldingsversjoner som støttes i e-resept og sammenhengene mellom disse. Sammenhengene mellom hodemelding, meldingsversjon på en melding, tilhørende svarmelding og evt. AppRec klargjøres som en del av dette på standardisert format og publiseres av Direktoratet for e-helse. Det skal også angis krav til støtte for versjon på bilag og versjon på konvolutten.

2 Det må verifiseres/testes at aktuelle aktører håndterer meldinger med andre meldinger som vedlegg med blanding av gammel og ny M1. Testcase for å sikre håndtering av flere M1-versjoner i parallell må utvikles.

3 Det må også verifiseres/testes at rekvirent og utleverer håndterer M9.6 og M9.4 med blanding av gammel og ny M10. Testcase for å sikre håndtering av flere M10-versjoner i parallell må utvikles.

4 Det må også verifiseres/testes at rekvirent og utleverer håndterer M9.12 med blanding av gammel og ny M25. Testcase for å sikre håndtering av flere M25-versjoner i parallell må utvikles.

5 Konsekvenser av meldingsendringer for M1 og M10, må alltid sees i sammenheng med M9.4, M9.6 og M18. Konsekvenser av meldingsendringer for M25, må alltid sees i sammenheng med M9.12. Revisjon av den generelle forskrivningsmodellen må alltid sees i en større sammenheng; M30, M1, M10 og M25.

6 Konsekvenser av endringer i de andre meldinger kan sees på mer isolert, men eventuelle konsekvenser for andre meldinger og funksjoner hos aktørene må vurderes.

7 Serveren til Test- og Godkjenningsordningen må utvikles til å håndtere kombinasjoner av godkjente meldingsversjoner som vedlegg for de relevante meldinger.

Design av meldinger og funksjonalitet

1 E-resept aktørene må sikre at leverandørene etterlever og forstår de momenter som gjelder for håndtering av versjoner i parallell.
2 Meldingsversjon skal inngå som en del av alle meldinger, uansett hvordan disse er implementert. NameSpace benyttes for dette formålet.
3 For M1 må det være støtte for alle gyldige resepter uansett versjon, dvs. 3 år og 6 måneder (pluss etterslep inntil siste legekontor har byttet versjon) gammel versjon av M1 må støttes i M18, også i påfølgende meldinger, se også neste punkt.
4 En endring i M1 skal ikke nødvendigvis medføre endring i M9.4 (kan også påvirke M9.2), M9.6 og M18.
5 En endring i M10 skal ikke nødvendigvis medføre endring i M9.4 og M9.6.
6 En endring i M25 skal ikke nødvendigvis medføre endring i M9.12
7 For meldinger som sendes ut til mange ulike aktører, for eksempel M21, M6, M8, kan det forutsettes at mottager støtter nyeste versjon av meldingen, slik at avsender ikke behøver å holde rede på meldingsversjon. Det vil vurderes om Adresseregisteret kan utvikles på sikt for å støtte dette.
8 For meldinger på ny versjon som sendes aktører med gammel versjon kan dette gjøres forståelig ved å oversende skjema for visning av meldingen som en del av meldingen. Dette punktet er spesielt viktig for M21, hvor det er viktig at mottaker agerer ut fra meldingen. En mekanisme for dette kan være å gjenkjenne melding mot NameSpace og dermed vite hvilken type melding, og så søke å lese med siste kjente versjon.

Innføring av endrede versjoner

1 Direktoratet for e-helse beslutter i samarbeid med aktørene hvilke meldingsversjoner som skal være gyldige
2 Ved innføring av nye meldingsversjoner må innføringen av støtte for dette starte bakerst i den delen av verdikjeden som berøres. Dersom en endring påvirker M18, må HELFO først ha støtte før utleverene må ha støtte, deretter Reseptformidleren og til slutt rekvirent og evt. SLV.
3 Å sende meldinger basert på nyversjon følger verdikjeden, men det forutsettes at støtte er implementert i henhold til rekkefølgen som angitt i punkt 1.

Vedlegg A: Foreliggende dokumentasjon

Innenfor og i tilknytning til e-resept er det utarbeidet en rekke dokumenter som på ulike nivåer og detaljeringsgrader spesifiserer løsningen for elektroniske resepter i Norge. Arkitekturdokumentet utgjør således sammen med en rekke andre dokumenter den samlede spesifikasjon av e-reseptløsningen.

Disse dokumentene er listet opp nedenfor. Dokumenter høyere i hierarkiet oppfattes å være mer overordnet og gir føringer for dokumenter lavere i hierarkiet.

Dokumentene er her beskrevet kort:

1. E-resept lovhjemmel og forskrift (se kapittel 3.3)
2. E-resept overordnet funksjonell spesifikasjon (OFS) – beskrivelse av løsningen på overordnet nå.
3. E-resept detaljert funksjonell spesifikasjon (DFS)
4. E-resept arkitektur – dette dokumentet
5. E-resept meldingsdefinisjoner.
6. Inkluderer logiske modeller, eksempelmeldinger, XML-skjema.
7. Systemspesifikke krav

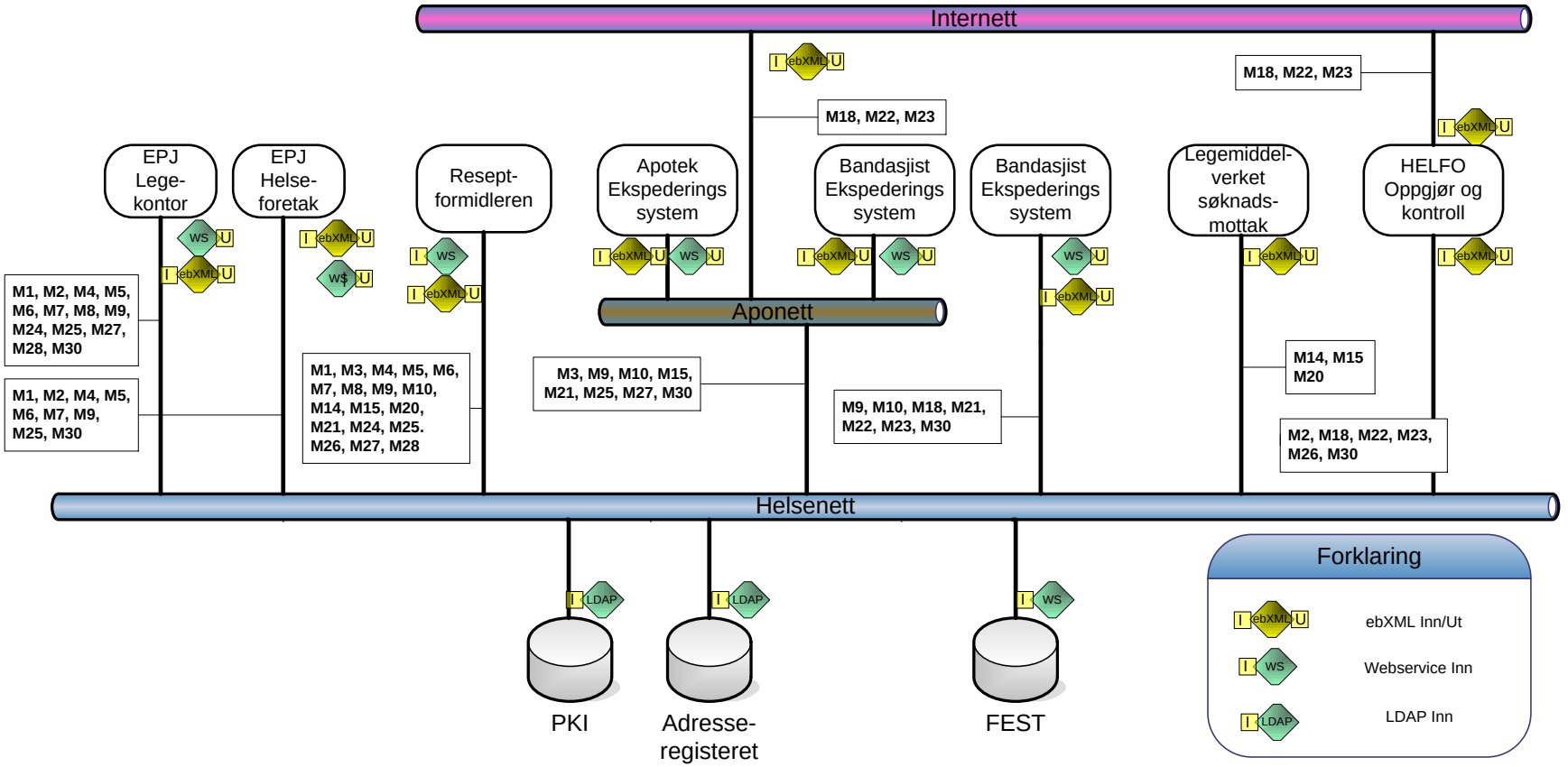
For tilgang tilde systemspesifikke kravene, ta kontakt med den relevante leverandør. Lovhjemmel og forskrift er publisert på www.lovdata.no, og de andre dokumentene er publisert på ehelse.no.

Vedlegg B: Referanser

E-resepts samlede dokumentasjon omfatter både etablerte standarder i sektoren og egne spesifikasjoner. De viktigste dokumentene fremgår av tabellen under.

Referanse	Navn	Lenke
DFS	E-resept detaljert funksjonell spesifikasjon	
E-resept begrepsliste		
E-resept meldingsdefinisjoner	Komplett dokumentasjon på alle meldinger i e-resept.	
Forskrivning av legemidler	Dokumentering av forskrivning og administrering av legemidler mv. Kravspesifikasjon og teknisk standard, KITH R08/03	Last ned
Informasjonssikkerhet	Norm for informasjonssikkerhet i helsesektoren	Last ned
HIS 80601:2006	Standard for hodemelding: Informasjonsmodell og XML meldingsbeskrivelse	Last ned
KITH 1304	KITH Rapport 13/2004. Anbefalinger og standarder for PKI i helsesektoren	Last ned
HIS 1037:2011	Rammeverk for elektronisk meldingsutveksling i helsevesenet.	Last ned
HIS 80415:2004	Applikasjonskvittering. Informasjonsmodell, XML meldingsbeskrivelse og retningslinjer for bruk. Versjon 1.0 rev2	Last ned
Kodeverk i e-resept		
OFS	E-resept overordnet funksjonell spesifikasjon	
PKI	Kravspesifikasjon for PKI i offentlig sektor	Last ned
Regeldokument oppgjør og kontroll		
Reseptformidler forskriften	FOR-2007-12-21-1610 Forskrift om behandling av helseopplysninger i nasjonal database for elektroniske resepter	Last ned
WS-SEC	WS-I Basic Security Profile 1.1 av 19-10-2006	Last ned

Vedlegg C: Nettverk meldinger og protokoller



Figur 8. Nettverk, meldinger og protokoller

Vedlegg D: Identifisering, autentisering og autorisering

Identifisering

Identifisering handler i denne sammenheng om å avgjøre hvilket individ eller organisasjon som står bak et dokument eller har utført en handling. For at en identifisering skal være endelig, må identifikatoren være unik, dvs. kun knyttet til én person eller virksomhet. For virksomheter benyttes organisasjonsnummer registrert i Enhetsregisteret som unike identifikator, For rekvirenter er HPR-nummeret og fødselsnummeret unike identifikatorer, og i samband med elektroniske resepter utfyller disse hverandre. HPR-nummer er likevel den primære identifikator. Den er en offentlig opplysning, og er den ID som er knyttet til rekvirentens virke. Fødselsnummeret brukes primært til autentisering (se under).

Autentisering

Autentisering kan beskrives som det å etablere et visst nivå av tillit til en påstått identitet. I en elektronisk resept skjer autentiseringen ved elektronisk signatur (se vedlegg E) og vi oppnår vi sterkest autentisering ved å etablere en komplett fødselsnummerkjede mellom sertifikatet resepten er signert med, HPR-registeret og HPR-nummer på resepten.

Autorisering

Autorisering av rekvirenter i e-resept (i Reseptformidler, hos HELFO, utleverer og Legemiddelverket) bruker HPR-registeret som autoritativ kilde. Nøkkelen i dette registeret er HPR-nummeret. Hvis HPR-nummeret er autentisert, så legges opplysningene i HPR-registeret til grunn for forholdet til individet som har dette HPR-nummeret: vedkommende *autoriseres* da i henhold til HPR-registerets opplysninger.

Vedlegg E: Bruk av PKI

Alle aktører i e-resept skal via Norsk Helsenett få tilgang til både adresseinformasjon og pekere til virksomhetssertifikater fra Adresseregisteret. Katalogtjenester for sertifikater, revokeringslister og fødselsnummeroppslag skal være tilgjengelige i Norsk Helsenett.

Sertifikater er sentralt i et PKI system. Sertifikater som inneholder privat nøkkel må håndteres konfidensielt. Det er essensielt i systemet at uvedkommende ikke får tilgang til private nøkler. Sertifikat som inneholder offentlig nøkkel må være tilgjengelig for alle som skal kryptere meldinger eller validere signaturer.

Standarden X.509 spesifiserer formatet på sertifikater som brukes for PKI.
Et sertifikat vil også inneholde informasjon om hva nøkkelen i sertifikatet kan brukes til. De tre nøkkeltypene som er mest relevante i denne sammenheng er:

- contentCommitment (tidligere: nonRepudiation)
  benyttes til signering (Elektronisk signering) av kjent innhold, og støtter «ikke-benektning» dvs. at man ikke senere kan nekte for å ha signert innholdet.
- dataEncipherment
  benyttes til kryptering av innhold for konfidensialitet
- digitalSignature
  også kalt “kryptografisk signatur”. Benyttes for autentiseringsformål. Kan benyttes til signering av ukjent innhold (=challenge) og må derfor ikke forveksles med contentCommitment.

De sentrale dokumentene som setter krav til bruk av PKI i offentlig sektor generelt og helsesektoren spesielt er:

- Esignaturloven
- Kravspesifikasjon for PKI i offentlig sektor
- Rammeverk for autentisering og uavviselighet
- Rammeverk for elektronisk meldingsuveksling i helsevesenet basert på ebXML

«Kravspesifikasjon for PKI» refererer til tre sertifikatnivåer: Virksomhet, Person-Standard og Person-Høyt, mens «Rammeverk for autentisering og uavviselighet» definerer sikkerhetsnivåer.

For personsertifikater er det entydig definert at «Person-høyt» tilfredsstiller sikkerhetsnivå 4. Når det gjelder virksomhetssertifikater er situasjonen litt mindre entydig, og det referes til tiltak og rutiner for å ivareta sikkerheten på et høyt nivå også med disse.

Ved signering av innholdet i elektronisk resept brukes rekvirentens «Person-Høyt» sertifikat. Signeringen skjer med rekvirentens private nøkkel for ikke-avvisning (Content commitment), og kan kontrolleres av alle som mottar dokumentet med rekvirentens offentlige nøkkel. Reseptformidleren vil sjekke signatur ved mottak og bekrefte denne signaturen med en tidsstemplet godkjenning.

Ved signering av forsendelser skal det i henhold til «Rammeverk for elektronisk meldingsuveksling i helsevesenet basert på ebXML» benyttes virksomhetssertifikater med ikke-avvisning (Content commitment). Disse er rene software-sertifikater som benyttes automatisk ved forsendelse og mottak av meldinger. Ved kryptering av forsendelser skal det benyttes virksomhetssertifikater med «dataEncipherment».

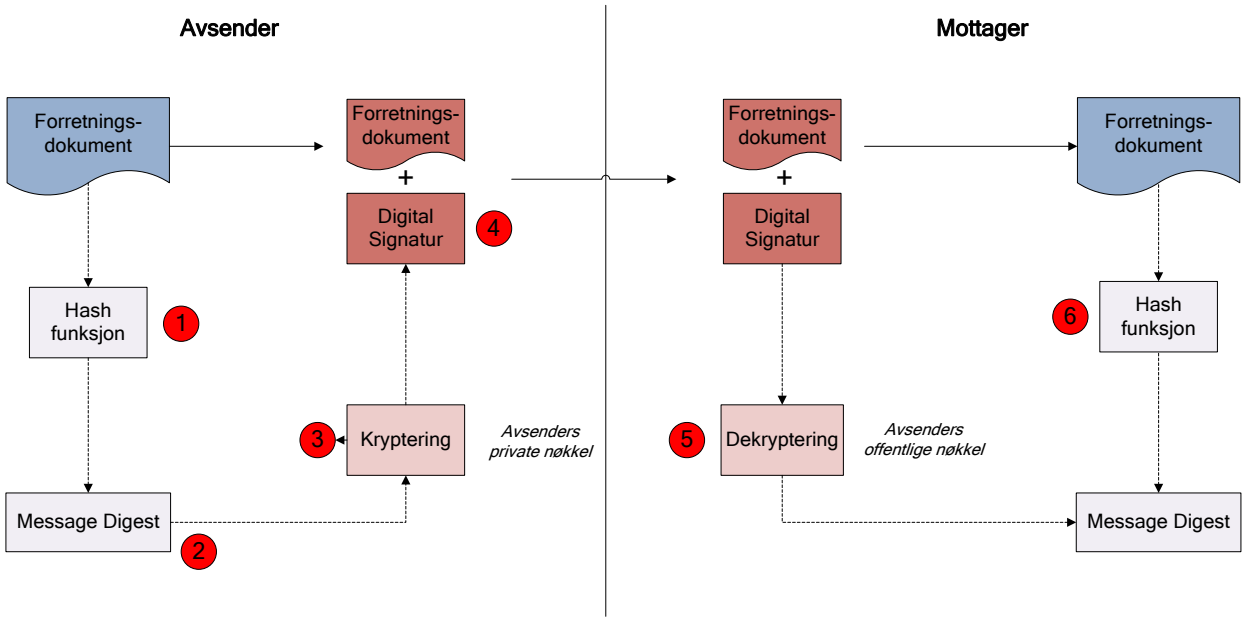
I e-Resept benyttes ebXML for asynkrone forsendelse, mens all synkron kommunikasjon med Reseptformidleren er webservice-basert, med fagmeldinger pakket direkte i SOAP konvolutt. For denne typen kommunikasjon er det akseptert å signere med «digitalSignature» sertifikat/nøkkel.

Signering gjøres med egen privat nøkkel, mens kryptering gjøres med mottakerens offentlige nøkkel.

Signering spesifiseres i e-Resept på to nivåer som er signering av forretningsdokument og signering av forsendelse.

Signering av forretningsdokument

Figuren under illustrerer hvordan et forretningsdokument (for eksempel en resept) signeres:



Figur 8 Signering av et forretningsdokument

Figuren over viser trinnene ved signering av et dokument og kontroll av signaturen.

1: En hash funksjon tar forretningsdokumentet og genererer en (2) message digest. Message digest er en verdi av bestemt lengde.

3: Message digest krypteres med avsenders private nøkkel, og dette danner den digitale signaturen (4). Den digitale signaturen sendes sammen med resepten og som en del av forretningsdokumentet.

Dekryptering av den digitale signaturen skjer ved at mottaker benytter avsenders offentlig nøkkel (5). Mottaker lager også en message digest av forretningsdokumentet (6) som sammenlignes med den dekrypterte signaturen. Det er dette som kontrollerer forretningsdokumentets integritet, da en endring i dokumentet vil gi en annen verdi for message digest.

En viktig forutsetning er at avsender og mottager benytter samme hash funksjon.

En signatur på et forretningsdokument er persistent, dvs. følger med gjennom hele dokumentets livsløp og sikrer at det til enhver tid kan etterprøves at dokumenetet ikke er endret.

Ved signering av forretningsdokument skal nøkkel for «contentCommitment» benyttes.

Signering av forsendelse

Ved signering av en forsendelse gjelder samme prinsipper som ved signering av et forretningsdokument, men det er avsenders virksomhetssertifikat som benyttes. Denne kontrolleres av mottager med avsenders offentlige nøkkel.

Sertifikatets offentlige nøkkel legges ved forsendelsen.

Virksomhetssertifikater kan lastes ned dynamisk, men vil ofte foreligge som en del av kommunikasjonsavtalen mellom aktørene (CPA).

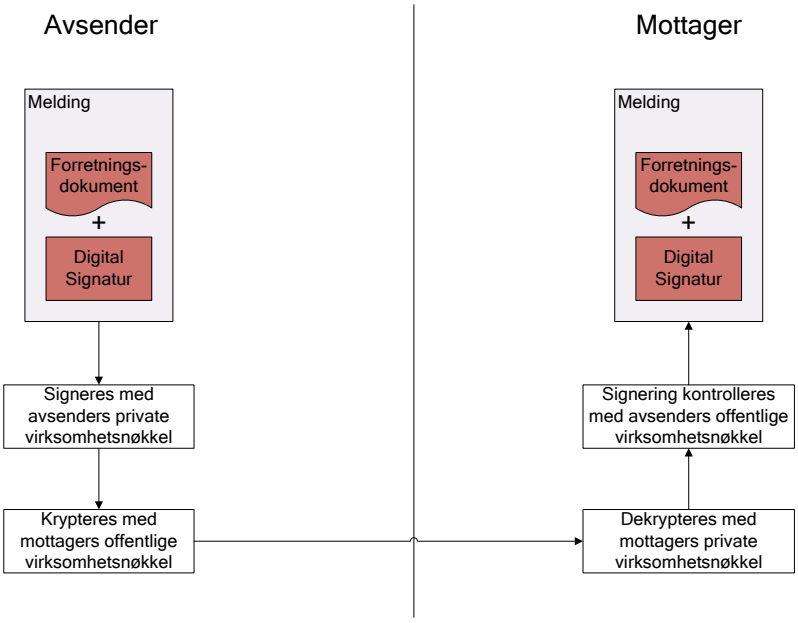
Asynkrone forsendelser som er basert på ebXML skal signeres med nøkkel for contentCommitment.

Synkrone webservice meldinger mot Reseptformidleren skal signeres med «digitalSignature». (Merk at det er støtte for kun ett sertifikat for signering av request og kryptering av response. Dersom det ikke benyttes kombinert sertifikat skal «dataEncryption» benyttes).

Kryptering av forsendelse

For å sikre konfidensialitet ved en forsendelse krypteres hele forsendelsen av avsender med den offentlige nøkkelen til mottagers virksomhetssertifikat. Mottagere dekrypterer med den private nøkkel tilhørende eget virksomhetssertifikat.

Kryptering og dekryptering av meldinger skal skje innenfor sikker sone



Figur 9 Signering med avsenders virksomhetssertifikats private nøkkel og kryptering med mottagers virksomhetssertifikats offentlige nøkkel.

Behandling ved mottak

Alle aktører som behandler elektroniske resepter må verifisere meldingens integritet. Dette kan gjøres ved å sammenlikne beregnet hash-verdi for mottatt melding med tilsvarende verdi i signaturkontrollobjektet (SKO, se kapittel 4.3.5.2).

Ved behov gjøres oppslag i CRL/OCSP-tjenestene til CA, samt at det skal legges til rette for at virksomhetssertifikater kan lastes ned dynamisk. Av ytelseshensyn kan Reseptformidleren basere seg på revokeringslister (CRL) som lastes ned en gang per døgn og mellomlagres lokalt.

Spesielle forhold i e-resept

E-resept er en ny anvendelse av PKI i helsesektoren der signerte dokumenter ikke bare oversendes direkte til den endelige mottakeren. I e-resept signeres resepter av rekvirent, lagres i Reseptformidleren, hentes ved behov av utleverer og senere legges ved oppgjørskravet til HELFO. I mangel av et tiltrodd signeringstidspunkt valideres signaturen vanligvis i mottaksøyeblikket, ved å benytte mottakstidspunkt som effektivt signeringstidspunkt. I e-resept mottas resepten mange steder så lenge etter faktisk signeringstidspunkt at sertifikatstatus ofte vil ha endret seg siden signeringen. Dette løses ved å ta i bruk avanserte signaturer, XAdES, i henhold til ETSI TS 101 903 v1.3.2 eller nyere. En XAdES signatur kan utvides over tid ved å legge til valideringsdata som signeres og valideres. Med valideringsdata menes tidsstempler fra tiltrodd tredjepart (TSA – time stamping authority), referanser til eller kopier av elementer i sertifikatkjeden og sertifikatstatus (her: OCSP svaret inklusiv fødselsnummer). Utformingen av konkrete e-resept signaturer og hvordan disse valideres ville da måtte dokumenteres i henhold til ETSI 102 038 v1.1.1 eller nyere.

For å kunne ta i bruk XAdES må det tilbys TSA tjenester. Disse må benytte referanseklokker og sertifikater med utvidet gyldighet, med tilsvarende lange nøkler og algoritmer med tilstrekkelig styrke, samtidig som TSAer i e-resept må være minst like tilgjengelig som Reseptformidleren. Tidsstempler må produseres i henhold til RFC3161.

Da disse forutsetningene er vurdert ikke å være på plass, har e-resept valgt å løse utfordringen med det nye tidsaspektet på en pragmatisk måte som drar nytte av tankene i ETSI TS 101 903 v1.3.2 og anvender aktuelt tilgjengelig PKI.

SignaturKontrollObjekt(SKO)
SKO inneholder reseptens mottakstidspunkt i Reseptformidleren. Dette tidspunktet er definert som effektiv signeringstidspunkt og benyttes her og senere i verdikjeden ved validering av signaturen.
Videre referer SKO til rekvirentens sertifikat og inneholder et entydig sammendrag av reseptens signaturverdi. SKO opprettes og signeres av Reseptformidleren i mottakstidspunktet.
Kombinerte sertifikater
Enkelte utstedere av PKI sertifikater kombinerer flere «keyUsage» typer i ett sertifikat. Den samme nøkkelen er dermed tillatt brukt for flere formål. Typisk gjelder dette kryptering og digitalSignatur (=autentisering). Nøkkel for ikke-avvisning (Content commitment) vil finnes i eget sertifikat kun til dette formål. Det er viktig at implementasjonene støtter valg av sertifikat av rett type under konfigurering.

Noen systemer i e-resept baserer seg på at det eksisterer kombinert sertifikat som kan benyttes både for kryptering, autentisering og signering. I noen systemer som kun signerer synkrone meldinger er det støtte kun for ett sertifikat, basert på at dette støtter begge funksjoner. I sentrale registre (AR) er det støtte for to sertifikat: Kryptering og Signering. For PKI leverandører som leverer separate sertifikat for hver nøkkeltype er det ikke full støtte for all bruk.

Nye versjoner bør støtte automatisk seleksjon av nøkkeltyper, og også ha støtte for både kombinerte og separate sertifikater.

Vedlegg F: Web-tjenere

Reseptformidleren

Adresser til testmiljø på internett, testmiljø på Norsk helsenett og QA-miljø på Norsk helsenett finnes i Reseptformidlerens grensesnittdokument publisert av EVRY.

Webservice for M30 (FEST)

Legemiddelverkets webservice for M30 skiller seg fra Reseptformidlerens. M30 krever ikke kryptering. For versjon 2 av FEST benyttes en standard webservice uten sikkerhet.

Adresser til testmiljø og produksjonsmiljø finnes i «Teknisk grensesnittdokumentasjon» på www.legemiddelverket.no/Bruk_og_raad/FEST/hvordan-bruke

Vedlegg G; Dokumentasjon av SKO

Denne dokumentasjonen er ikke knyttet til en enkelt melding, men berører funksjonalitet på tvers av meldinger gjennom verdikjeden. Den hører derfor ikke til meldingsdokumentasjonen og er for detaljert for å tas inn i DFS. Det er derfor besluttet at denne dokumentasjonen fremkommer som et vedlegg til arkitekturdokumentet.

Faglig bakgrunn

I e-resept er det besluttet at Reseptformidleren skal gjennomføre en stringent kontroll av rekvirentens autorisasjon i HPR i forhold til sertifikatinformasjonen. Beslutning om dette ble først tatt av styringsrådet i juni 2007 og deretter er dette bekreftet av forskriften. De resepter som ikke oppfyller disse kravene forkastes av Reseptformidleren. Et slikt regime gjør situasjonen oversiktlig og enkel for utleverer; alle resepter i Reseptformidleren er kontrollert og akseptert (innenfor disse gitte rammer) men detaljer rundt rekvisisjonsrett (Kobling vare – rekvisisjonsrett fra HPR) sjekkes av utleverer. Det betyr at resepter blir avvist av Reseptformidleren hvis ikke rekvirentens fødselsnummer ligger korrekt i HPR og at vedkommende har autorisasjon.
Utleverer har fortsatt ansvaret for at utlevering skjer på en forsvarlig måte.
Disse kontrollene er dokumentert i DFS.

I e-resepts verdikjede formidles den elektroniske resepten gjennom mange ledd, først som M1, deretter som vedlegg i M9.4 og til slutt som vedlegg i M18. For alle ekspederte resepter vil både rekvirent, Reseptformidleren (RF) og en utleverer være involvert. For alle ekspederte blå resepter vil også HELFO være involvert grunnet refusjon

Det er viktig at alle aktørene oppfatter resepten på samme måte og at det ikke er tolkningsrom mellom aktørene. Det er sentralt at alle partene har en felles oppfatning av reseptens gyldighet og varighet.

Beskrivelse av signaturkontrollobjektet

Formål

Formålet med signaturkontrollobjektet (SKO) er å etablere en tillitskjede mellom partene i e-resept, for å sikre en felles basis for vurdering av en resepts gyldighet.

SKO vil konkret dokumentere de kontrollene som Reseptformidleren har utført, og resultatene av disse, for å kunne formidle dette til andre aktører, på en persistent måte over tid. Grunnen til å dokumentere resultatet av kontrollene er for å kunne videreformidle at resepten var gyldig på mottakstidspunktet hos Reseptformidleren, ut fra validering av sertifikater og oppslag og validering mot HPR, siden resultatet av kontrollene kan endres over tid, avhengig av endringer i de relevante tilhørende registre.

SKO vil dessuten omfatte en tidsstempling av resepten. Reseptformidlerens tidsstempling innebærer en økt beskyttelse av den opprinnelige signeringen av resepten, og sikrer at denne oppfattes som gyldig i en lenger periode. Tidspunktet for kontrollen er i seg selv viktig, da andre parter kan benytte mottakstidspunktet (tidsstemplingen) som en verifikasjon av tidsangivelse og gyldighet av resepten og SKO.

Plassering av SKO

SKO plasseres som et eget XML-objekt i signaturobjektet på den opprinnelige M1. Dette kan gjøres uten å bryte rekvirentens signatur. Ved å gjøre det på denne måten vil SKO kunne sendes med når resepten formidles videre mellom partene.

Bruk av standardisert format (ETSI XAdES)

Det har vært et viktig mål for arbeidet med SKO å finne en form på det som gjør gjenbruksverdien av SKO størst mulig for partene. Bruk av aktuelle standarder for slike objekter har derfor vært vurdert. Slike standarder er ikke i bred bruk innenfor helsesektoren i Norge i dag. E-resept vil derfor gjøre nybrottsarbeidet med bruken av slike standarder. Den standard som legges til grunn er ETSI XAdES. Det antas at vi ved å legge ETSI XAdES v1.3.2[6] til grunn, kan oppnå viktige fordeler som:

[6] http://uri.etsi.org/01903/v1.3.2/ og altså ETSI TS 101 903 V1.3.2 (2006-03)

1. Bruken av avanserte XML-signaturer er transparent og krever ikke at et nytt XML-dokument spesifiseres.
2. Bruken av **XAdES** vil minske arbeidet med å implementere og bruke SKO.
3. XAdES er en bæredyktig standard som forventes å bringe elektronisk samhandling og dokumenthåndtering i helse- og sosialsektoren videre.

Avanserte XML signaturer kvalifiserer en signatur i henhold til XMLDsig. Ved å utvide signaturen med tidsstempler (XAdES-T), sertifikater og sertifikatstatusinformasjon (XAdES-X-L eller -A) gjøres validering av signaturen etter lang tid mulig.

XAdES signaturer kan også utvides over tid.

Detaljer i bruken av XAdES i SKO er vist i eksemplene til slutt i dette vedlegget.

Policy

Roller

I e-resept er Reseptformidleren akseptert som tiltrodd tidsstemplingsautoritet TSA. Dette forutsetter at Reseptformidleren disponerer en klokke som oppfyller kravene til Kravspesifikasjon for PKI i offentlig sektor[7], hvilket anses som oppfylt.

Sertifikater

Kravene til sertifikater i e-resept er som følger:

1. CA sertifikater
   minst 2048 bit RSA
2. Personlige kvalifiserte sertifikater
   minst 1024 bit RSA
3. OCSP signeringssertifikater
   minst 1024 bit RSA
4. TSA sertifikater
   minst 2048 bit RSA

[7] V1.02 http://www.regjeringen.no/upload/kilde/mod/rap/2004/0002/ddd/pdfv/234033-kravspek_pki_v102.pdf

Nøkkelbrukutvidelser

E-resept krever nøkkelbrukutvidelser som følger:

1. OCSP signeringssertifikater
   extendedKeyUsage id-pkix-ocsp-nocheck
2. TSA sertifikater
   extendedKeyUsage id-kp-timeStamping

Algoritmer / styrke

E-resept krever algoritmer med styrke som følger:

1. Signering
   RSA + minst SHA-256
2. OCSP signering
   RSA + minst SHA-256
3. Tidsstempling
   RSA + minst SHA-256

Konkrete verdier og parametre som skal brukes

Tidsstempelet som legges ved i rekvirentens signatur inneholder et element (<dss:TSA>) som identifiserer utstederen av tidsstempelet, i dette tilfellet er Reseptformidleren. Identiteten til TSA'en bør representeres som DN (Distinguished Name) fra sertifikatet som benyttes til tidsstempling. Denne verdien vil bli beskrevet i Reseptformidlerens grensesnittsdokument.

Regler ved bortfall av katalogtjenester for PKI

RF skal validere virksomhetssertifikater sertifikater opp mot revokeringslister. Revokeringslister lastes ned fra sertifikattilbyder. Følgende prinsipper gjelder for dette:

- RF kan akseptere meldinger opp til 12 timer etter at gyldigheten for siste CRL utløp
- Det etableres en mulighet for å revokere/sperre sertifikater eller på annen måte hindre tilgang lokalt i Reseptformidleren. Dette kan benyttes hvis oppdatering av CRL ikke er tilgjengelig til å sperre utleverere på bakgrunn av manuelt innhentet informasjon.
- Varslingsrutiner mellom Reseptformidleren og sertifikattilbyder etableres for å få overført revokeringsdata ved feilsituasjoner
- Ved utilgjengelig OCSP-oppslag kan Reseptformidleren benytte cashet verdi som beskrevet i kap 4.3.2.2.

Innhold i SKO

SKO omfatter informasjon om

- gyldigheten av rekvirentens personlige sertifikat og tilhørende fødselsnummer som Reseptformidleren innhenter fra CA i form av et OCSP-oppslag.
- resultatet av Reseptformidlerens HPR-kontroll sammen med kopi av OCSP-oppslaget for Reseptformidlerens virksomhetssertifikat
- et tidsstempel på resepten, sammen med kopi av OCSP-oppslaget for Reseptformidlerens tidsstemplingssertifikat

I det videre vil hvert av disse elementene bli beskrevet.

Gyldighet til rekvirentens personlige sertifikat

Dokumentasjon av gyldigheten til rekvirentens personlige sertifikat dokumenteres med å bruke resultatet av oppslaget Reseptformidleren gjør mot VA. Ved å benytte signert dataobjekt i henhold til XAdES-standarden (ETSI TS 101 933) er det et behov for å inkludere revokeringsstatus-informasjon på et standard format slik at det er mulig for andre aktører å verifisere disse i etterkant.

Informasjonen i SKO om gyldigheten til rekvirentens personlige sertifikat vil derfor baseres på en standard OCSP-respons fra CA/VA.

SKO vil inneholde rekvirentens fødselsnummer, da dette er innehold i standard OCSP-respons. Det vurderes at denne informasjonen kan tilgjengeliggjøres på denne måten for utleverere og HELFO, da disse har behov for tilgang til denne informasjonen for å kunne utøve sin funksjon.

HPR-oppslag

HPR-oppslaget er ikke en del av PKI-strukturen, men anses å være en sentral del av tillitskjeden knyttet til e-resept. Det er derfor valgt å inkludere resultat av Reseptformidlerens oppslag i HPR inn i SKO.

Tidsstempling

En vanlig resept er gyldig for ekspedering i inntil et år og visse resepter er gyldige i inntil tre år. I perioden mellom reseptens utstedelse og reseptens bruk kan rekvirentens personlige sertifikat utløpe. Dette er et eksempel på at sertifikatstatus for et sertifikat (I dette tilfelle rekvirentens) kan endres over tid fra initiell kontroll og frem til siste kontroll av resepten. Reseptformidleren vil derfor tilføre en langtidsbeskyttelse av SKO som hviler på en annen signatur enn signaturen på OCSP-responsen.

Ved at Reseptformidleren gjennomfører en egen tidsstempling av resepten i SKO, basert på eget tidsstemplingssertifikat, oppnås to viktige forhold:

1. tidspunktet for beregning av starten av reseptens gyldighet (Utstedelsestidspunktet) fastslås autoritativt
2. reseptens sertifikatmessige gyldighet økes til gyldigheten for Reseptformidlerens tidsstemplingssertifikat.

I påvente av at NHN eller andre etablerer TSA tjenester, er Reseptformidleren akseptert som TSA i e-resept.
Reseptformidleren vil dermed opptre som tiltrodd tidsstemplingsautoritet (TSA), og vil i den forbindelse benytte dedikert sertifikat med extendedKeyUsage utvidelsen id-kp-timeStamping, jf. RFC3161.

Tidsstempling implementeres i Reseptformidleren ved å bruke XAdES-T for tidsangivelsen.

Buypass kan levere sertifikat til Reseptformidleren for tidsstempling under følgende forutsetninger:

1. Sertifikatet utstedes under CP for Buypass virksomhetssertifikater
2. E-resept/HELFO må produsere en CSR (Certificate Signing Request) som Buypass benytter for å generere det aktuelle sertifikatet
3. Nøkkelen skal være 2048 bits
4. Levetiden på sertifikatet settes lik 3 år

Dette vurderes å være tilstrekkelig, og e-resept vil basere seg på dette.

Reseptformidleren vil synkronisere sin klokkefunksjon mot en klokkefunksjon hos Universitetet i Oslo: (fartein.ifi.uio.no), kontrollert mot 4 andre autoritative klokkefunksjoner.

Spesielle forhold knyttet til varighet av tidsstempling i 3 år
Som nevnt tidligere vil det finnes resepter som skal være gyldige i opp til 3 år etter utstedelse. Etter tre år kan både rekvirentens personlige sertifikat, Reseptformidlerens virksomhetssertifikat og Reseptformidlerens tidsstemplingssertifikat være utgått. Med bruken av XAdES vil det være gyldigheten av Reseptformidlerens tidsstemplingssertifikat som blir styrende. Det er derfor viktig at dette sertifikatet til enhver tid ikke har for kort gjenværende gyldighet. For å hindre at dette blir et problem vil Reseptformidlerens tidsstemplingssertifikat fornyes hvert år. Det er dermed bare de resepter som har tre års gyldighet i utgangspunktet, hvorav mange er hvite resepter, og som ikke er slettet/utekspedert etter to år, som vil bli berørt av dette problemet. Det forventes at dette vil løse problemet for en dominerende andel av reseptene. For alle resepter som har gyldighet innenfor utløpstiden til Reseptformidlerens tidsstemplingssertifikat vil SKO inneholde all

informasjon senere parter trenger for validering av resepten, uten å måtte gjøre oppslag mot eksterne parter.
Dersom det viser seg at årlig fornyelse av Reseptformidlerens tidsstemplingssertifikat skaper problemer, kan det vurderes to tilnærminger:

1. Øke frekvens for oppdatering av Reseptformidlerens tidsstemplingssertifikat til halvårlig kvartalsvis, eller månedlig
2. Reseptformidleren kan utvide sin tidsstempling av de aktuelle reseptene med XAdES-A-signatur

Erfaringer med bruken av XAdES vil vurderes etter hvert og tilnærming velges i tråd med dette.

Det vil også være slik at HELFO vil kunne motta resepter i lang tid etter at resepten er ekspedert (og utgått). En utleverer må fremme sitt krav overfor HELFO innen 6 måneder etter ekspedering, men kan etter initiell avvisning fortsette å fremme kravet i ubestemt tid. Reseptene vil på et slikt tidspunkt være utenfor Reseptformidlerens kontroll og det SKO som er laget av Reseptformidleren vil kunne være utgått. I slike situasjoner vil utleverer kunne utvide reseptens tidsstempling ved å tilføre XAdES-A inn i SKO, før den opprinnelige tidsstemplingen utløper. Dette er ikke forutsatt som et krav nå, men kan bli en aktuell utvidelse senere, dersom dette viser seg å bli et praktisk problem.

Funksjonalitet

SKO opprettes i Reseptformidleren for alle[8] M1 som lagres i Reseptformidleren. SKO lagres som en del av det opprinnelige signaturobjektet på resepten. På denne måten følger SKO med resepten i den videre behandling. Rekvirentens opprinnelige signering eller integriteten i meldingen ødelegges ikke ved dette.
Når Reseptformidleren mottar en resept vil den validere resepten. Når resepten er validert i henhold vedtatte kontroller blir godkjent resept lagret og resultatet av valideringen blir lagret i SKO. SKO blir lagret i signaturobjektet til den opprinnelige resepten.

> Reseptformidleren vil foreta et nytt OCSP-oppslag av rekvirentens personlige sertifikat for hver resept som behandles. Det er derfor kritisk at dette oppslaget kan utføres raskt. Buypass har forpliktet å levere dette på 2-300 ms.
>
> Reseptformidleren vil benytte OCSP for eget virksomhetssertifikat for signering av HPR-data. Reseptformidleren vil gjøre dette oppslaget en gang per dag, og cache og gjenbruke resultatet for hver SKO. Siden Reseptformidleren vil kjenne til eventuell revokering av eget sertifikat vurderes dette å være en forsvarlig policy.

[8] SKO er mest aktuell for blå resepter, men det vurderes dit hen at det er like enkelt å lage SKO for alle resepter som behandles av Reseptformidleren.

Reseptformidleren vil benytte OCSP for eget tidsstemplingssertifikat for signering av tidsstemplingen. Reseptformidleren vil gjøre dette oppslaget en gang per dag, og cache og gjenbruke resultatet for hver SKO. Siden Reseptformidleren vil kjenne til eventuell revokering av eget sertifikat vurderes dette å være en forsvarlig policy. Reseptformidleren vil logge tidsstemplingen sammen med en unik ID for tidsstemplingen.

SKO blir videresendt med M1 (resepten) til utleverer i M9.4, men ikke til rekvirenter i M9.6, M6, M8, eller M15 eller til SLV i M14).

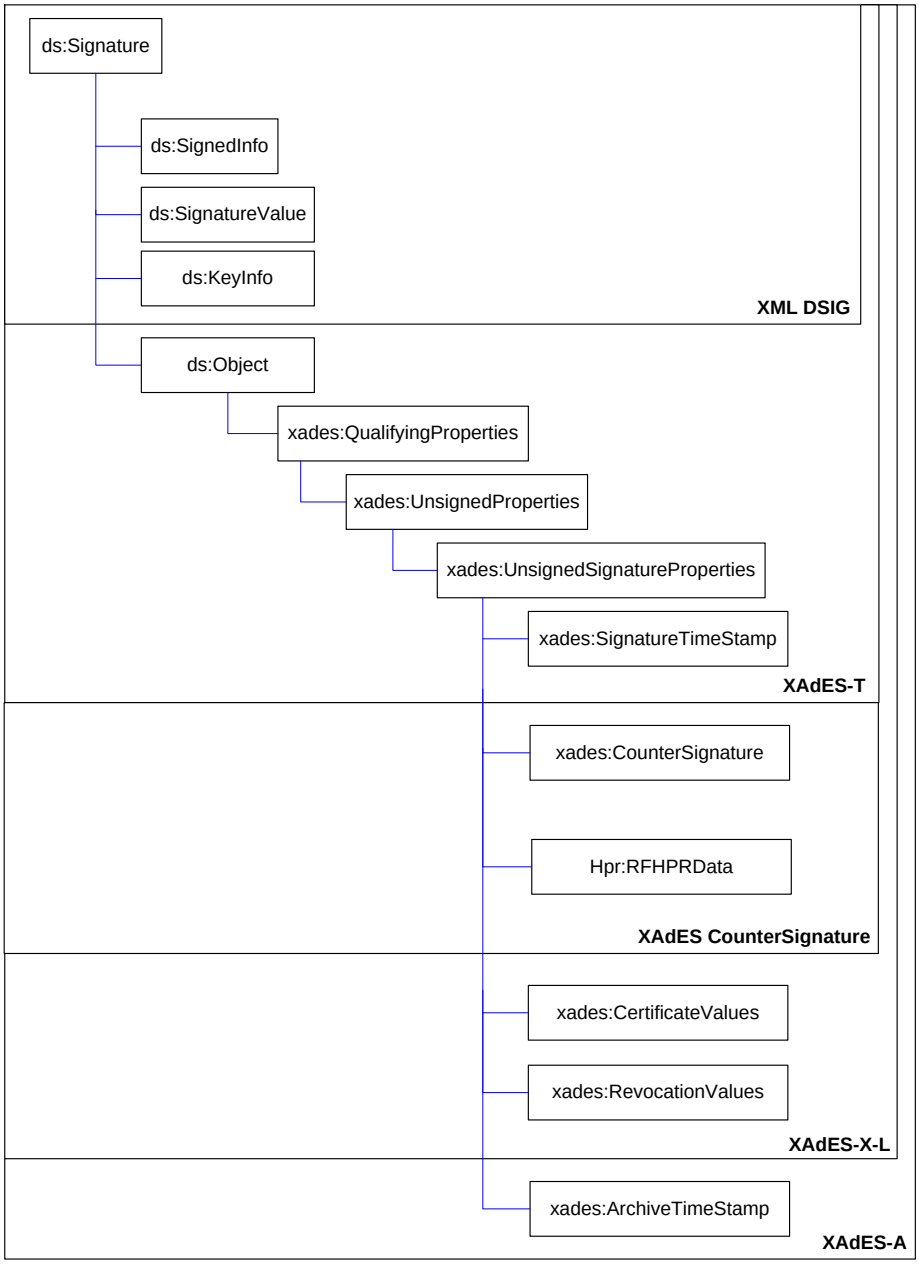
Når utleverer laster ned en resept med M9.4 vil SKO mottas som en del av M1. Utleverer kan legge til grunn dokumentasjonen av utførte kontroller samt andre kontrollverdier i SKO ved utførelse av sin ekspedering.

Merk: Ved innføring av SKO forsterkes kravene til håndtering av sertifikater hos utleverer ved at utleverersystem må kunne motta M9.4 fra Reseptformidleren inneholdende to ulike sertifikater. Eksempelvis kan SKO være signert med et gammelt virksomhetssertifikat, mens M9.4 er signert med ett nytt virksomhetssertifikat.

SKO fra Reseptformidleren blir deretter (for blå resepter) videresendt sammen med resepten i Oppgjørsmeldingen M18 fra utleverer til HELFO. Når HELFO mottar en M18 vil M18 valideres og de vedlagte M1 vil valideres. Ved at SKO fra Reseptformidleren medfølger vil kontrollen hos HELFO muliggjøres.

Eksempler

Strukturen for de ulike signaturelementer i SKO fremgår av figuren under:



Figur 1: Struktur for SKO

XMLDsig angir hvordan rekvirentens signatur generelt utvides

XAdES – T vises hvordan tidsstemplingen legges til.

XAdES – CounterSignature vises hvordan HPR-data legges til

XAdES-X-L vises hvordan signeringsinformasjon legges til

XAdES – A vises hvordan ytterligere arkivering av tidsstempling kan foretas

XMLDSig

I henhold til DSIG utformes rekvirentens signatur som enveloped signature, der signaturen blir en del av XML dokumentet som signeres, som vist i eksempelet under:

```
<?xml version="1.0" encoding="UTF-8"?>
<MsgHead xmlns="http://www.kith.no/xmlstds/msghead/2006-05-24" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:schemaLocation="http://www.kith.no/xmlstds/msghead/2006-05-24 MsgHead-
v1_2.xsd">
        <MsgInfo>
                <Type DN="Resept" V="ERM1"/>
        </MsgInfo>
        <Document>
                <RefDoc>
                        <IssueDate V="2008-08-12T14:52:26"/>
                        <MsgType DN="XML-instans" V="XML"/>
                        <Content>
                                <Resept xmlns="http://www.kith.no/xmlstds/eresept/m1/2007-11-
23" xmlns:fk1="http://www.kith.no/xmlstds/felleskomponent1" xmlns:kith="http://www.kith.no/
xmlstds" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.kith.no/xmlstds/eresept/m1/2007-11-23 ER-M1-2007-11-23.xsd">
                                        <Forskrivningsdato>2008-08-12</Forskrivningsdato>
                                        <ds:Signature>
</MsgHead>
```

XML

Eksempel 1 XMLDsig

<ds:Signature> elementet i eksempelet over inneholder en referanse til det omsluttende XML dokumentet, dvs. resepten.

Eksempelet under viser hvordan et slikt <ds:Signature> element typisk kan se ut slik det foreligger i M1 etter rekvirentens signering:

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo >
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>GJunG+L8z9omau5FpDL0gHmjDiU=</ds:DigestValue>
```

Eksempel 2 XMLDsig med Signature

Rekvirentens signatur vil av Reseptformidleren utvides med ny informasjon i elementene <ds:Signature> , <ds:SignatureValue> og <ds:KeyInfo> , som vist i eksempelet under, slik at det entydig kan refereres til i XAdES. Attributtene kan tilføyes etter at signaturen er produsert av rekvirenten uten å bryte signaturen.

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>ByGrS9cJoRra12hjSia5yFwzBMc=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="SignatureValue">YVauwq0…aCk+Dws8=</ds:SignatureValue>
    <ds:KeyInfo Id="KeyInfo">
        <ds:X509Data>
            <ds:X509Certificate>MIID3…dAW2+</ds:X509Certificate>
        </ds:X509Data>
```

Eksempel 1 XMLDsig med utvidet signaturinformasjon

XAdES-T

XMLDSIG definerer `<ds:Object>` elementet for å supplere informasjon i en signatur.

XAdES definerer XAdES-T formatet for å tidsstemple en signatur. Tidsstemplet gjelder som effektivt signeringstidspunkt ved all validering av signaturen.

To standarder definerer tidsstempler: RFC3161[9] i ASN.1 og OASIS DSS[10] i XML syntaks. Uansett gjelder kravene fra RFC3161 når det gjelder hva et tidsstempel inneholder og hvordan slike produseres. OASIS DSS tidsstempler er enkle å produsere med standardbiblioteker, siden de egentlig bare er XMLDSIG enveloping signaturer. Derfor vurderes OASIS DSS som enklest å implementere i e-resept, og legges til grunn.

[9] RFC3161 www.ietf.org/rfc/rfc3161.txt Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

[10] OASIS DSS www.oasis-open.org/committees/dss/ OASIS Digital Signature Services

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="">....</ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="SignatureValue">YVauwq0…aCk+Dws8=</ds:SignatureValue>
    <ds:KeyInfo Id="KeyInfo">....</ds:KeyInfo>
    <ds:Object>
        <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#Signature">
            <xades:UnsignedProperties>
                <xades:UnsignedSignatureProperties>
                    <xades:SignatureTimeStamp Id="SignatureTimeStamp">
                        <xades:XMLTimeStamp>
                         <!-- Se neste eksempel for innhold i OASIS DSS XML timestamp-->
                        </xades:XMLTimeStamp>
                    </xades:SignatureTimeStamp>
                </xades:UnsignedSignatureProperties>
            </xades:UnsignedProperties>
        </xades:QualifyingProperties>
    </ds:Object>
</ds:Signature>
```

Eksempel 4 XAdES-T – plassering av SignatureTimeStamp

```
....
<dss:Timestamp xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
          <ds:Signature Id="XMLTimeStampTokenSignature" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <ds:SignedInfo>
                              <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                              <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                              <ds:Reference URI="#SignatureValue">....</ds:Reference>
                              <ds:Reference URI="#XMLTimeStampTokenKeyInfo">....</ds:Reference>
                              <ds:Reference URI="#TstInfo" Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken">
                                   ....
                              </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue Id="XMLTimeStampTokenSignatureValue">JNRFS1aj...KLjY=</ds:SignatureValue>
                    <ds:KeyInfo Id="XMLTimeStampTokenKeyInfo">
                              <ds:X509Data><ds:X509Certificate>
                                       <!-- base64-kodet TSA sertifikat -->
                              </ds:X509Data></ds:X509Certificate>
                    </ds:KeyInfo>
                    <ds:Object Id="TstInfo">
                              <dss:TstInfo>
                                        <dss:SerialNumber>1227859557799</dss:SerialNumber>
                                        <dss:CreationTime>2008-11-28T09:05:57+01:00</dss:CreationTime>
                                        <dss:TSA NameQualifier="CN"
                                        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
                                        CN=NAV Test
                                        </dss:TSA>
                              </dss:TstInfo>
                    </ds:Object>
          </ds:Signature>
</dss:Timestamp>
....
```

Eksempel 5 XAdES-T – innhold i XMLTimeStamp

XAdES CounterSignature

Elementet <xades:CounterSignature> refererer til rekvirentens signatur samt HPR-data. Elementet er en signatur av Reseptformidleren og inneholder således Reseptformidlerens sertifikat.

```
<ds:Object>
    <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#Signature">
        <xades:UnsignedProperties>
            <xades:UnsignedSignatureProperties>
                <xades:CounterSignature>
                <ds:Signature>
                    <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <ds:Reference Type="http://uri.etsi.org/01903#CountersignedSignature" URI="#SignatureValue">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                            <ds:DigestValue>rBmeyy0stU4vxxGkabzy1XO/PXc=</ds:DigestValue>
                        </ds:Reference>
                        <ds:Reference Type="http://uri.etsi.org/01903#CountersignedSignature"
URI="#KeyInfoCounterSignature">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                            <ds:DigestValue>somethirddigestvalue=</ds:DigestValue>
                        </ds:Reference>
                        <ds:Reference Type="http://uri.etsi.org/01903#CountersignedSignature" URI="#HPR">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                            <ds:DigestValue>someotherdigestvalue=</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>
                    <ds:SignatureValue>Szxwaa...=</ds:SignatureValue>
                    <ds:KeyInfo Id="KeyInfoCounterSignature">
                        <ds:X509Certificate>MIIE3z...+dwQa</ds:X509Certificate>
                    </ds:KeyInfo>
                </ds:Signature>
            </xades:CounterSignature>
            <hpr:RfHprData Id="HPR" xmlns:hpr="http://www.reseptformidleren.no/schema/rf-hpr-data">
                <hpr:HPR-nummer>string</hpr:HPR-nummer>
                <hpr:HPRMerknad V="token" S="0" DN="string" OT="string"/>
                <hpr:Autorisasjonskode>string</hpr:Autorisasjonskode>
                <hpr:Rekvireringskode>string</hpr:Rekvireringskode>
            </hpr:RfHprData>
        </xades:UnsignedSignatureProperties>
    </xades:UnsignedProperties>
</xades:QualifyingProperties>
</ds:Object>
```

Eksempel 6 XAdES-CounterSignature

Eksempel på skjema for HPR data er vist under:

```
<?xml version="1.0"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:rfhpr="http://www.reseptformidleren.no/schema/rf-hpr-data"
targetNamespace="http://www.reseptformidleren.no/schema/rf-hpr-data"
xmlns:EISI="http://www.EISI.no/xmlstds">
    <xsd:import namespace="http://www.EISI.no/xmlstds"
schemaLocation="http://www.EISI.no/xmlstds/EISI.xsd"/>
    <xsd:complexType name="RfHprDataType">
        <xsd:sequence>
            <xsd:element name="HPR-nummer" type="EISI:ST"
minOccurs="1"/>
            <xsd:element name="HPRMerknad" type="EISI:CV"
minOccurs="1"/>
            <xsd:element name="Autorisasjonskode" type="EISI:ST"
minOccurs="0"/>
            <xsd:element name="Rekvireringskode" type="EISI:ST"
minOccurs="0"/>
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="required"/>
    </xsd:complexType>
```

Eksempel 7; HPR-data

Det kan tenkes at dette vil forbedres noe i implementasjonen.

XAdES-X-L

Her utvides elementet <UnsignedSignatureProperties> med alle sertifikater og all statusinformasjon.

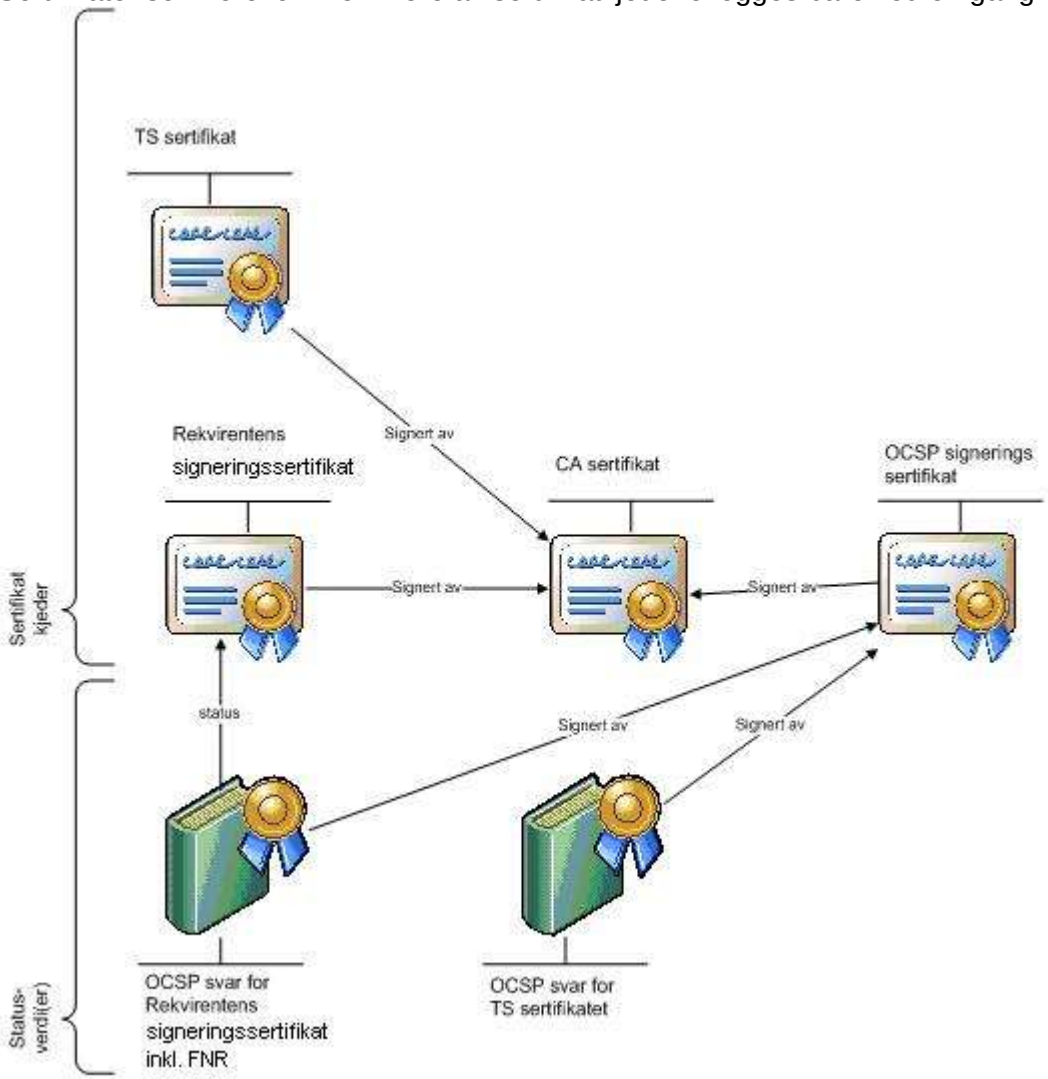
Under <xades:CertificateValues> legges det ved

- hele sertifikatkjeden for rekvirenten, dvs. rekvirentens sertifikat og CA sertifikatet for dette.

Hvis nødvendig legges det også ved

- hele sertifikatkjeden for statusinformasjon (OCSP eller CRL),
  dersom det benyttes delegerte OCSP signeringssertifikater uten utvidelsen id-pkix-ocsp-nocheck.

Sertifikater som forekommer i flere av sertifikatkjedene legges bare ved én gang.



Figur 2 Illustrasjon av sertifikatkjeden

Under <xades:RevocationValues> legges det ved

- OCSP svaret for rekvirentens signeringssertifikat, inkludert fødselsnummer
- OCSP svaret for TSA tidsstemplingssertifikat

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature">
...
<!-- Rekvirentens signatur -->
...
    <ds:Object>
        <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#Signature">
            <xades:UnsignedProperties>
                <xades:UnsignedSignatureProperties>
                    <xades:SignatureTimeStamp Id="SignatureTimeStamp">
                        <xades:XMLTimeStamp>
                            <dss:Timestamp xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
                                <!-- … -->
                            </dss:Timestamp>
                        </xades:XMLTimeStamp>
                    </xades:SignatureTimeStamp>
                    <xades:CertificateValues Id="CertificateValues">
                            <xades:EncapsulatedX509Certificate>mkpUl…Pg=</xades:EncapsulatedX509Certificate>
                            <xades:EncapsulatedX509Certificate>MIIFs…8Fw=</xades:EncapsulatedX509Certificate>
                            <xades:EncapsulatedX509Certificate>MIIE9…scDe</xades:EncapsulatedX509Certificate>
                     </xades:CertificateValues>
                     <xades:RevocationValues Id="RevocationValues">
                            <xades:OCSPValues>
                                <xades:EncapsulatedOCSPValue>MIIIZA…SlSU+A==</xades:EncapsulatedOCSPValue>
                                <xades:EncapsulatedOCSPValue>MIIInIt…GDwXA==</xades:EncapsulatedOCSPValue>
                            </xades:OCSPValues>
                    </xades:RevocationValues>
                </xades:UnsignedSignatureProperties>
            </xades:UnsignedProperties>
        </xades:QualifyingProperties>
    </ds:Object>
</ds:Signature>
```

Eksempel 8 XAdES Revocation values

XAdES-A

Formålet med XAdES-A er å kunne holde X-L formen gyldig utover gyldighetsperioden til sertifikatene og valideringsdata i den. Bruken av XAdES-A er ikke forutsatt ved initiell implementering av SKO mellom partene i e-resept, men kan være aktuelt som en utvidelse senere. Ref. også drøfting i kapittel 2.5.3.

- Arkivtidstempelet signerer all XAdES-data og binder disse dermed uforanderlig til den opprinnelige signaturen.
- En XAdES-A signatur rommer vilkårlig mange arkivtidsstempel. Et nytt tidsstempel forlenger dermed gyldigheten til hele signaturen.

Arkivtidstempelet produserer ved hjelp av en TSA, jf. XAdES-T. NB Dette trenger ikke være samme TSA eller samme TS sertifikat som ble benyttet i SignatureTimestamp i XAdES-T.

I e-resept kan dette anvendes for å presentere en gyldig signatur til utleverer og HELFO selv i de tilfellene der

- både rekvirentens og TSAens (Reseptformidleren) sertifikater har enten gått ut på dato eller endret status.
- RF skifter virksomhetssertifikat.
- TSAens (Reseptformidleren) sertifikat som benyttes til SignatureTimestamp er gyldig i mindre enn ett år til.

Alle aktører kan legge til nye arkivtidsstempler ved behov over tid.

Eksempelet på neste side viser bruken av XAdES-A i XML.

Eksempel 9 XAdES-A (Neste side)

```
    <ds:Object>
        <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#Signature">
            <xades:UnsignedProperties>
                <xades:UnsignedSignatureProperties>
                    <xades:SignatureTimeStamp Id="SignatureTimeStamp"><!-- --></xades:SignatureTimeStamp>
                    <xades:CertificateValues Id="CertificateValues"><!-- --></xades:CertificateValues>
                    <xades:RevocationValues Id="RevocationValues"><!-- --></xades:RevocationValues>
                    <xades:ArchiveTimeStamp Id="ArchiveTimeStamp">
                            <xades:XMLTimeStamp>
                            <dss:Timestamp xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
                                <ds:Signature Id="XMLArchiveTimeStampTokenSignature">
                                    <ds:SignedInfo>
                                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                                        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                                        <ds:Reference URI="#SignatureValue"><!-- --></ds:Reference>
                                        <ds:Reference URI="#KeyInfo"><!-- --></ds:Reference>
                                        <ds:Reference URI="#SignatureTimeStamp"><!-- --></ds:Reference>
                                        <!-- <ds:Reference URI="#CounterSignature"/> -->
                                        <ds:Reference URI="#CertificateValues"><!-- --></ds:Reference>
                                        <ds:Reference URI="#RevocationValues"><!-- --></ds:Reference>
                                        <ds:Reference URI="#ArchiveTstInfo"
                                        Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken">
                                        <!-- -->
                                        </ds:Reference>
                                        <ds:Reference URI="#XMLArchiveTimeStampTokenKeyInfo"><!-- --></ds:Reference>
                                    </ds:SignedInfo>
                                    <ds:SignatureValue
Id="XMLTimeStampTokenSignatureValue">JNR...jY=</ds:SignatureValue>
                                    <ds:KeyInfo Id="XMLArchiveTimeStampTokenKeyInfo"><!-- --></ds:KeyInfo>
                                    <ds:Object Id="ArchiveTstInfo">
                                        <dss:TstInfo>
                                                <!-- Se XAdES-T eksempel for beskrivelse av innhold -->
                                        </dss:TstInfo>
                                    </ds:Object>
                                </ds:Signature>
                            </dss:Timestamp>
                        </xades:XMLTimeStamp>
                    </xades:ArchiveTimeStamp>
                </xades:UnsignedSignatureProperties>
            </xades:UnsignedProperties>
```

Vedlegg H; Feilhåndtering og alternative rutiner i behandling av ekspederingsanmodning (M21) i RF

I utvikling av e-resept er det lagt stor vekt på å håndtere ulike feilsituasjoner slik at løsningen er sikker. Dersom feil skulle oppstå knyttet til ekspederingsanmodning er det nødvendig å ha etablert alternative rutiner som kan settes i verk. Det er da nødvendig at rekvirent, utleverer (apotek eller bandasjist) og e-reseptforvaltning er omforent om disse rutinene og at disse tar hensyn til pasientens beste. Helsedirektoratets fagavdeling for legemidler (SPML) er blitt bedt om å vurdere forvaltningens forslag til en alternativ rutine i det tilfellet der e-resept med ekspederingsanmodning (M21) vellykket er sendt til RF, men der utleverer av forskjellige årsaker ikke har mottatt M21.

M21 er nødvendig for at én bestemt utleverer skal få melding om, og ekspedere forsendelsesresepten, og deretter å sende av gårde varepakken. Fagavdelingens vurdering er gjengitt på nedenfor..

Problemstilling

I dag (uten e-resept) overfører legen forsendelsesresepter til spesifikke utleverere pr. telefon eller telefaks. Dette gjøres gjerne på faste klokkeslett som er tilpasset rutetider for videre transport til kommisjonær. Kommisjonæren vil typisk være et utsalg i butikk på ett mindre tettsted uten egen utleverer. Pasienten henter så medisinpakken hos kommisjonæren.

I e-resept vil legen sende reseptene til RF på vanlig måte merket med <Forsendelse>. RF vil så generere en M21 melding som sendes direkte til den aktuelle utleverer.

Feilsituasjon som kan oppstå:

Rutinene for feilhåndtering er utarbeidet i forbindelse med følgende feilsituasjoner:

> *Legen sender resepten til RF og får en positiv applikasjonskvittering (AppRec) fra RF som bevis på at resepten har kommet korrekt fram til RF. M21 derimot, kommer ikke fram til utleverer på grunn av kommunikasjonsproblemer mellom RF og utleverer. Utleverer er derfor uforberedt på at forsendelsesresepten ligger klar for ekspedering i RF.*
>
> *RF vil sende M21på nytt etter 25 minutter dersom det ikke mottas kontakt med utleverer. Dersom denne også feiler igangsettes avvikshåndtering.*

Hvilke tiltak skal settes i verk?

To prinsipielle spørsmål:

1. **Hastegrad**? Hvor raskt skal varsling igangsettes? Skal det være oppfølging/bekreftelse på at avviksrutiner er igangsatt?
2. **Hvem mottar varsel om avvik?** Skal dette sendes til utleverer eller lege?

Helsedirektoratets vurdering

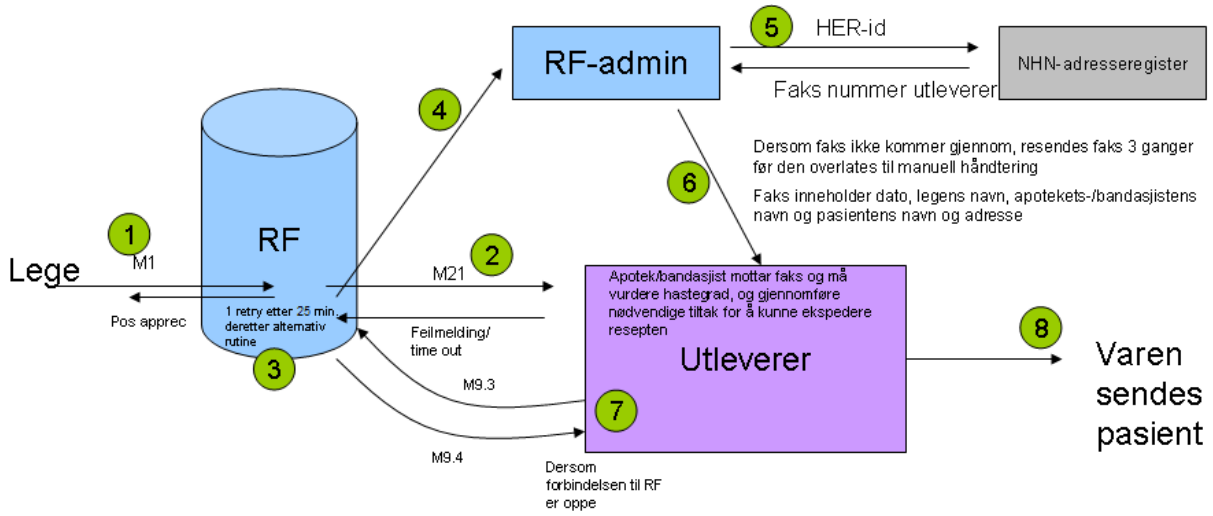
1. **Hastegrad**? Dersom det er viktig at pasienten får medisinen samme dag (akutt sitasjon) vil legen normalt gjøre tiltak for å forsikre seg om dette skjer gjennom å kontakte utleverer og gjøre de oppmerksomme på hastegraden. Legen vil også som oftest kunne initiere hastebehandling med medisiner fra egen legekoffert eller lokalt lager. Det er derfor lite trolig at en normal forsendelsesresept, der legen ikke samtidig kontakter utleverer, har en kritisk hastegrad. Dersom medisinpakken skulle miste sin normale tidsfrist i forhold til transport til kommisjonær vil dette altså normalt ikke ha en negativ effekt på pasientens sin helsetilstand. Helsedirektoratet vil påpeke at lignende situasjoner også kan oppstå med dagens rutiner (uten e-resept) ved at forsendelses-resepten av forskjellige årsaker ikke kommer fram til utleverer i tide, eller at medisinpakken ikke kommer fram til transportør i tide. I slike tilfeller vil det som oftest være en lokal forståelse mellom lege og utleverer hvordan situasjonen bør håndteres. Denne lokale forståelsen må selvsagt opprettholdes med e-resept.
2. **Hvem mottar varsel om avvik?** *Utleverer* vil etter Helsedirektoratets vurdering ha størst behov for å varsles da det er utleverer som er avhengig av tidsfristen til forsendelsestransportørene og som kan forholde seg til, og eventuelt påvirke, denne. Dette begrunnes i følgende: Rutinene hos utleverer for å etterspørre resepter hos legen er erfaringsmessig såpass godt innarbeidet at Helsedirektoratet har tillit til at utleverer vil kunne håndtere dette på en best mulig måte. Dersom det skulle være umulig å få tak i legen har utleverer mulighet til å iverksette nødrutiner som nødekspedisjon eller kontakte annen utleverer som *har* kommunikasjon med RF og som kan lese den komplette reseptinformasjonen. Utleverer har også mulighet til å kontakte kommisjonær og/eller pasient/kunde og avtale ekstraordinære leveringsløsninger. Et ytterligere argument vil være at utleverer i mange tilfeller vil ha lengre åpningstid enn legekontoret. Legen kan således ha forlatt kontoret på den tiden feilmeldingen returneres fra RF.

Forvaltningens løsning:

To påfølgende negative applikasjonskvitteringer, feilmeldinger eller time-out vil utløse en automatisk blokkering av denne utleverer i RF. På grunnlag av dette vil RF stanse nye forsendelsesanmodninger til den aktuelle utleverer inntil kommunikasjonen er gjenopprettet og feilsituasjonen lukket. Rekvirenter vil ved forsøk på forsendelsesanmodning til denne utleverer deretter få en spontan negativ applikasjonskvittering og må vurdere alternative løsninger for formidling av resepten (telefon, telefaks, forsendelsesanmodning til annen utleverer eller lignende). Avtale om dette gjøres mellom den enkelte lege og utleverer.

Utleverer vil også kunne blokkeres basert på melding fra leverandør om planlagt nedetid eller ved andre driftsmessige avvik hos utleverer. Dette gjør at legen i disse tilfellene vil få en umiddelbar negativ AppRec ved forsøk på å sende forsendelsesanmodning til denne utleverer.

Resepter som ble sendt før blokkeringen (der legen allerede har fått en positiv AppRec på innsending til RF) vil, dersom RF ikke mottar kvittering fra utleverer på mottatt M21, generere et varsel til utleverer pr. telefaks der legens og pasientens entydige identifikasjon samt reseptens utstedelsestidspunkt er spesifisert. Utleverer vil kunne få beskjed om dette pr. telefaks etter ca. 51 minutter. Utleverer vil dermed kunne iverksette rutiner for å skaffe tilveie resepten(e) fra legen på alternative måter, for eksempel via telefon eller telefaks. Dersom kontakten med Reseptformidleren i mellomtiden er gjenopprettet vil den gyldige resepten også kunne hentes fra RF til utleverers datasystem.



Figur 11.

Trinn 1: M1 m/forsendelsesanmodning sendes RF, M1/M21 er ankommet RF og rekvirent mottar positiv AppRec fra RF (unntatt hvis utleverer er blokkert.)

Trinn 2: M21 sendes og resendes til RF mottar positiv AppRec fra utleverer

Trinn 3: Dersom resending feiler (Ingen AppRec eller negativ AppRec) initierer RF alternativ rutine

Trinn 4: Varsel sendes til RF-admin og trigger en alarm her

Trinn 5: Faksnummer og annen relevant utleverer-info samt info om rekvirent hentes i adresseregisteret

Trinn 6: Det genereres en faks med relevante opplysninger fra RF (legenavn, pasientnavn, pasientadresse) som sendes til utleverer

Trinn 7: Utleverer iverksetter alternativ rutine (Henter resept) dersom kontakten med RF er tilgjengelig, kontakter lege dersom RF er utilgjengelig. Dersom det er grunnlag for nødekspedering skal dette benyttes)

Trinn 8: Varen ekspederes og forsendes etter alternativ rutine

Til trinn 6: Dersom telefaksmeldingen ikke kommer igjennom etter for eksempel 3 forsøk vil forvaltningen innen ordinær åpningstid (08.00 – 15.45) manuelt prøve å kontakte utleverer pr telefon. Forvaltningen får varsel på e-post både når telefaks er sendt og når telefaks er forsøkt sendt men har feilet.

Driftsoperatør hos systemleverandør/utleverer vil varsles gjennom ordinært feilhåndteringssystem.

Oppsummering:

- Det er rekvirents ansvar å sikre at hasteresepter når utleverer i tide. Det må inn i legens rutiner, at rekvirent forsikrer seg om at slike resepter kommer til utleverer.
- Det sendes telefaks (med kvitteringsfunksjon) til utleverer fra RF dersom RF ikke mottar positiv AppRec etter ca. 51 minutter (sending pluss én resending).
    - Hvis utleverer *har* kontakt med RF, kan utleverer hente ned reseptene og iverksette forsendelsen ut fra opplysninger på telefaksen.
    - Dersom utleverer er avskåret fra RF, *og situasjonen hos utleverer tilsier at det er praktisk mulig*, tar utleverer kontakt med legen slik at legen har mulighet for å sende resept på alternativ måte. Hvis legen resender resepter på alternativ måte må de opprinnelige reseptene i RF trekkes tilbake av legen.
    - Hvis utleverer *ikke* får kontakt med rekvirent iverksetter utleverer andre tiltak for å få tak i reseptene, dersom det er praktisk mulig.
    - Hvis det ikke er praktisk mulig for utleverer å sette i verk alternative tiltak (utleverer, og da særlig apotek, vil i utgangpunktet være i en unntakstilstand dersom de er avskåret fra RF), bruker utleverer opplysninger fra telefaks og laster ned reseptene fra RF når situasjonen er normalisert og det igjen oppnås kontakt med RF.

Vedlegg I; Feltlengder

Det er ingen lengdebegrensning på felter i XML dokumenter, men det er flere andre forhold i e-resept som begrenser hvor lange felter i meldingene i praksis kan være.

Under følger en oversikt over felter i meldinger med begrensninger. Feltlengder øverst i tabellen danner grunnlag for andre feltlengder (gjenbrukes).

For Familyname, MiddleName og GivenName er det ingen begrensning på feltet i meldingen, men Reseptformidleren vil trunkere feltet til maks lengde før det lagres,

Feltnavn	Melding	Maks lengde
MsgId	Hodemelding	36
FamilyName	Hodemelding	30
MiddleName	Hodemelding	30
GivenName	Hodemelding	30
FNR (Patient/Ident TypeID = FNR)	Hodemelding	11
DNR (Patient/Ident TypeID = DNR)	Hodemelding	11
Orgnr (Organisation/Ident TypeID = ENH)	Hodemelding	9
OrganisationName	Hodemelding	60
Her-id (Organisation/Ident TypeID = HER)	Hodemelding	20
Her-id (Healtcareproffesional/Ident TypeID = HER)	Hodemelding	20
HPR (Healtcareproffesional/Ident TypeID = HPR)	Hodemelding	9
StreetAdresse	Hodemelding	50
PostalCode	Hodemelding	4
City	Hodemelding	30
TeleAdress	Hodemelding	20
Postbox	Hodemelding	30
RefNr	Flere meldinger	10
Utleverer (EkspAnm)	M1	12

Kontaktperson (EkspAnm)	M1	60
Merknad (EkspAnm)	M1	255
UtlevererNavn (EkspAnm)	M1	60
Merknad (ReseptDokLegem..)	M1 m.fl.	255
KomLegemdlAdm	M1	20
Reiterasjon	M1 m.fl.	3
Begrunnelse	M1	1000
Produsent (LegemiddelutenMT)	M1	60
Bruksomrade	M1 m.fl.	1000
DosVeiledEnkel	M1 m.fl.	2000
Merknad (doseringsregel)	M1 m.fl.	255
NavnFormStyrke	M30, M1 m.fl.	255
Varenummer	M30, M1 m.fl.	8
Varenavn (LegemiddelMerkevare, PakningsInfoResept)	M1 m.fl.	255
Pakningsstr	M1 m.fl.	60
Navn (Legemiddelblanding)	M1 m.fl.	255
TilbOppl	M1 m.fl.	2000
NavnFormStyrke (BestandAnnet)	M1 m.fl.	255
Merknad (ReseptDokHandelsvare)	M1 m.fl.	255
Bruksveiledning	M1 m.fl.	2000
Kommentar	M3	255
Kommentar (Allergi)	M25	1000
Virkestoff (Legemiddelreaksjon)	M25	255
Id (Enkeltoppforing)	M25	36
ReseptId	M25, M10	36
Merknad (LegemidlerIBruk)	M25	255
RefM10	M25	36
Bilderef	M25	1000
Navn (Utleverer)	M10 m.fl.	60
AnnulleringsId	M10	36
AnsattId	M10	11
Begrunnelse (Intervensjon)	M10	255

Batchnummer	M10	255
Begrunnelse	M2	400
Merknad	M2	400
Underterm	M2	60
Merknad	M5	200
NavnUtleverer	M9.6	60
NavnRekvirent	M9.2	92
MerknadTilbakekalling	M9.2	200
NavnUtleverer	M9.2	60
LegemiddelblandingNavn	M9.2	255
Bruksomrade	M9.2	1000