

Direktoratet for forvaltning og IKT

Arkitekturbeskrivelse for Sikker digital posttjeneste

Versjon 1.0

Endringslogg

Versjon	Når	Hvem	Beskrivelse
1.0	16.8.2013		Arkitekturbeskrivelse

Innhold

1. INNLEDNING	1
2. ARKITEKTURVISJON.....	2
2.1 OMFANG OG AVGRENSNINGER.....	2
2.2 VIRKSOMHETSMÅL OG STRATEGIER	3
2.2.1 <i>Bedre tjenester og kostnadseffektivitet</i>	3
2.2.2 <i>Sikker kommunikasjon</i>	4
2.2.3 <i>Regelverk</i>	4
2.3 DIGITALISERINGSPROGRAMMETS PRINSIPPER	4
2.3.1 <i>Arkitekturprinsipper:</i>	4
2.3.2 <i>Designprinsipper</i>	5
2.3.3 <i>Løsningsprinsipper</i>	5
3. FORRETNINGSARKITEKTUR	6
3.1 AKTØRER OG ROLLER.....	6
3.1.1 <i>Aktører i den digitale kommunikasjonen</i>	6
3.1.2 <i>Aktører i den digitale postforsendelsen</i>	7
3.1.3 <i>Avsender- og mottakerroller</i>	9
3.1.4 <i>Avsender av digital post fra offentlig virksomhet</i>	10
3.1.5 <i>Oppslagstjeneste for kontakinformasjon</i>	13
3.1.6 <i>Aktører og roller sett i relasjon til overordnede forretningstjenester</i>	15
3.1.7 <i>Difi som sentralforvalter og tilbyder av Sikker digital posttjeneste</i>	16
3.2 TJENESTEMODELL	17
3.2.1 <i>Overordnet tjenestemodell</i>	17
3.2.2 <i>Detaljert tjenestemodell</i>	18
3.2.3 <i>Oppslagstjeneste for kontakinformasjon</i>	19
3.2.4 <i>Postformidling</i>	20
3.2.5 <i>Avtale- og administrasjonstjeneste</i>	22
3.2.6 <i>Loggtjeneste</i>	28
3.2.7 <i>Distribusjon av postformidlingstjenesten</i>	28
3.3 VIRKSOMHETSPROSESSER.....	30

3.3.1 De overordnede prosessene som realiserer den digitale postformidlingstjenesten i Sikker digital posttjeneste	30
3.3.2 Detaljering av forretningsprosessen Ekspedere post	31
3.3.3 Detaljering av forretningsprosessen Formidle post	32
3.3.4 Detaljering av forretningsprosessen Oppbevare post	33
3.3.5 Detaljering av forretningsprosessen Lese post	34
3.3.6 Sikker digital posttjenestens håndtering av papirpost	35
3.3.7 Kvittering i forbindelse med postformidling	37
3.3.8 Detaljering av oppslagstjenesten	38
3.3.9 Opprette digital postkasse	39
3.3.10 Registrere digital postkasse	39
3.3.11 Bytte digital postkasse	41
4. INFORMASJONSARKITEKTUR	42
4.1 FORRETNINGSOBJEKTER	42
4.1.1 Digital post	42
4.1.2 Kontakt- og kommunikasjonsinformasjon	43
4.1.3 Logg	45
4.1.4 Dataobjektene som realiserer forretningsobjektene	48
4.2 INFORMASJONSMODELLER	48
4.2.1 Digital post	49
Informasjon om distribusjonen	50
Informasjon om innholdet	51
Dokument	52
Varslingsinformasjon	53
4.2.2 Batch-forsendelse	53
4.2.3 Innbyggers kontaktinformasjon	54
4.2.4 Virksomhetens kommunikasjonsinformasjon	56
4.2.5 Logg	57
4.2.6 Kvittering	58
5. SIKKERHETSARKITEKTUR	60
5.1 SIKKERHETSFORUTSETNINGER OG BETINGELSER	60

5.2	TEKNISKE TILTAK FOR ETTERFORSKNING.....	60
5.2.1	<i>Unik identifikator for digital post.....</i>	60
5.2.2	<i>Tilgangskontroll</i>	60
5.2.3	<i>Kryptografisk sikkerhet</i>	61
5.2.4	<i>Systemkvitteringer</i>	61
5.2.5	<i>Sporing</i>	61
5.2.6	<i>Hinder mot uautorisert tilgang</i>	61
5.3	NIVÅ FOR AKSEPTABEL RISIKO.....	61
5.4	VERDIER OG EIERE	61
5.5	KONSEKVENSER FOR BRUDD PÅ TILGJENGELIGHET.....	61
5.6	KRYPTOGRAFISK BESKYTTELSE AV DIGITAL POST.....	62
5.6.1	<i>Konfidensialitet</i>	62
5.6.2	<i>Integritet</i>	63
APPENDIKS A.	METODE OG RAMMEVERK.....	64
A.1.1	<i>ADM – Architecture Development Method</i>	64
A.1.2	<i>Architecture Content Framework - Content Metamodel</i>	64
A.1.3	<i>Archimate metamodeller.....</i>	65
A.1.4	<i>Archimate – symbolforklaring</i>	67

Figurer

FIGUR 1: VERDIKJEDE	2
FIGUR 2: AKTØRENE I DEN DIGITALE KOMMUNIKASJONEN.....	7
FIGUR 3: AKTØREN SIKKER DIGITAL POSTTJENESTE	7
FIGUR 4: DETALJERING AV AKTØREN SIKKER DIGITAL POSTTJENESTE	9
FIGUR 5: AVSENDER OG MOTTAKER AV DIGITAL POST FRA DET OFFENTLIGE	10
FIGUR 6: AVSENDER AV DIGITAL POST FRA OFFENTLIG VIRKSOMHET	11
FIGUR 7: AKTØRENES ROLLER KNYTTET TIL DIGITAL POST	12
FIGUR 8: FORVALTERE OG TILBYDERE AV KONTAKTREGISTERTJENESTER.....	14
FIGUR 9: AKTØRENES ROLLER KNYTTET TIL INNBYGGERS KONTAKTINFORMASJON	14
FIGUR 10: AKTØRER OG ROLLER MHT. POSTFORMIDLING GENERELT.....	16
FIGUR 11: VIRKSOMHETER SOM FORVALTERE OG LEVERANDØRER	17
FIGUR 12: OVERORDNET TJENESTEMODELL	18
FIGUR 13: DETALJERT TJENESTEMODELL	19
FIGUR 14: GODKJENNING AV AVSENDERE.....	25
FIGUR 15: INTEGRASJON OG TEST	26
FIGUR 16: DISTRIBUSJON AV POSTFORMIDLINGSTJENESTEN	29
FIGUR 17: OVERORDNET PROSESSMODELL	30
FIGUR 18: EKSPEDERE POST	32
FIGUR 19: FORMIDLE POST	33
FIGUR 20: OPPBEVARE POST	34
FIGUR 21: LESE POST	35
FIGUR 22: HÅNDTERING AV PAPIRPOST	36
FIGUR 23: SENDE PAPIRPOST	37
FIGUR 24: KVITTERINGER I FORBINDELSE MED POSTFORMIDLING	38
FIGUR 25: DETALJERING AV OPPSLAGSTJENESTEN	39
FIGUR 26: INNBYGGERS PROSESSER FOR Å REGISTRERE DIGITAL POSTKASSE	40
FIGUR 27: KONTAKTREGISTERETS PROSESSER FOR Å REGISTRERE DIGITAL POSTKASSEADRESSE	40
FIGUR 28: INNBYGGERS PROSESSER FOR Å BYTTE DIGITAL POSTKASSE.....	41
FIGUR 29: DIGITAL POST.....	42

FIGUR 30: KONTAKT- OG KOMMUNIKASJONSINFORMASJON	43
FIGUR 31: LOGG	45
FIGUR 32: KVITTERING	46
FIGUR 33: DATAOBJEKTER	48
FIGUR 34: DIGITAL POST.....	49
FIGUR 35: INFORMASJON OM DISTRIBUTJON	50
FIGUR 36: INFORMASJON OM INNHOLDET	51
FIGUR 37: DOKUMENT.....	52
FIGUR 38: VARSLINGSINFORMASJON.....	53
FIGUR 39: BATCH.....	53
FIGUR 40: INNBYGGERS KONTAKTINFORMASJON	54
FIGUR 41: VIRKSOMHETENS KOMMUNIKASJONSINFORMASJON	56
FIGUR 42: LOGG	57
FIGUR 43: KVITTERING	58
FIGUR 44: ARCHITECTURE DEVELOPMENT METHOD.....	64
FIGUR 45: TOGAF FULL CONTENT METAMODEL	65
FIGUR 46: FORENKLET METAMODELL - AKTØRER OG ROLLER.....	66
FIGUR 47: FORENKLET METAMODELL - FORRETNINGSTJENESTER OG –PROSESSER.....	66
FIGUR 48: FORENKLET METAMODELL - INFORMASJONS- OG APPLIKASJONSARKITEKTUR	67

1. Innledning

Dette dokumentet er en beskrivelse av arkitekturen til Sikker digital posttjeneste og er utarbeidet av arkitekturprosjektet i Program for sikker digital post. Dokumentet er et uttrekk av arkitekturarbeidet som er gjort i prosjektet. Formålet er å gi en helhetlig beskrivelse av målarkitekturen.

Sikker digital posttjeneste består av fem sentrale aktører:

- Oppslagstjeneste for kontaktinformasjon
- Kontakt- og reservasjonsregister
- Meldingsformidler
- Digitale postkasser
- Utskrifts- og forsendelsestjeneste

Dokumentet beskriver disse aktørene og setter dem i sammenheng med avsendervirksomhetene og deres ekspederingstjeneste og innbygger i rollen som postmottaker.

Prosjektet har benyttet TOGAF arkitekturrammeverk i arbeidet og det er hovedsakelig arbeidet med forretningsarkitektur, informasjonsarkitektur og sikkerhetsarkitektur som er tatt med her. Innledende arbeid og utredninger er ikke tatt med i dokumentet.

Forretningsarkitekturen er beskrevet gjennom aktør og rollemodeller, tjenestemodeller og virksomhetsprosesser. Informasjonsarkitekturen er beskrevet gjennom forretningsobjekter og dataobjekter.

Alle figurer i forretningsarkitekturen og informasjonsarkitekturen er laget i Archimate modelleringsspråk. Metamodeller og tegnforklaring ligger i slutten av dokumentet i Appendiks A.

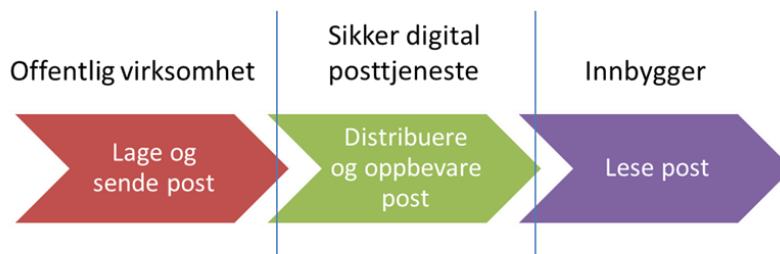
2. Arkitekturvisjon

Arkitekturvisjonen til fellestjenesten Sikker digital posttjeneste er basert på eksisterende beslutninger, strategidokumenter og utredninger. Arkitektgruppen i Difi har sammenfattet og strukturert det eksisterende til en visjon for arkitekturen

2.1 Omfang og avgrensninger

Arkitekturen har fokus på dialogene mellom offentlig forvaltning og innbygger og næringsliv. Sikker digital posttjeneste som etableres på bakgrunn av anskaffelsesprosess startet opp i mai 2013, omfatter kun dialogene mellom offentlig forvaltning og innbygger.

Hovedmålet er å etablere digital kommunikasjon mellom forvaltningen og mottakere. Dette er i tråd med politikken om digitalt førstevalg. Dialogen mellom forvaltningen (offentlige virksomheter) og innbyggere og næringsliv (mottakere) skal skje elektronisk der det er mulig og formålstjenlig.



Figur 1: Verdikjede

Følgende avgrensninger er gjort i arkitekturen:

- I første omgang avgrenses arkitekturarbeidet til å etablere fellestjenesten *Sikker digital posttjeneste*.
- Sikker digital posttjeneste skal understøtte sikker digital kommunikasjon *fra* offentlig forvaltning *til* postmottaker, i første omgang avgrenset til innbyggere.
- Sikker digital posttjeneste skal understøtte digital kommunikasjon som skjer i *skriftlig form* mellom forvaltningen og postmottaker og som kan kreve skjerming.
- Sikker digital posttjeneste er *ikke* en tjeneste for innsyn i offentlige virksomheters arkiv og saksbehandlingssystemer, men en fellestjeneste der innbyggere kan motta post fra offentlige virksomheter.
- Sikker digital posttjeneste skal legge til rette for at innbyggere skal kunne fortsette dialogen med forvaltningen, etter at post er mottatt, i andre digitale tjenester uten å autentisere seg på nytt overfor disse tjenestene.
- Sikker digital posttjeneste vil i første omgang ikke ha sentrale løsninger for å håndtere fullmakter, vergemål og mindreårige. Dette er overlatt til avsendervirksomhetene.

Sentrale forutsetninger i arkitekturarbeidet:

- Den offentlige virksomheten som sender en melding har behandlingsansvaret for meldingen til det er bekreftet at den er mottatt i mottakers postkasse.
- ID-porten skal kunne benyttes til å autentisere innbyggere overfor Sikker digital posttjeneste hvor innbyggere skal kunne lese post fra offentlige, selv om posttjenesten er levert av private aktører.
- Regelverket vil legge opp til at innbyggere skal kunne reservere seg mot å motta enkeltvedtak og andre meldinger av særlig betydning digitalt, se høringsnotat av 11. juni 2013 fra Fornyings-, administrasjons og kirkedepartementet, med utkast til endringer av eForvaltningsforskriften.
- Sikker digital posttjeneste skal utformes slik at innbyggere selv skal kunne velge mellom ulike tilgjengelige postkasser hvor han vil ha sin post fra det offentlige.
- Arkitekturen legger opp til at det kan etableres en løsning for utskrift, konvoluttering og forsendelse av brev til mottakere som har reservert seg eller ikke registrert/oppdatert sin kontaktinformasjon.

2.2 Virksomhetsmål og strategier

Med bakgrunn i strategidokumenter er det trukket fram en del virksomhetsmål og strategier som kan påvirke arkitekturen. Oversikten er ikke ment å være uttømmende, det finnes andre mål og strategier med potensiell effekt på arkitekturarbeidet. Imidlertid antas listen å være representativ med tanke på krav til arkitekturen.

Arkitekturen baserer seg på følgende strategidokumenter:

- Regjeringens digitaliseringsprogram (2012): [På nett med innbyggerne](#)
- St.meld. nr. 17 (2006-2007) [Eit informasjonssamfunn for alle](#)
- St.meld. nr. 19 (2008-2009) [Ei forvaltning for demokrati og fellesskap](#)

I tillegg utgjør følgende utredninger en basis for strategimålenes rasjonale og relasjoner til Sikker digital posttjeneste:

- *Difi rapport 2011-7. [En felles meldingsboks](#)*
- *Difi rapport-2012-10. [Sikker digital post](#)*

2.2.1 Bedre tjenester og kostnadseffektivitet

Det er en forutsetning at Sikker digital posttjeneste innebærer effektiv utnyttning av offentlige ressurser, og gir innbyggerne enklere og bedre tjenester.

Etablering av Sikker digital posttjeneste:

- Skal redusere investeringsbehov for forvaltningen som helhet.
- Skal redusere forvaltningskostnader knyttet til IT.
- Skal redusere forvaltningskostnader knyttet til distribusjon av post (utskrift, konvoluttering, porto etc.).
- Skal bidra til at forvaltningen raskt kan etablere utsending av digital post til innbyggere.

- Skal sikre at innbyggere kan få digital post fra det offentlige i en sikker postkasse.

2.2.2 Sikker kommunikasjon

For forvaltningen og innbyggere er det en forutsetning at en Sikker digital posttjeneste ivaretar den lovpålagte og egenvurderte informasjonssikkerheten for informasjonen som sendes via tjenesten.

Etablering av Sikker digital posttjeneste:

- Skal sikre at det oppnås tillit hos forvaltningen og mottakere til definert sikkerhetsnivå.
- Skal sikre at meldingenes konfidensialitet, integritet og tilgjengelighet ivaretas.

2.2.3 Regelverk

Følgende lover med forskrift regulerer en felles løsning for digital post (ikke uttømmende):

- Personopplysningsloven (LOV 2000-04-14 nr. 31 - Lov om behandling av personopplysninger)
- Forvaltningsloven (LOV-1967-02-10 - Lov om behandlingsmåten i forvaltningssaker)
- Helseregisterloven (LOV 2001-05-18 nr. 24 - Lov om helseregistre og behandling av helseopplysninger)
- Esignaturloven (LOV 2001-06-15 nr. 81 - Lov om elektronisk signatur)

Følgende policydokumenter er også relevante referanser:

- Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf
- Veiledning i risikoanalyse. <http://www.difi.no/artikkel/2010/02/veileder-i-risikovurdering-for-elektronisk-kommunikasjon>
- Norm for informasjonssikkerhet i helsesektoren. <http://www.helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/Sider/default.aspx>
- Overordnede arkitekturprinsipper for offentlig sektor. <http://www.difi.no/filearchive/arkitekturprinsipper-2.1.pdf>

2.3 Digitaliseringsprogrammets prinsipper

Regjeringen har i sitt digitaliseringsprogram "På nett med innbyggeren" satt noen prinsipper for hva som skal realiseres og hvordan.

2.3.1 Arkitekturprinsipper:

- Digital kommunikasjon skal være hovedregelen for kommunikasjon med forvaltningen
- Forvaltningen skal tilby helhetlige og brukervennlige digitale tjenester

- Utvikling av IKT-løsninger skal sees i sammenheng med forvaltningens arbeidsprosesser og organisering
- Digitaliseringstiltak som har betydning for flere tjenester, skal samordnes

2.3.2 Designprinsipper

- Innlogging til offentlige nettjenester skal være enkel og sikker
- Innbyggere skal få hjelp til å finne fram til og bruke digitale tjenester
- Hensyn til personvern og informasjonssikkerhet skal ivaretas

2.3.3 Løsningsprinsipper

- «Innbyggere og bedrifter skal få post fra forvaltningen i én sikker, digital postkasse». Sikker digital posttjeneste, som etableres på bakgrunn av anskaffelsesprosess startet opp i mai 2013, har kun fokus på innbyggere.
- «Innbyggere og bedrifter skal få varsling på sms og e-post». Andre varslingsformer enn sms og e-post kan også være aktuelle for å oppfylle prinsippet.

3. Forretningsarkitektur

Forretningsarkitekturen beskriver forretningsstrategien mht. eierskap til og ansvar for forretningstjenester, arbeidsdeling og informasjonsflyt mellom aktører, samt de kritiske forretningsmessige begrepene som definerer aktørenes roller og verdiene forretningen håndterer. Formålet med forretningsarkitekturen er å beskrive etablert enighet om ønsket forretningsstrategi mellom involverte forretningsaktører og etablere forretningskonteksten for arkitekturarbeidet i de øvrige arkitekturdomenene (informasjon, applikasjon og teknologi). Forretningsarkitekturen skal kommunisere med interessentene til arkitekturen og arkitekturens sluttprodukt.

Forretningsarkitekturen til fellestjenesten Sikker digital posttjeneste er basert på eksisterende beslutninger, strategidokumenter og utredninger. Arkitekturen er beskrevet av arkitektgruppen i Difi.

3.1 Aktører og roller

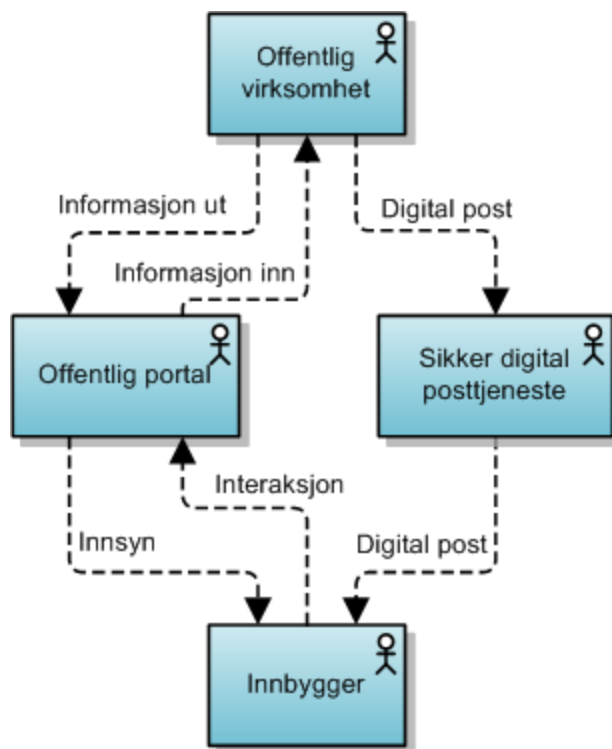
En aktør er en person, organisasjon eller system som har en rolle som initierer eller interagerer med aktiviteter. Aktører kan være interne eller eksterne i forhold til en organisasjon. (TOGAF).

En rolle er ansvaret en aktør tildeles for å utføre bestemte oppgaver (Archimate). En aktør kan ha mange roller (TOGAF).

3.1.1 Aktører i den digitale kommunikasjonen

Offentlige portaler og *Sikker digital posttjeneste* realiserer den digitale kommunikasjonen mellom *offentlige virksomheter* og *innbyggere*. I modellen under illustreres informasjonsflyten mellom disse aktørene.

- *Digital post* fra offentlig virksomhet til innbygger distribueres av Sikker, digital posttjeneste
- *Informasjon ut* fra offentlig virksomhet til innbygger distribueres av offentlig portal
- *Informasjon inn* til offentlig virksomhet fra innbygger samles av offentlig portal



Figur 2: Aktørene i den digitale kommunikasjonen

Sikker digital posttjeneste vil være distribusjonskanalen for digital post fra det offentlige til innbyggerne.

Den øvrige digitale dialogen mellom det offentlige og innbyggerne blir håndtert gjennom innsynstjenester og interaksjonstjenester i offentlige portaler, og arkitekturen skal legge til rette for at posttjenesten skal kunne brukes slik at dialogen mellom partene ivaretas. Dette vil i første hånd være gjennom bruken av lenker i dokumenter og eventuelt gjennom bruk av HTML med mulighet for å legge inn skjemaelementer, knapper, avkrysningsbokser og liknende.

3.1.2 Aktører i den digitale postforsendelsen

Sikker digital posttjeneste (kortnavn *posttjeneste*) vil være distribusjonskanalen for digital post fra det offentlige til innbyggerne.

Offentlig virksomhet sender digital post til Sikker digital posttjeneste, som igjen gir posten videre til innbygger. Figuren under viser den overordnede informasjonsflyten mellom aktørene i den digitale postforsendelsen.



Figur 3: Aktøren Sikker digital posttjeneste

Basert på en arkitekturutredning gjennomført av Difi skal det etableres én meldingsformidler som har til hensikt å understøtte en kostnadseffektiv sentral styring og forvaltning av posttjenesten. Når det gjelder digitale postkasser, har Regjeringen bestemt at Difi skal anskaffe sikre digitale postkasser i markedet. Regjeringens beslutning er basert på en samfunnsøkonomisk analyse som konkluderer med at anskaffelse av postkasser i markedet vil være kostnadseffektivt, bidra til raskere utbredelse, stimulere til innovasjon og gi bedre tjenester til innbyggere.

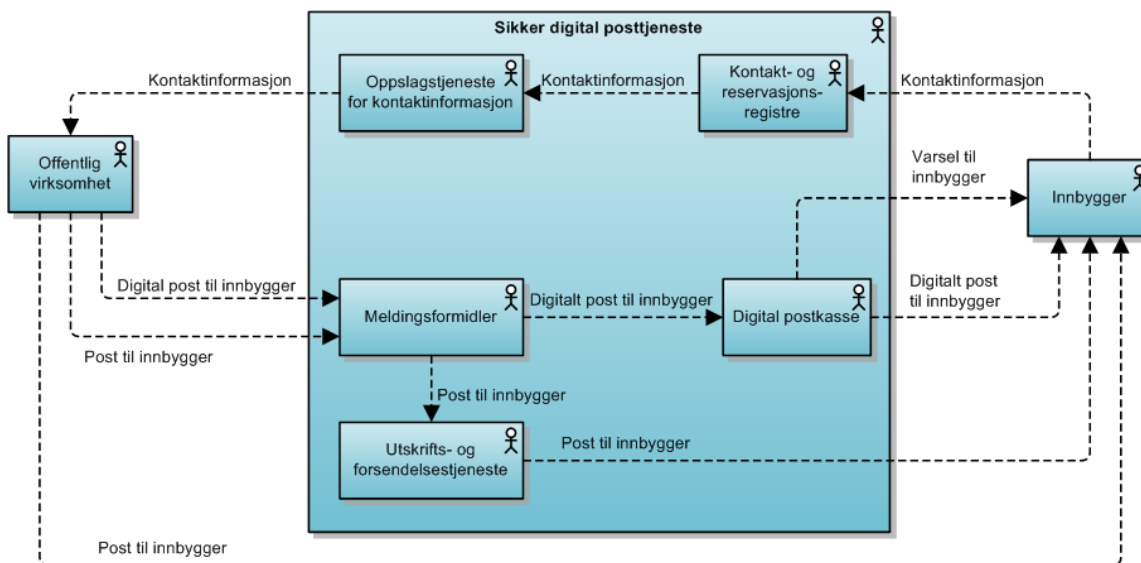
For at offentlige virksomheter skal kunne sende brev til innbyggere, må det offentlige kjenne til hvilken digital postkasse innbyggerne har eller om innbyggerne har reservert seg. Arkitekturen beskriver en oppslagstjeneste for kontaktinformasjon som vil gi tilgang til denne informasjonen. Oppslagstjenesten er tenkt å kunne brukes også til andre formål enn digital post.

Videre legges det til rette for at Sikker digital posttjeneste skal kunne være offentlige virksomheters totalleverandør for postforsendelse til innbyggere. Det vil si at aktøren skal kunne håndtere både digital og papirbasert post til innbygger.

Sikker digital posttjeneste består av fem sentrale aktører:

- *Oppslagstjeneste for kontaktinformasjon*: Offentlig virksomheters grensesnitt mot offentlige kontaktregistre som holder rede på innbyggerens valg knyttet til dialog med og postgang fra det offentlige.
- *Kontakt- og reservasjonsregistre*: Register for innbyggerens kontaktinformasjon til den digitale dialogen med det offentlige. Offentlig virksomhet har tilgang til innbyggerens kontaktinformasjon via oppslagstjeneste for kontaktinformasjon.
- *Meldingsformidler*: Offentlig virksomheters grensesnitt mot posttjenesten og som har ansvaret for å formidle post til innbygger, enten som digital post til innbyggerens selvvalgte digitale postkasse eller som papirbrev til innbyggerens postadresse.
- *Digital postkasse*: Innbyggerens grensesnitt mot posttjenesten og som har ansvaret for å gjøre tilgjengelig og oppbevare innbyggerens digitale post fra det offentlige.
- *Utskrifts- og forsendelsestjeneste*: Ivaretar Sikker digital posttjeneste som en totalleverandør for post til innbygger fra det offentlige, ved å sende papirbrev til innbygger som ikke kan eller ønsker å motta digital post.

Figur 4 viser en detaljering av posttjenesteaktøren, og flyten av informasjonsobjekter mellom aktørene.



Figur 4: Detaljering av aktøren Sikker digital posttjeneste

Arkitekturen legger opp til at offentlig virksomhet henter kontaktinformasjon til innbygger via oppslagstjeneste for kontaktinformasjon. Oppslagstjenesten henter kontaktinformasjon fra kontakt- og reservasjonsregistre. Innbygger er ansvarlig for at kontaktinformasjonen i registrene er oppdatert, og at de ikke legger inn skjermingsverdig kontaktinformasjon.

Når offentlig virksomhet har hentet kontaktinformasjon til innbygger, legger arkitekturen opp til at offentlige virksomhet adresserer postforsendelsen helt frem til innbygger. Dette kan gjøres på flere måter:

- Digital post til innbygger adresseres til innbyggers digitale postkasse og sendes via meldingsformidler.
- Post til innbygger adresseres til innbyggers postadresse og sendes til utskrifts- og forsendelsestjenesten via meldingsformidler.
- Post til innbygger adresseres til innbyggers postadresse og offentlig virksomhet bruker annen posttjeneste for videre transport.

3.1.3 Avsender- og mottakerroller

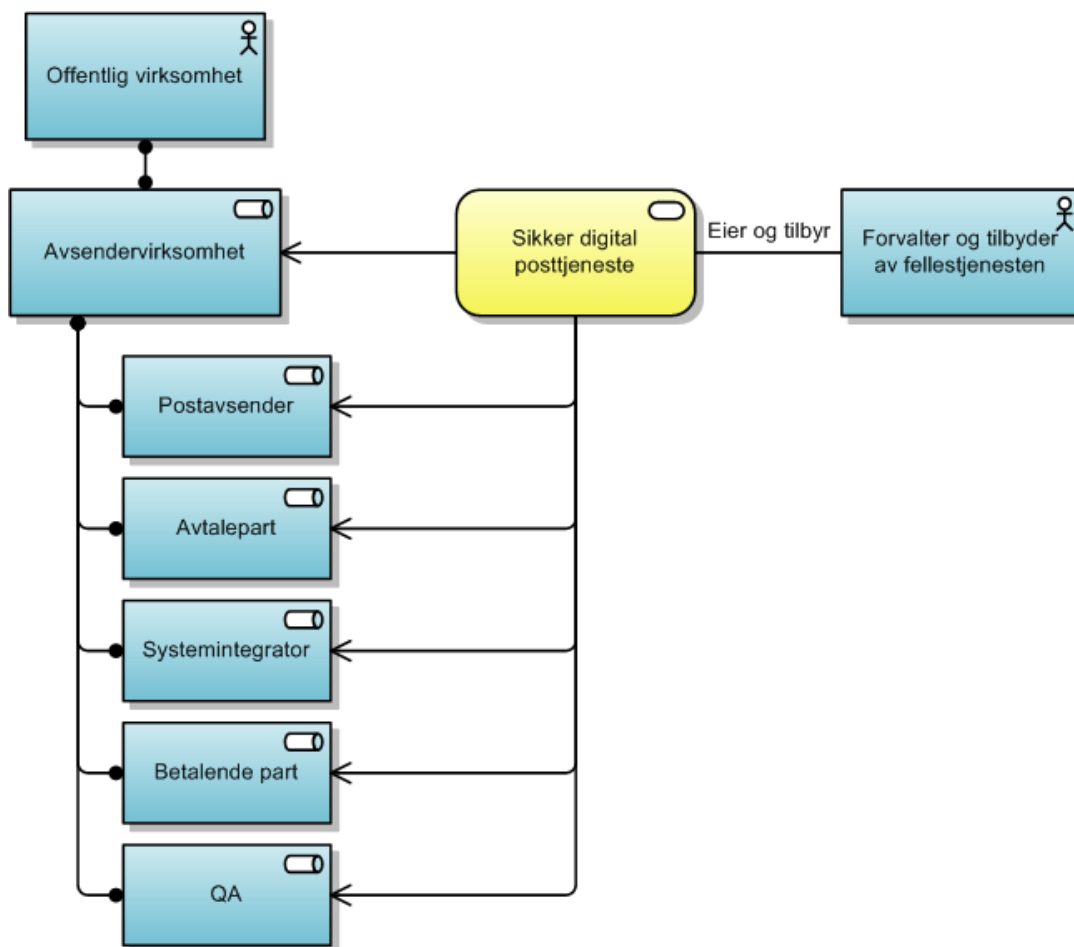
Offentlige virksomheter i rollen som *avsendervirksomhet* (kortnavn: postavsender) bruker posttjenesten til å sende digital post til innbygger. Innbygger i rollen som *mottaker av digital post fra offentlig virksomhet* (kortnavn: postmottaker) bruker posttjenesten for å lese og administrere sin digitale post fra det offentlige. Modellen (Figur 5) viser at det er én aktør som forvalter tjenesten og tilbyr denne til postavsendere og postmottakere (kortnavn: sentralforvalter eller forvalter). Forvalteren kan benytte andre til å utføre deler av tjenesten (f eks en markedsleverandør av digital postkasse som sentralforvalter har inngått avtale med.)



Figur 5: Avsender og mottaker av digital post fra det offentlige

3.1.4 Avsender av digital post fra offentlig virksomhet

Når en offentlig virksomhet skal sende digital post til innbyggerne er det flere oppgaver som må utføres. Figuren nedenfor viser forskjellige roller virksomheten har i forbindelse med utsending av digital post til innbyggerne.



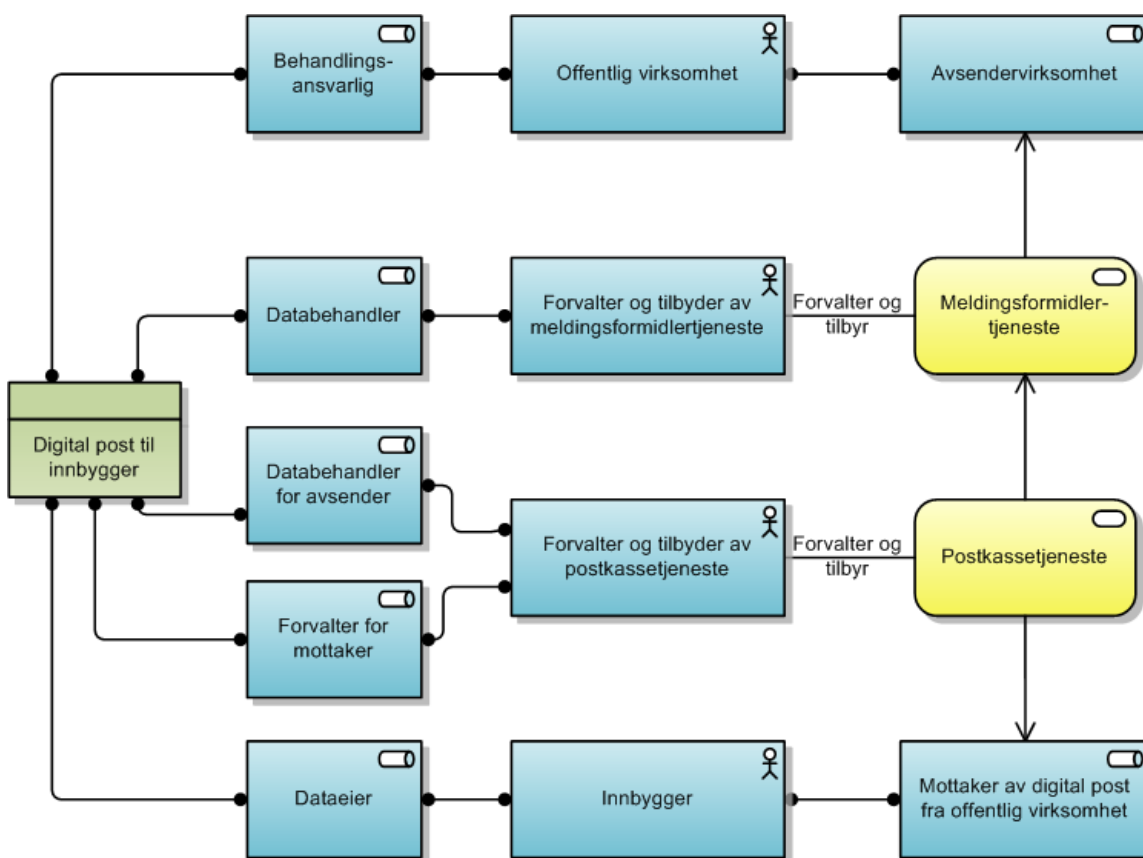
Figur 6: Avsender av digital post fra offentlig virksomhet

Rolle	Beskrivelse
Postavsender	Postavsenderen vil normalt være en saksbehandler som har post som ønskes formidlet digitalt til en eller flere postmottakere.
Avtalepart	Den offentlige virksomheten inngår en avtale med sentralforvalteren/ aksepterer sentralforvalters bruksvilkår før tjenesten benyttes. Den offentlige virksomheten vil ha ansvar for å benytte tjenesten i henhold til avtalen/bruksvilkårene.
Systemintegrator	Det vil ikke være mulig å sende digital post igjennom tjenesten uten først å gjøre en teknisk integrasjon mot tjenesten. For eksempel må virksomhetssertifikater bestilles og benyttes for å koble opp mot tjenesten.

Betalende part	Det er en kost forbundet med bruk av tjenesten, og denne må betales i henhold til avtale med sentralforvalter.
QA	Det vil være naturlig å følge opp statistikk forbundet bruk av tjenesten, og ved spesielle hendelser vil det være nødvendig å undersøke hva som har gått galt.

Aktørenes roller til digital post til innbygger

Digital post til innbygger er det sentrale forretningsobjektet som skal håndteres av de samhandlende aktørene i Sikker digital posttjeneste. Figuren under viser aktørenes roller til denne posten.



Figur 7: Aktørenes roller knyttet til digital post

Aktør	Beskrivelse
Innbygger	Innbygger er dataeier. Når digital post fra offentlig virksomhet er levert til innbygger, er den innbyggers eiendom.
Forvalter og tilbyder av meldingsformidlertjeneste	Forvalter og tilbyder av meldingsformidlertjenesten er databehandler av digital post til innbygger på vegne av offentlig virksomhet (postavsender).
Forvalter og tilbyder av postkassetjeneste	Forvalter og tilbyder av postkassetjenesten er databehandler av digital post til innbygger på vegne av offentlig virksomhet frem til det er bekreftet at digital post er levert til mottakers digitale postkasse. Deretter forvaltes den digitale posten på vegne av innbygger (postmottaker).
Offentlig virksomhet	Den offentlige virksomheten som sender digital post har behandlingsansvaret for posten til det er bekreftet at den er gjort tilgjengelig (mottatt) i mottakerens postkasse.

3.1.5 Oppslagstjeneste for kontaktinformasjon

Oppslagstjenesten for kontaktinformasjon er en felles tjeneste som kan benyttes av offentlige virksomheter og virksomheter som utfører tjenester på vegne av det offentlige. Oppslagstjenesten er en overbygning på de registrene som er nødvendig for forvaltningens elektroniske kommunikasjon.

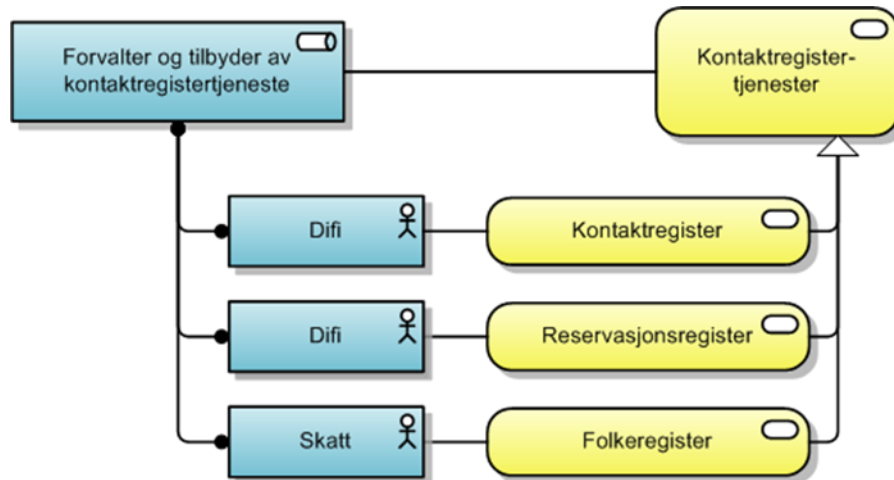
Figur 7: Aktørenes roller knyttet til digital post viser aktører og roller til forretningstjenester som tilbyr bruk og forvaltning av innbyggers kontaktinformasjon. Oppslagstjeneste for kontaktinformasjon tilbyr kontaktinformasjonsbruker (avsendervirksomhet) et sett av definerte grensesnitt til innbyggers kontaktinformasjon i forhold til innbyggers dialog med det offentlige.

Forvaltere av kontaktregistertjenester

Når det gjelder kontaktregistertjenester, eksisterer det i dag to relevante registre:

- *Digitalt kontaktregister:* Difi forvalter og tilbyr. Registeret skal videreutvikles til også å håndtere tilstrekkelig informasjon om innbyggers postkasse for at offentlige virksomheter kan sende digital post til innbyggers postkasse på en sikker måte.
- *Folkeregisteret:* Skatteetaten forvalter og drifter. Registeret inneholder innbyggers postadresse.

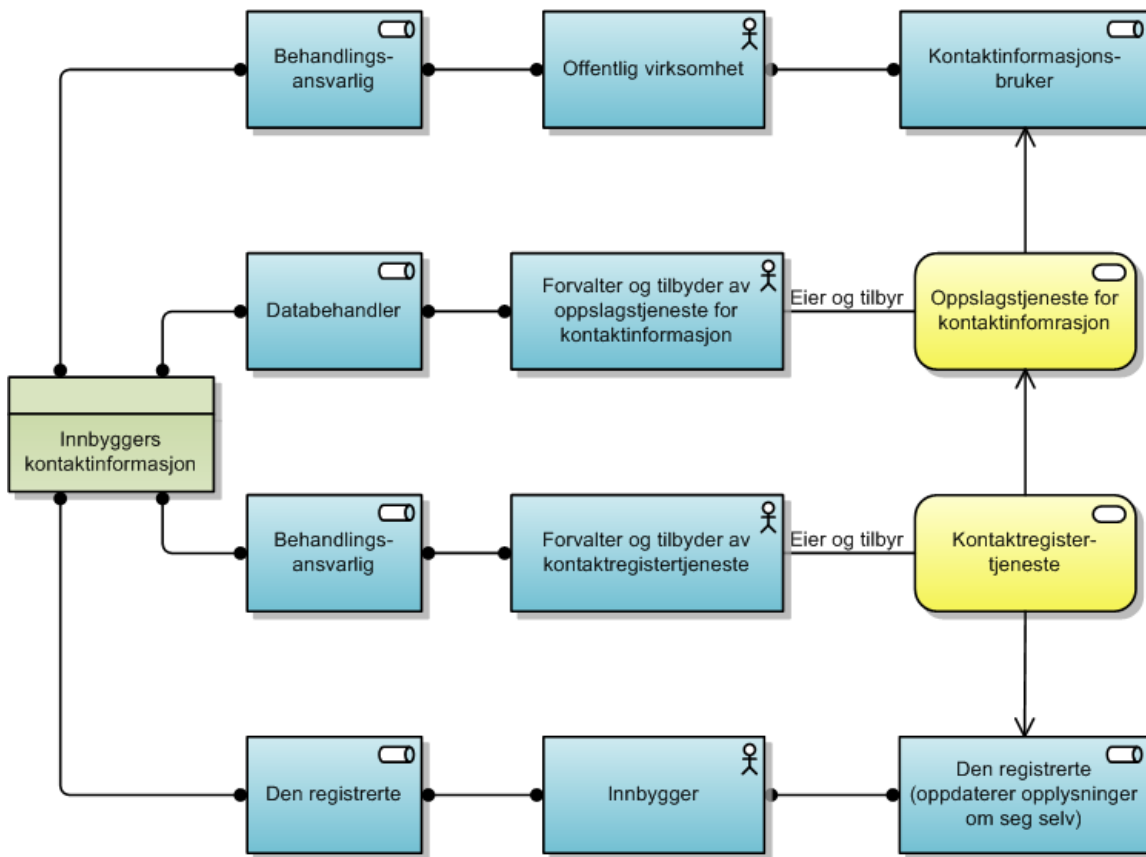
I tillegg skal det etableres et reservasjonsregister som Difi vil være forvalter og tilbyder av.



Figur 8: Forvaltere og tilbydere av kontaktregistertjenester

Aktørenes roller til innbyggers kontaktinformasjon

Innbyggers kontaktinformasjon er et sentralt forretningsobjekt som brukes for å kunne adressere digital post til innbygger. Figuren under viser en forenklet oversikt over aktørenes roller til denne informasjonen.



Figur 9: Aktørenes roller knyttet til innbyggers kontaktinformasjon

Aktør	Beskrivelse
Innbygger	<p>Innbyggeren oppdaterer som hovedregel selv opplysningene om seg i kontaktinformasjonsregisteret.</p> <p>(Hvis det blir aktuelt med automatisk oppretting av postkasser, så vil noe informasjon, slik som postkasseadresse og sertifikater registreres uten innbyggerens kontroll).</p>
Forvalter og tilbyder av oppslagstjeneste for kontaktinformasjon	<p>En offentlig virksomhet som mottar kontaktinformasjon vil være behandlingsansvarlig for sin bruk av den kontaktinformasjonen som utleveres.</p> <p>Forvalter og tilbyder av oppslagstjenesten for kontaktinformasjon er databehandler for den offentlige virksomheten som etterspør kontaktinformasjon.</p>
Forvalter og tilbyder av kontaktregistertjeneste	<p>Forvalter og tilbyder av kontaktregistertjeneste har behandlingsansvaret for innbyggers kontaktinformasjon som innbygger eier og forvalter i deres registre.</p>
Offentlige virksomhet	<p>Den offentlige virksomheten som bruker kontaktinformasjon fra oppslagstjenesten har behandlingsansvaret for sin bruk av innbyggers kontaktinformasjon.</p>

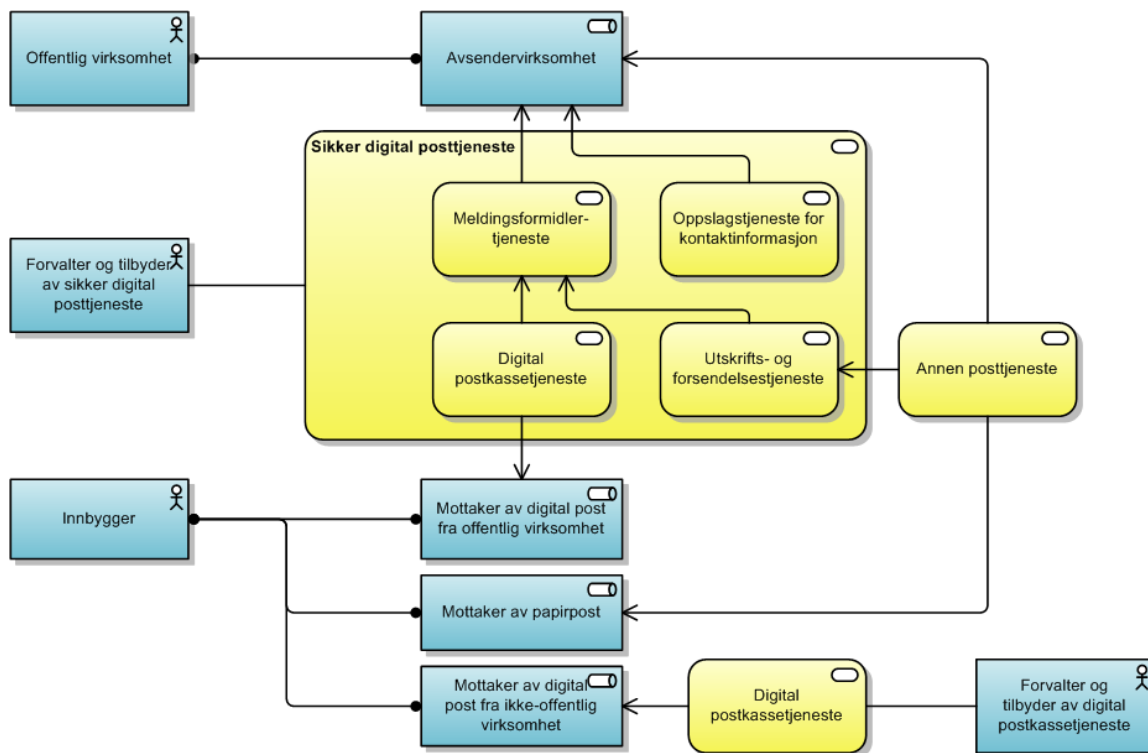
3.1.6 Aktører og roller sett i relasjon til overordnede forretningstjenester

Arkitekturen forutsetter at posttjenesten utformes slik at mottaker av digital post fra offentlige virksomheter selv skal kunne velge sin egen postkasse blant flere tilgjengelige, men at avsendervirksomhet bare har ett grensesnitt mot tjenesten som da sørger for at den digitale posten sendes til mottakerens selvvalgte postkasse (Arkitekturvisjonen). Disse forutsetningene, at mottaker skal motta digital post i sin egen postkasse og at avsendervirksomhetene skal slippe å forholde seg til de enkelte postkassetjenestene, danner grunnlaget for posttjenestens formidlertjeneste.

Overordnet modularisering av tjenester og tilhørende aktører

Figur 10 viser modulariseringen av Sikker digital posttjeneste og samspillet med øvrige tjenester i formidlingen av post til innbyggere.

I forhold til postforsendelse via Sikker digital posttjeneste bruker avsendervirksomhet meldingsformidlertjeneste til å formidle post til innbygger. Mottaker av digital post fra offentlig virksomhet bruker digital postkassetjeneste for å motta og oppbevare digital post fra det offentlige.



Figur 10: Aktører og roller mht. postformidling generelt

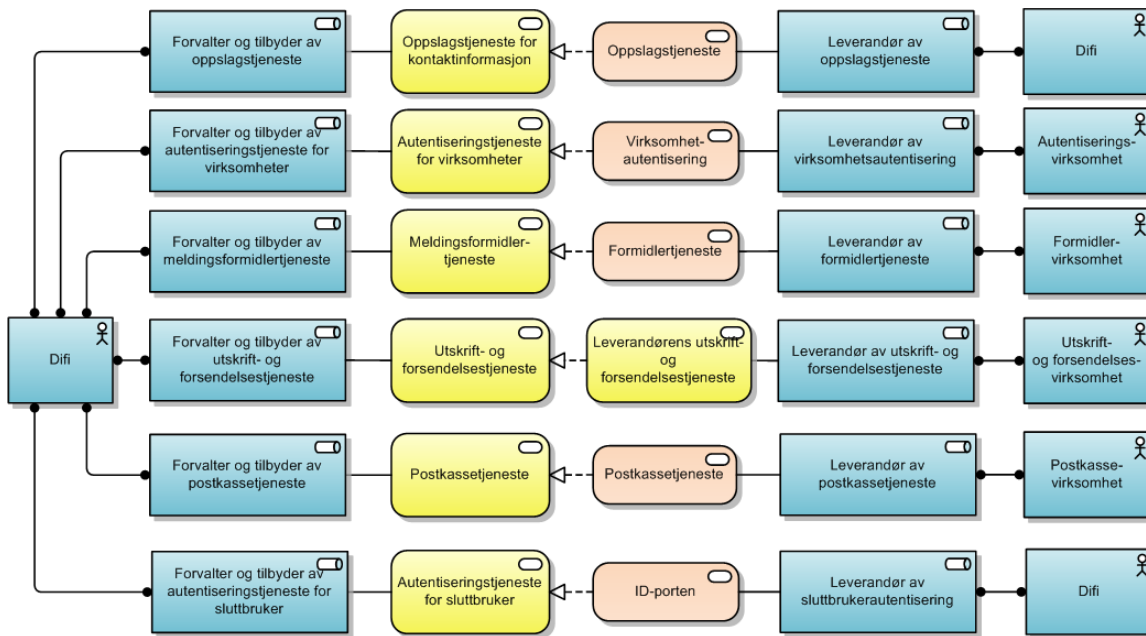
Sikker digital posttjeneste og avsendervirksomhet kan bruke *annen posttjeneste* for å sende papirpost til innbygger, og innbygger kan bruke en digital postkassetjeneste for mottak av digital post fra ikke-offentlige virksomheter. Innbygger kan bruke samme digitale postkasse for både offentlig og ikke-offentlig post.

3.1.7 Difi som sentralforvalter og tilbyder av Sikker digital posttjeneste

Forretningstjenestene i Sikker digital posttjeneste skal realiseres av leverandørens forretningstjenester og eller applikasjonstjenester. Arkitekturen legger opp til at avsendervirksomhetene i Sikker digital posttjeneste har et avtaleforhold med sentralforvalter.

Difi vil være forvalter og tilbyder av forretningstjenestene som brukes av offentlig virksomhet og innbygger. I tillegg vil Difi være leverandør av applikasjonstjenesten oppslagstjeneste og Difi er allerede leverandør av innbyggerautentisering, ID-porten.

Figur 11 viser hva som skal anskaffes og utvikles av hvilke leverandører for å realisere Sikker digital posttjeneste.



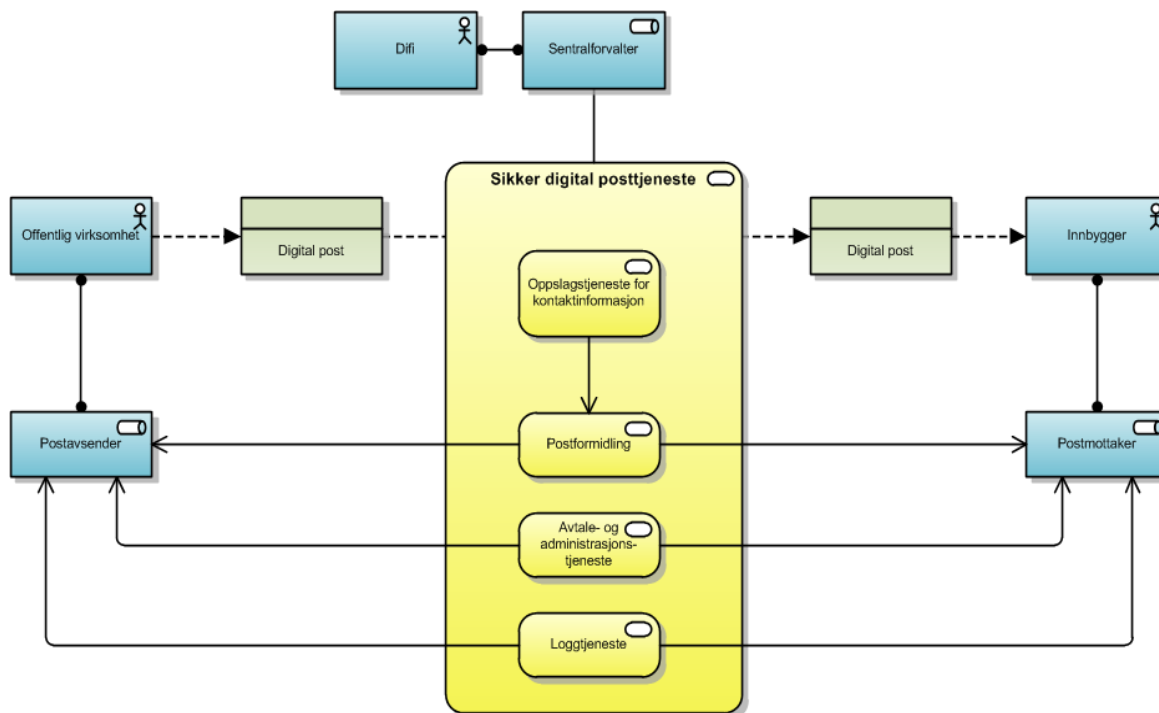
Figur 11: Virksomheter som forvaltere og leverandører

3.2 Tjenestemodell

3.2.1 Overordnet tjenestemodell

Modellen under viser hvilke overordnede tjenester en sikker digital postløsning vil bestå av. I den overordnede tjenestemodellen er Sikker digital posttjeneste delt opp i tjenester for kontaktinformasjon og postformidling, avtale- og administrasjonstjeneste og loggtjeneste.

- Oppslagstjeneste for kontaktinformasjon vil ivareta behovet for tilgang til postmottakers oppdaterte kontaktinformasjon og krypteringsmekanisme
- Postformidlingstjenesten består av ekspedering hos avsender, formidlingstjeneste og postkassetjenestene som benyttes av mottaker. Formidlingstjenesten er et felles integrasjonspunkt for posthåndtering.
- Avtale- og administrasjonstjeneste består av alle administrative funksjoner som registrering av aktører, brukerstøtte, feilhåndtering, støtte til integrasjon og test mv. Dette er funksjoner som tilrettelegges og styres sentralt.
- Loggtjeneste vil ivareta behovet for sporing og statistikk og være grunnlaget for bl.a. fakturering.



Figur 12: Overordnet tjenestemodell

Figuren over viser de sentrale rollene offentlig virksomhet, innbygger og Difi har til Sikker digital posttjeneste:

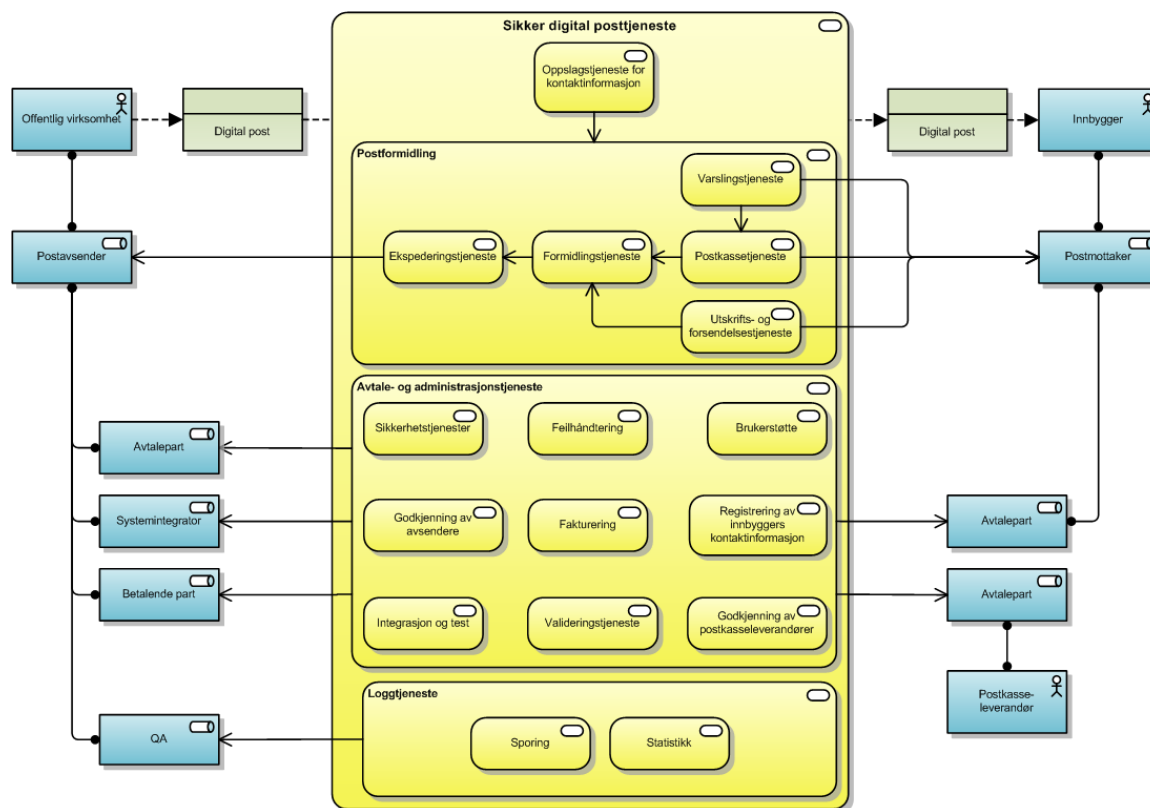
- Difi i rollen som sentralforvalter tilbyr tjenesten Sikker digital posttjeneste
- Offentlig virksomhet i rollen som postavsender bruker tjenestene:
 - postformidling for å distribuere post til postmottaker
 - avtale- og administrasjonstjeneste for å kunne ta Sikker digital posttjeneste i bruk
 - loggtjeneste for å dokumentere og kontrollere postforsendelser
- Innbygger i rollen som postmottaker bruker tjenestene:
 - postformidling for å motta, lese og administrere mottatt post
 - avtale- og administrasjonstjeneste for å kunne ta Sikker digital posttjeneste i bruk
 - loggtjeneste for å kontrollere postforsendelser

3.2.2 Detaljert tjenestemodell

Figuren under viser en detaljering av forretningstjenestene som Sikker digital posttjeneste består av og de sentrale rollene offentlig virksomhet, innbygger og postkasseleverandør har til tjenesten:

- Offentlig virksomhet i rollen som postavsender bruker ekspederings-tjenesten for å sende utgående post til innbyggere
- Innbygger i rollen som postmottaker bruker postkassetjenesten for å lese, oppbevare og administrere digital post

- Offentlig virksomhet (postavsender), innbygger (postmottaker) og postkasseleverandør i rollen som avtalepart bruker avtale- og administrasjonstjenesten til å forplikte seg til kravene for bruk av Sikker digital posttjenesten og for å ivareta sine rettigheter som bruker av posttjenesten
- Offentlig virksomhet (postavsender) i rollen som systemintegrator bruker avtale- og administrasjonstjenesten for å tilpasse egne systemer og sikre teknisk og semantisk samvirkeevne med posttjenesten
- Offentlig virksomhet (postavsender) i rollen som betalende part bruker fakturerings-tjenesten for å motta og kontrollere inngående faktura (fra sentralforvalter) for bruk av posttjenesten
- Offentlig virksomhet (postavsender) i rollen som QA bruker loggtjenesten for å kontrollere sine postforsendelser



Figur 13: Detaljert tjenestemodell

3.2.3 Oppslagstjeneste for kontaktinformasjon

Oppslagstjenesten for kontaktinformasjon er en felles tjeneste som kan benyttes av offentlige virksomheter og virksomheter som utfører tjenester på vegne av det offentlige. Oppslagstjenesten er en overbygning på de registrene som er nødvendig for forvaltningens elektroniske kommunikasjon. I første omgang er dette informasjon om reservasjon og digital kontaktinformasjon. På sikt kan oppslagstjenesten gi tilgang til andre registre, som for eksempel folkeregisteret. Reservasjonsstatus inneholder informasjon om innbyggeren har reservert seg mot

digital kommunikasjon fra det offentlige. Kontaktinformasjon er blant annet foretrukket e-postadresse, mobilnummer, digital postkasse og sertifikatinformasjon.

Registrering og oppdatering av informasjonen vil ligge til de ulike registrene og vil ikke være en del av oppslagstjenesten.

Det vil tilbys grensesnitt med enkel funksjonalitet for å hente informasjon om enkeltindivider og grensesnitt med mer kompleks funksjonalitet for å hente ut informasjon om større grupper. Eksempler på funksjonalitet kan være at en virksomhet sender over et fødselsnummer og får tilbake beskjed om vedkommende er reservert eller ikke. En mer kompleks funksjonalitet er å sende over en liste med fødselsnummer og få tilbake kontaktinformasjon på alle som ikke er reservert.

Kontaktregistertjenester tilbyr innbygger å oppdatere og verifisere sin egen kontaktinformasjon.

3.2.4 Postformidling

Postformidling består av de forretningstjenestene i Sikker digital posttjeneste som operativt håndterer postgangen fra postavsender til postmottaker.

Forretningstjeneste	Beskrivelse	Brukere av tjenesten
Ekspederingstjeneste	<p>En tjeneste som tilbyr ekspedering av utgående post for postavsender. Denne etableres av avsendervirksomhetene, og innebærer å adressere, sikre og tilpasse utgående post iht. posttjenestens krav. Dette kan inkludere tilpasning av postens innhold til valgt kanal (papirpost versus digital post)</p> <p>Ekspederingstjenesten bruker:</p> <ul style="list-style-type: none">• oppslagstjenesten for kontaktinformasjon for å håndtere adressering til riktig postmottaker (inkl. postmottakers kanalvalg)• oppslagstjenesten for kontaktinformasjon og de sentrale sikkerhetstjenestene for å håndtere sikring av digital post mht.:<ul style="list-style-type: none">○ Tilgjengelighet (hvordan sikre at posten er tilgjengelig for postmottaker innenfor de tilgjengelighetskrav som er satt for Sikker digital posttjeneste)○ Konfidensialitet (hvordan sikre at posten bare er tilgjengelig for de som skal ha tilgang)○ Integritet (hvordan sikre at posten ivaretar sin korrekthet, gyldighet og fullstendighet fra postavsender og helt frem til postmottaker)	Postavsender

Forretningstjeneste	Beskrivelse	Brukere av tjenesten
	<ul style="list-style-type: none"> den sentrale valideringstjenesten for å tilpasse den digitale postforsendelsens innhold og formater til posttjenestens krav den sentrale formidlingstjenesten til å distribuere utgående post til postmottakers valgte postkasse 	
Formidlingstjeneste	<p>En tjeneste som tilbyr formidling av utgående post fra postavsender og ekspederingstjenesten til postmottakernes postkasser. Tjenesten fungerer som ett felles integrasjonspunkt som tar i mot og viderefremidler post til rett postkassetjeneste eller en utskrifts- og forsendelsestjeneste. Tjenesten håndterer også batchsending av utgående post fra avsender usortert med hensyn på postkassetjeneste eller en utskrifts- og forsendelsestjeneste.</p> <p>Formidlertjenesten bruker:</p> <ul style="list-style-type: none"> loggtjenesten til å dokumentere postforsendelsen som grunnlag for fakturering, statistikk, sporbarhet og feilsøking sikkerhetstjenestene for å autentisere og autorisere avsendervirksomhetene valideringstjenesten for å validere den digitale posten sikkerhetstjenestene for å autentisere og autorisere postkassetjeneste postkassetjeneste til å distribuere digital post til postmottakers valgte postkasse den sentrale utskrifts- og forsendelsestjeneste til å distribuere papirpost til postmottaker 	<p>Ekspederingstjenesten</p> <p>Sentralforvalter</p>
Postkassetjeneste	<p>En tjeneste som tilbyr oppbevaring og tilgjengeliggjøring av digital post for postmottakere. På konseptuelt nivå består postkassetjenesten av en postarkivtjeneste for å oppbevare postmottakers post og en lese- og administrasjonstjeneste som postmottaker bruker for å få tilgang til og administrere sin post.</p> <p>Postkassetjenesten bruker:</p> <ul style="list-style-type: none"> valideringstjenesten for å validere mottatt digitale post loggtjenesten til å dokumentere brukerinteraksjon for statistiske formål sikkerhetstjenestene for å autentisere postmottaker 	<p>Formidlertjenesten</p> <p>Postmottaker</p>

Forretningstjeneste	Beskrivelse	Brukere av tjenesten
	<ul style="list-style-type: none"> varslingstjenesten for å varsle postmottaker om mottatt digital post 	
Utskrifts- og forsendelsestjeneste	<p>En tjeneste som tilbyr en papirposttjeneste ved å skrive ut posten på papir, konvoluttere og sende papirpost til postmottaker. Tjenesten bidrar til at Sikker digital posttjeneste fungerer som en totalleverandør for avsendervirksomhetene vedrørende post til innbyggere.</p> <p>Utskrifts- og forsendelsestjeneste bruker:</p> <ul style="list-style-type: none"> valideringstjenesten for å validere mottatt post sikkerhetstjenestene for å håndtere sikring av papirpost loggtjenesten til å dokumentere postforsendelsen som grunnlag for statistikk, sporbarhet og feilsøking 	<p>Formidlertjenesten (Postavsender)</p> <p>Postmottaker</p> <p>Sentralforvalter</p>
Varslingstjeneste	En tjeneste som tilbyr varsling til postmottaker om mottatt digital post.	<p>Postkassetjenesten</p> <p>Postmottaker</p>

3.2.5 Avtale- og administrasjonstjeneste

Avtale- og administrasjonstjenestene består av de forretningstjenestene i Sikker digital posttjeneste som håndterer det avtalemessige og forvaltningsmessige ved å ta i bruk og bruke tjenesten.

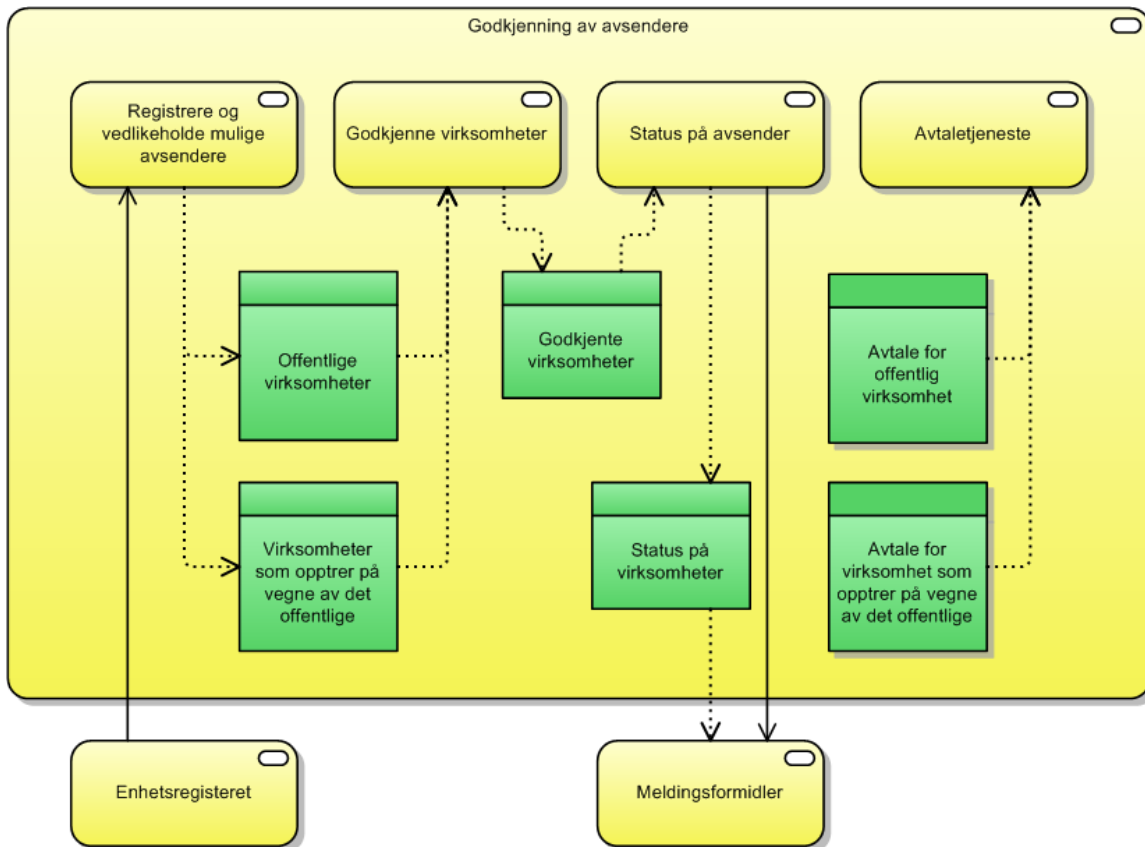
Forretningstjeneste	Beskrivelse	Brukere av tjenesten
Sikkerhetstjenester	<p>Tjenester som tilbyr og stiller krav til sikring av digital post mht. tilgjengelighet, konfidensialitet og integritet. Tjenestene inneholder sikkerhetspolicy, sikkerhetsregler og sikkerhetsmekanismer for Sikker digital posttjeneste som de samhandlende aktørene (avtalepartene) skal følge.</p> <p>Sikkerhetstjenestene er ytterligere beskrevet i sikkerhetsarkitekturen.</p>	<p>Ekspederingstjenesten</p> <p>Formidlertjenesten</p> <p>Postkassetjenesten</p> <p>Utskrifts- og forsendelsestjenesten</p> <p>Oppslagstjenesten</p> <p>Sentralforvalter</p>

Forretningstjeneste	Beskrivelse	Brukere av tjenesten
Valideringstjeneste	<p>En tjeneste som tilbyr validering av postforsendelsen. Tjenesten sikrer semantisk og teknisk samvirkeevne (interoperabilitet) mellom de samhandlende aktørene (avtalepartene).</p> <p>Ekspederingstjenesten bruker valideringstjenesten for å produsere postforsendelsen iht. formatkrav og for å identifisere gyldige grensesnitt.</p>	<p>Sentralforvalter</p> <p>Ekspederingstjenesten</p> <p>Formidlertjenesten</p> <p>Postkassetjenesten</p> <p>Utskrifts- og forsendelsestjenesten</p>
Godkjenning av avsendere	<p>En tjeneste som tilbyr registrering og forvaltning av de til en hver tid godkjente postavsenderne. Tjenesten godkjenner og registrerer offentlige virksomheter som postavsendere.</p> <p>Formidlertjenesten bruker oversikten over godkjente offentlig virksomheter i autorisering av postavsendere i postformidlingen.</p>	<p>Postavsender</p> <p>Sentralforvalter</p> <p>Formidlertjenesten</p>
Godkjenning av postkasseleverandører	<p>En tjeneste som tilbyr registrering og forvaltning av de til en hver tid godkjente postkasseleverandørene. Tjenesten godkjenner og registrerer postkasseleverandører.</p> <p>Formidlertjenesten bruker oversikten over godkjente postkasseleverandører i å autorisere postkassetjenester i postformidlingen.</p>	<p>Postkasseleverandør</p> <p>Sentralforvalter</p> <p>Formidlertjenesten</p>
Registrering av innbyggers kontaktinformasjon	<p>En tjeneste som tilbyr registrering og oppdatering av innbyggernes digitale kontaktinformasjon, herunder:</p> <ul style="list-style-type: none"> • innbyggernes digitale postkasseadresse • innbyggernes varslingsadresser • innbyggernes sertifikatinformasjon <p>Innbygger har selv ansvaret for at egen kontaktinformasjon er korrekt.</p>	<p>Innbygger</p> <p>Oppslagstjenesten</p> <p>Kontakt- og reservasjonsregistre</p>
Fakturering	<p>En tjeneste som brukes i fakturering av postavsendere for bruk av Sikker digital posttjeneste. Faktureringsreglene er nedfelt i avtaler/bruksvilkår mellom postavsenderne og sentralforvalter og sentralforvalter og postkasseleverandørene.</p> <p>Fakturering bruker tjenestene sporing og statistikk for å</p>	<p>Postkasseleverandør</p> <p>Sentralforvalter</p> <p>Postavsender</p>

Forretningstjeneste	Beskrivelse	Brukere av tjenesten
	beregne og fordele kostnader mellom sentralforvalter og postavsenderne	
Feilhåndtering	<p>En tjeneste som tilbyr identifisering og retting av feil. Tjenesten definerer feiltyper, feilkonsekvenser og ansvar, samt regler for og krav til feilhåndtering som er nedfelt i avtaler mellom postavsenderne og sentralforvalter og sentralforvalter og postkasseleverandørene.</p> <p>Forretningstjenesten Feilhåndtering skal fungere på tvers av brukerne av tjenesten.</p> <p>Feilhåndtering bruker tjenesten sporing.</p>	Postkasseleverandør Sentralforvalter Postavsender
Brukerstøtte	<p>En tjeneste som tilbyr brukerstøtte til aktørene (postmottaker og postavsender). Tjenesten er distribuert slik at postkasseleverandøren tilbyr en brukerstøttetjeneste til sine brukere (postmottakere), mens sentralforvalter tilbyr brukerstøttetjenester til postavsenderne.</p>	Postavsender Sentralforvalter Postmottaker
Integrasjon og test	<p>En tjeneste som tilbyr integrasjons- og testtjenester. Tjenesten definerer integrasjons- og testprosedyrer og regler som de samhandlende avtalepartene offentlig virksomhet, postkasseleverandør og sentralforvalter skal følge.</p>	Postavsender Sentralforvalter Postkasseleverandør

Godkjenning av avsendere

Tjenesten understøtter forvaltning av hvilke virksomheter som er godkjent for å bruke Sikker digital posttjeneste.



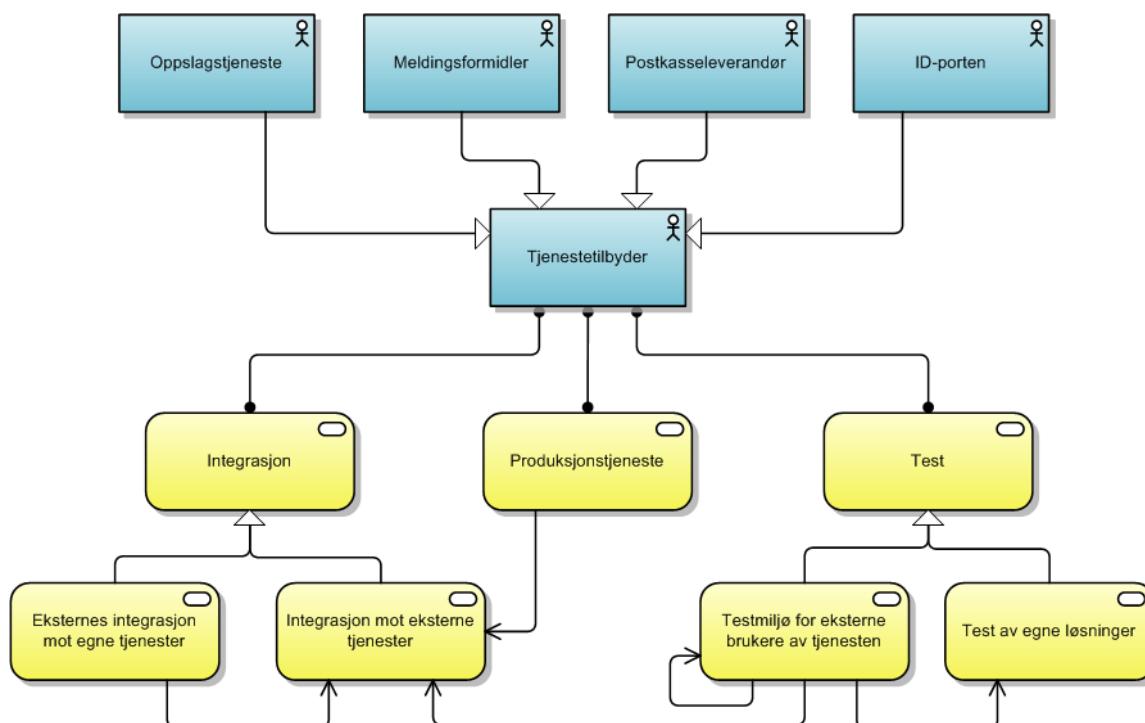
Figur 14: Godkjenning av avsendere

Tjeneste	Beskrivelse
Registrere og vedlikeholde mulige avsendere	En tjeneste som ved hjelp av enhetsregisteret vedlikeholder en liste over alle offentlige virksomheter. I tillegg tilbyr tjenesten at offentlige virksomheter registrerer virksomheter som opptrer på deres vegne. I oppstartsfasen kan tjenesten realiseres med manuelle prosesser, men på sikt bør tjenesten være helautomatisk for sentralforvalteren.
Godkjenne virksomheter	En godkjent virksomhet har lov til å benytte Sikker digital posttjeneste for å sende post. Kriterier for å bli godkjent er ikke definert, men på sikt bør de være helautomatiske for sentralforvalteren. For eksempel ved at Sikker digital posttjeneste registrerer at virksomheten har fullført et test og integrasjonsløp, og at virksomheten leverer en maskinlesbar bekreftelse på at avtalen/bruksvilkårene er lest og forstått.
Status på avsender	Leverer status på de virksomheter som er godkjent for å benytte Sikker digital posttjeneste. Tjenesten benyttes av meldingsformidleren, slik at den kan sjekke om en avsender er godkjent før posten videresendes.

	Postkasseleverandørene benytter også tjenesten, enten direkte, eller indirekte ved at meldingsformidleren bekrefter at posten som sendes kommer fra en godkjent virksomhet.
Avtaletjeneste	Inneholder avtalene for virksomhetene som benytter Sikker digital posttjeneste til å sende digital post. Avtalene/bruksvilkårene legges lett tilgjengelig, for eksempel på Difi sine hjemmesider. Avsendervirksomhetene godkjenner avtalene/bruksvilkårene, for eksempel ved å ta Sikker digital posttjeneste i bruk.

Integrasjon og test

Alle tjenestetilbydere i Sikker digital posttjeneste har et produksjonsmiljø hvor produksjonstjenestene kjører. Aktørene har behov for å teste både produksjonstjenestene og egne systemer som benytter tjenesten. I tillegg er det behov for å teste en kjede av tjenester levert av forskjellige aktører.



Figur 15: Integrasjon og test

Mot testmiljøet må alle aktørene kunne fremstå som avsendervirksomheter på den ene siden, og som innbyggere på den andre siden, slik at de kan fremprovosere de nødvendige meldinger og kvitteringer for å teste sine systemer.

Tjeneste	Beskrivelse
Integrasjon	Integrasjon er det arbeidet som utføres når to systemer skal kobles sammen, altså at en produksjonstjeneste hos en aktør skal benyttes av en annen aktør. Integrasjon deles inn i det arbeidet som utføres hos tjenestetilbyderen og det arbeidet som utføres hos den som skal benytte tjenesten.
Produksjonstjeneste	Tjeneste som kjører i et produksjonsmiljø og tilbys til andre aktører.
Test	Test deles inn i tjenesten som tilbys til andre aktører, slik at de kan utføre tester, og test av egne systemer. Testformål kan være integrasjonstest, ytelsestest, sikkerhetstest og funksjonstest ved endringer, etc. All testing skal gjennomføres med anonymiserte data. Testmiljø bør være så likt produksjon som mulig og forskjeller må være dokumentert. Forskjellen mellom Test og Produksjon kan være både kvalitetsforskjeller (eks: kapasitet, redundans) og funksjonalitet.
Eksternes integrasjon mot egne tjenester	Når en ekstern part skal integrere mot tjenestene som aktøren tilbyr vil det være behov for noe støtte, og kanskje noe teknisk arbeid. For eksempel vil integrasjonsveiledning, grensesnittspesifikasjoner, testscript, testdata og lignende være en del av det som tilbys. Det er svært nyttig å tilby referanseimplementasjon og støtteverktøy for gjennomføring av testing (f.eks. for å understøtter ytelsestesting). Tekniske arbeid kan være nødvendig, for eksempel ved oppretting av brukere, data og lignende.
Integrasjon mot eksterne tjenester	Ved integrasjon mot tjenester som tilbys av en annen aktør vil det være nødvendig å kjøre et testløp for å se at egne løsninger virker som forventet med tjenesten som tilbys. Etter at alle tjenesten er satt i produksjon kan det være nødvendig å ta noen siste tester i produksjon (e.g. sende post til seg selv gjennom Sikker digital posttjeneste).
Testmiljø for eksterne brukere av tjenesten	En virksomhet som tilbyr en tjeneste i produksjon må også tilby den samme tjenesten i et eller fler testmiljø, slik at andre aktører kan teste sine systemer før de tar i bruk tjenesten i produksjon. Testmiljøet hos en tjenestetilbyder vil bli brukt av testmiljøer hos andre tjenestetilbydere, slik at tester kan gjennomføres gjennom hele verdikjeden. Det er sentralt at testmiljøene dermed har overlappende testdata for å kunne understøtte funksjonelle og ikke-funksjonelle ende-til-ende tester.

Test av egne løsninger	En virksomhet som tilbyr, eller skal tilby, en tjeneste i produksjon vil ha behov for å teste at virksomhetens egen løsning fungerer som forventet, og i henhold til spesifisering. De interne testene bør være dokumentert, både i form av testscript og resultat. Test av egen løsning bør i størst mulig grad være automatisert.
------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.2.6 Loggtjeneste

Loggtjeneste vil ivareta behovet for sporing og statistikk og være grunnlaget for blant annet fakturering. Loggtjenesten vil brukes av postformidlingstjenesten og avtale- og administrasjonstjenesten.

Forretningstjeneste	Beskrivelse	Brukere av tjenesten
Sporing	En tjeneste som tilbyr sporing av postforsendelser. Tjenesten definerer hvordan postforsendelsen skal dokumenteres av de samhandlende avtalepartene offentlig virksomhet, sentralforvalter og postkasseleverandør. Forretningstjenesten Sporing skal fungere på tvers av brukerne av tjenesten.	Postkassetjenesten Formidlertjenesten Feilhåndtering Fakturering Postavsender Postmottaker Sentralforvalter
Statistikk	En tjeneste som tilbyr statistikk knyttet til bruk og forvaltning av Sikker digital posttjeneste.	Sentralforvalter Fakturering (Postavsender)

3.2.7 Distribusjon av postformidlingstjenesten

Ansvar for postformidlingstjenesten distribueres mellom offentlig virksomhet, sentralforvalter og postkasseleverandør. Hensikten i denne modellen er å synliggjøre de tjenestene som sentralforvalter, offentlig virksomhet og postkasseleverandører må etablere.

Figuren under viser at offentlig virksomhet etablerer og tilbyr ekspederingstjeneste til sine postavsendere. Denne tjenesten bruker:

- oppslagstjeneste for kontaktinformasjon
- sikkerhetstjenester
- valideringstjeneste

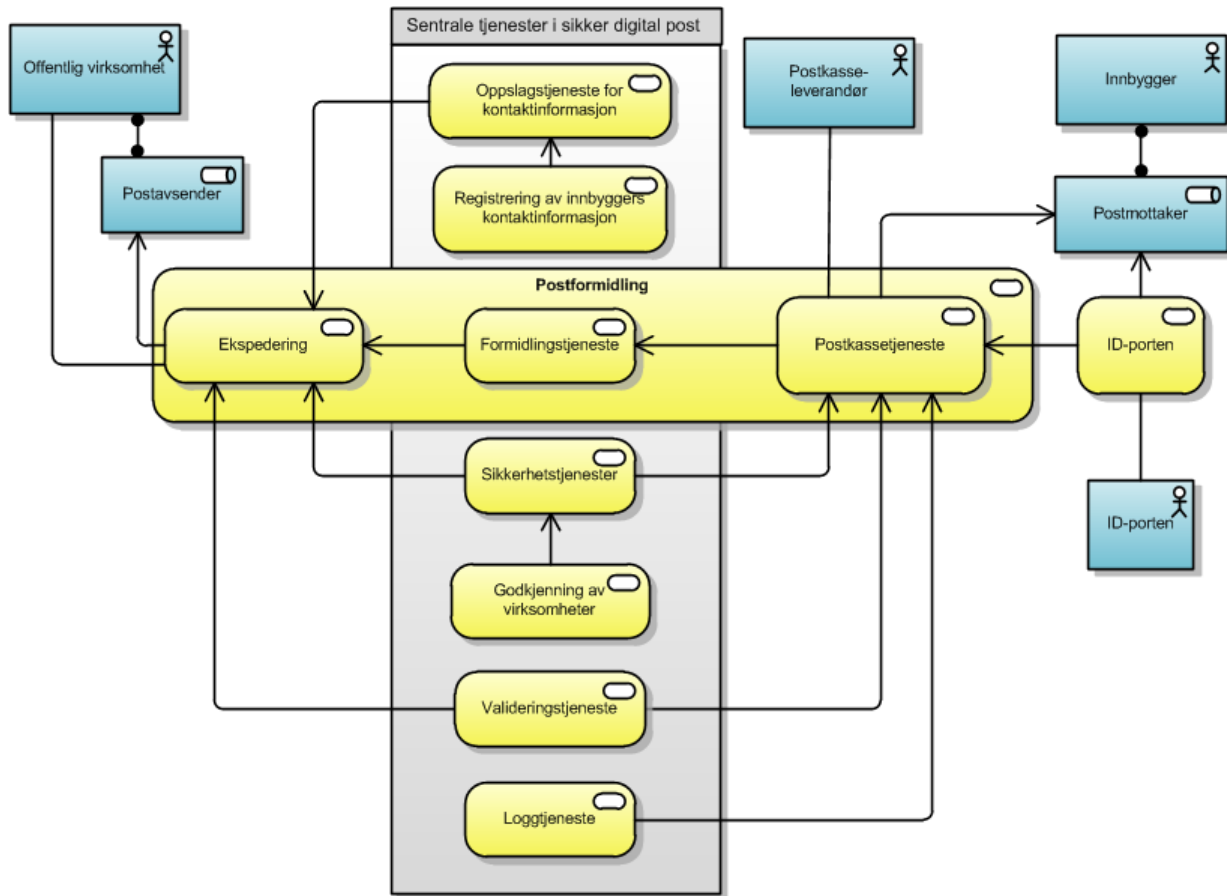
- formidlertjeneste

Postkasseleverandør etablerer og tilbyr postkassetjeneste. Denne tjenesten bruker:

- sikkerhetstjenester, bl.a. ID-porten
- valideringstjeneste
- loggtjeneste

Sentralforvalter etablerer og tilbyr formidlertjeneste. Formidlertjenesten bruker tjenestene:

- sikkerhetstjenester
- valideringstjeneste
- loggtjeneste
- postkassetjenestene



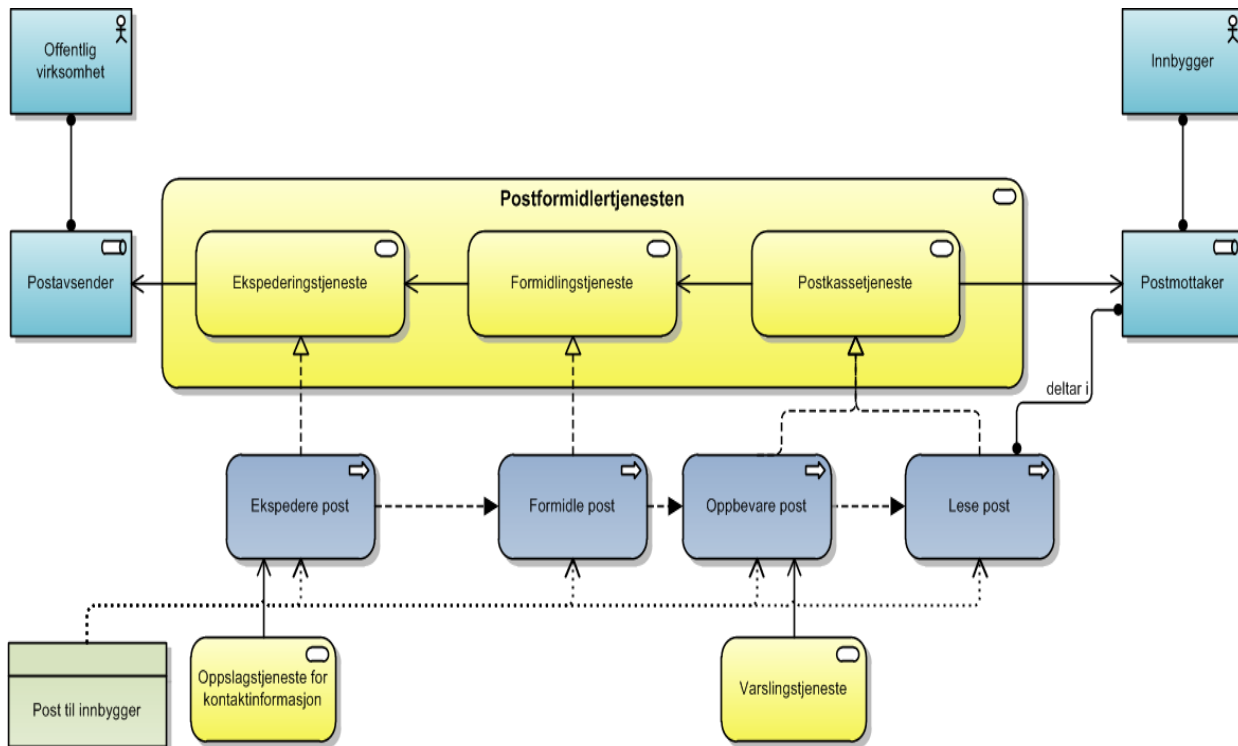
Figur 16: Distribusjon av postformidlingstjenesten

3.3 Virksomhetsprosesser

Avsnittet beskriver virksomhetsprosessene som realiserer tjenestene som er beskrevet over. Prosessene er beskrevet på et konseptuelt og logisk nivå.

3.3.1 De overordnede prosessene som realiserer den digitale postformidlingstjenesten i Sikker digital posttjeneste

Prosessmodellen under beskriver de overordnede forretningsprosessene som realiserer postformidlingstjenesten (ekspederingstjenesten, formidlingstjenesten og postkassetjenesten).



Figur 17: Overordnet prosessmodell

Ekspederingstjenesten realiseres av forretningsprosessen Ekspedere post. Prosessen starter ved at offentlige virksomhetenes informasjonssystemer oppretter post til innbygger. Ekspederingstjenesten hos offentlig virksomheten mottar utgående post og behandler den i prosessen Ekspedere post. Prosessen vil blant annet bruke Oppslagstjenesten for kontaktinformasjon.

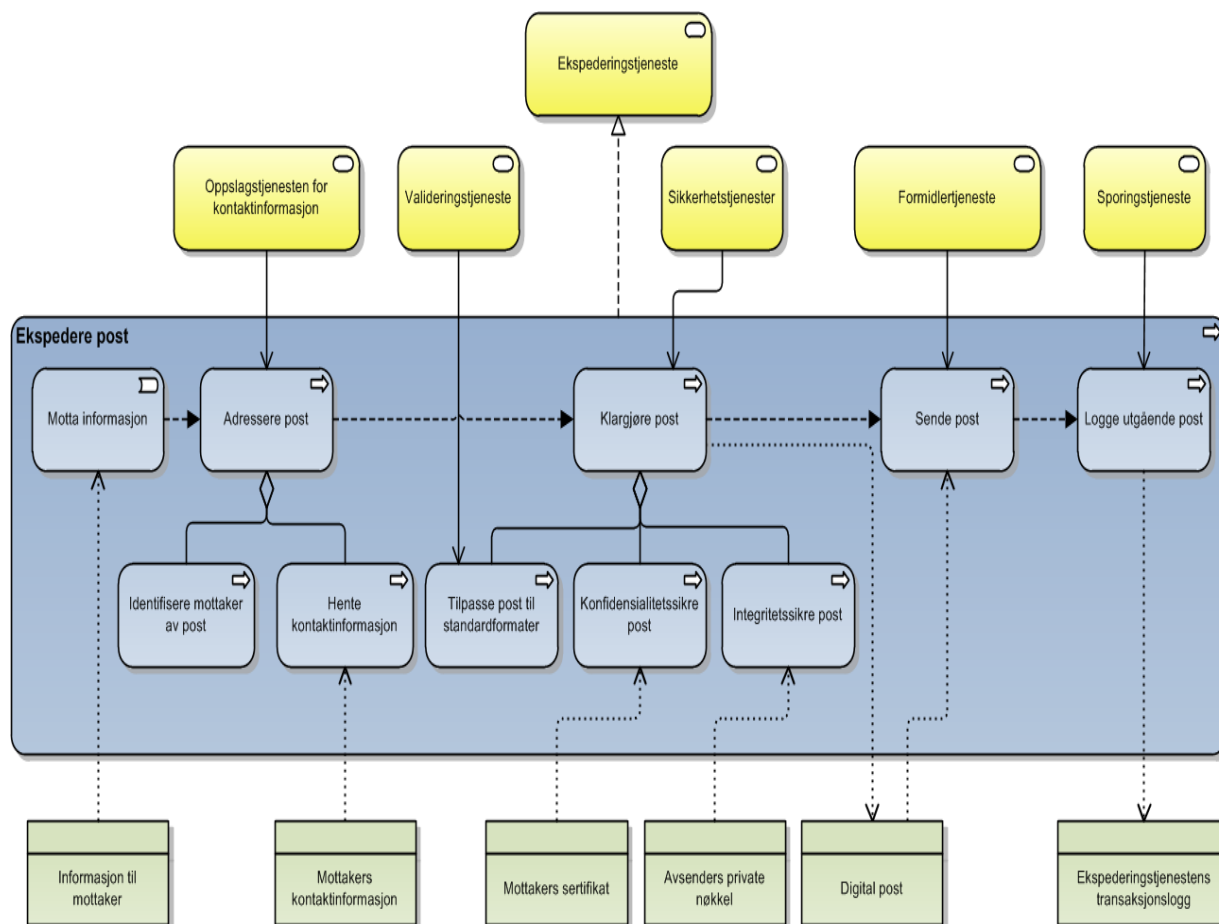
Formidlingstjenesten realiseres av forretningsprosessen Formidle post. Prosessen mottar, behandler og videresender post til Postkassetjenesten.

Postkassetjenesten realiseres av forretningsprosessene Oppbevare post og Lese post. Prosessen Oppbevare post vil blant annet bruke Varslingstjenesten til å varsle innbygger om mottatt post. Prosessen Lese post gir postmottaker mulighet til å lese og administrere sin post.

3.3.2 Detaljering av forretningsprosessen Ekspedere post

Ekspedere post består av følgende steg:

1. Motta informasjonen som skal distribueres til mottaker som post. Denne informasjonen produseres i f.eks. fag-, sak- eller arkivsystem
2. Adressere post identifiserer mottaker og henter mottakers kontaktinformasjon ved bruk av Oppslagstjenesten. Kontaktinformasjon legges til forsendelsen og består av mottakers:
 - Reservasjonsstatus
 - Postkasseadresse
 - Varslingsadresse
 - sertifikatinformasjon (enten postkasseleverandørens eller postmottakerens sertifikat)
 - postadresse (når mottaker har reservert seg eller ikke har en digital postkasse)
3. Klargjøre post resulterer i en klargjort digital post til mottaker. Prosessen:
 - tilpasser postforsendelsen til Sikker digital posttjenestens standardformater angitt av Valideringstjenesten
 - sikrer postforsendelsen mot uautorisert innsyn ved å kryptere posten med sertifikatinformasjon fra Oppslagstjenesten. Reglene for konfidensialitetssikring av postforsendelsen er beskrevet i Sikkerhetstjenestene
 - signerer postforsendelsen med Avsenders private nøkkel. Dette er også beskrevet i Sikkerhetstjenestene
4. Sende post sender posten videre til Formidlertjenesten
5. Prosessen Ekspedere post avsluttes ved at utgående post loggføres i Ekspederingstjenestens transaksjonslogg. Posttjenestens krav til denne loggen er beskrevet i Sporingstjenesten



Figur 18: Ekspedere post

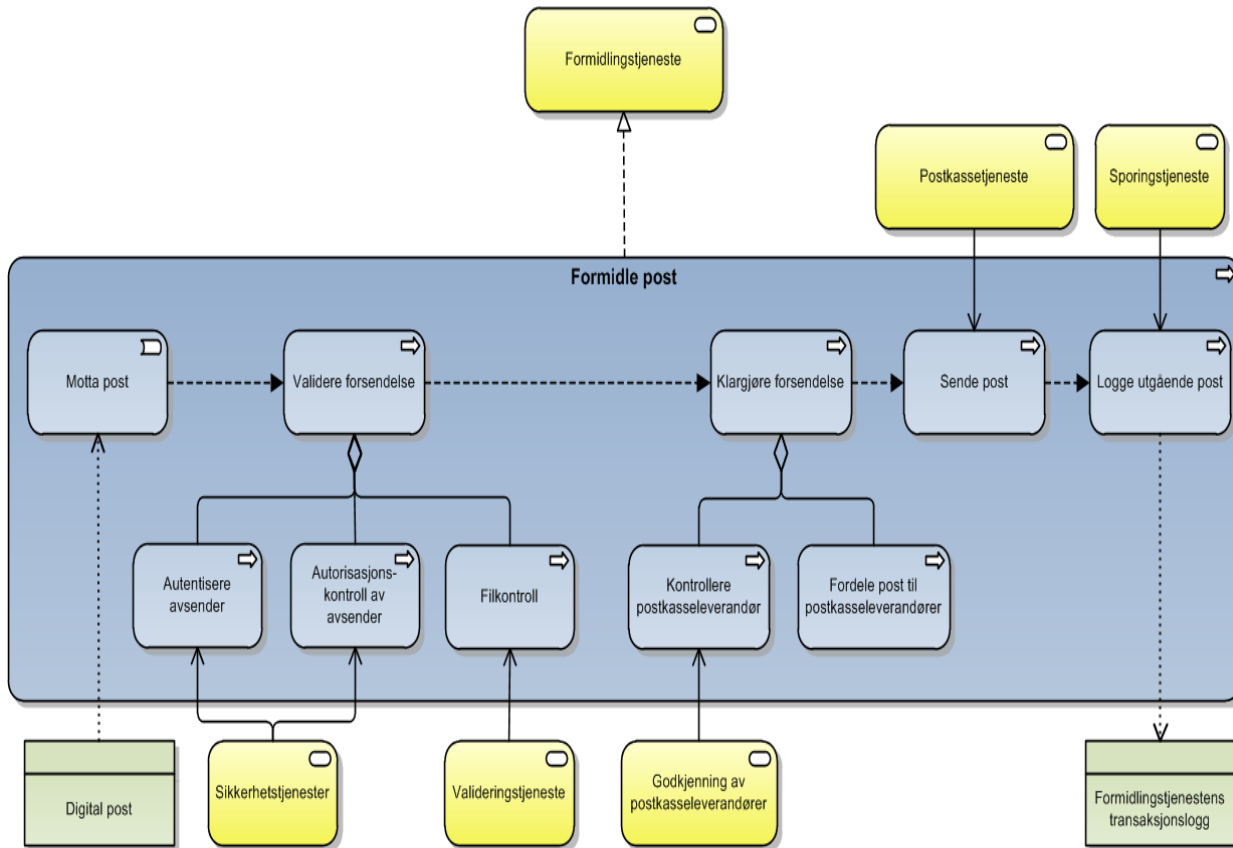
3.3.3 Detaljering av forretningsprosessen Formidle post

Formidle post består av følgende steg:

1. Motta digital post fra postavsender.
2. Validere forsendelsen ved å:
 - autentisere postavsender med bruk av Sikkerhetstjenestene og tredjepartsløsninger for autentisering av virksomheter.
 - kontroll av postavsenders autorisasjon med bruk av Sikkerhetstjenestene som blant annet består av en oversikt over godkjente avsendere.
 - kontrollere postforsendelsen i henhold til definerte formatstandarder fra Valideringstjenesten.
3. Klargjøre forsendelsen ved å kontrollere om postkasseleverandører er godkjent.
 - sortere og prioritere posten til riktig Postkassetjeneste.
4. Sende utgående post kan enten skje ved at Postkassetjenesten spør etter post eller at Formidlertjenesten sender uoppfordret til riktig Postkassetjeneste.

5. Prosessen avsluttes ved at behandlingen loggføres i Formidlingstjenestens transaksjonslogg.

Stegene beskriver normalsituasjonen. Feilsituasjoner skal også logges og kvittering sendes til avsendervirksomheten via meldingsformidleren.



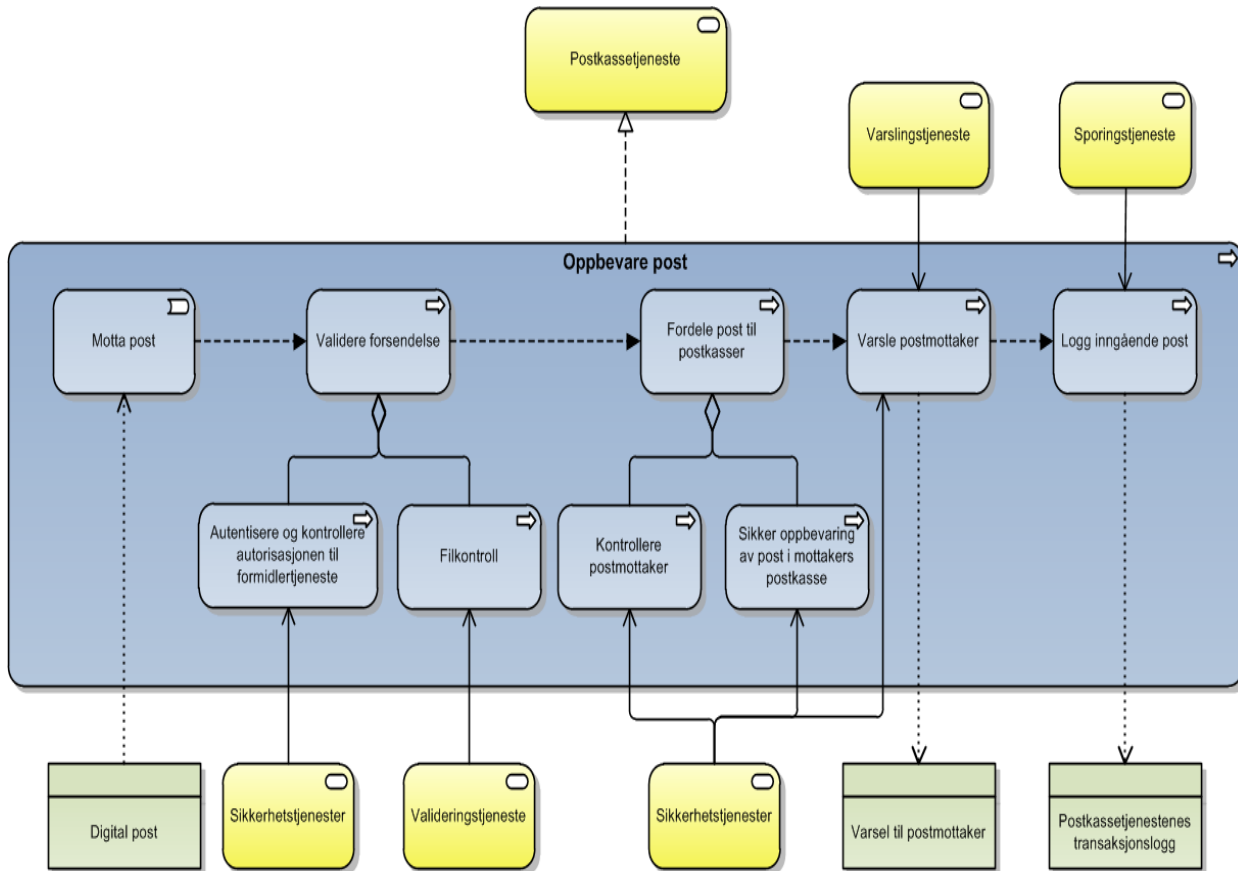
Figur 19: Formidle post

3.3.4 Detaljering av forretningsprosessen Oppbevare post

Oppbevare post består av følgende steg:

1. Motta post fra Formidlertjenesten
2. Validere forsendelsen
 - sikre at forsendelsen er sendt fra en autorisert Formidlertjeneste
 - kontrollere postforsendelsen i henhold til definerte formatstandarder fra Valideringstjenesten
3. Fordele post til postkasser
 - kontrollere at adressert postmottaker har postkasse hos postkassetjenesten
 - oppbevare post på en sikker måte i mottakers postkasse

4. Varsle postmottaker bruker Varslingstjenesten til å sende varsel til mottaker
 5. Prosessen avsluttes med å logge inngående post i Postkassetjenestens transaksjonslogg
- Stegene beskriver normalsituasjonen. Feilsituasjoner, som for eksempel feil ved varsling om ny post, skal også logges og kvittering sendes til avsendervirksomheten via meldingsformidleren.



Figur 20: Oppbevare post

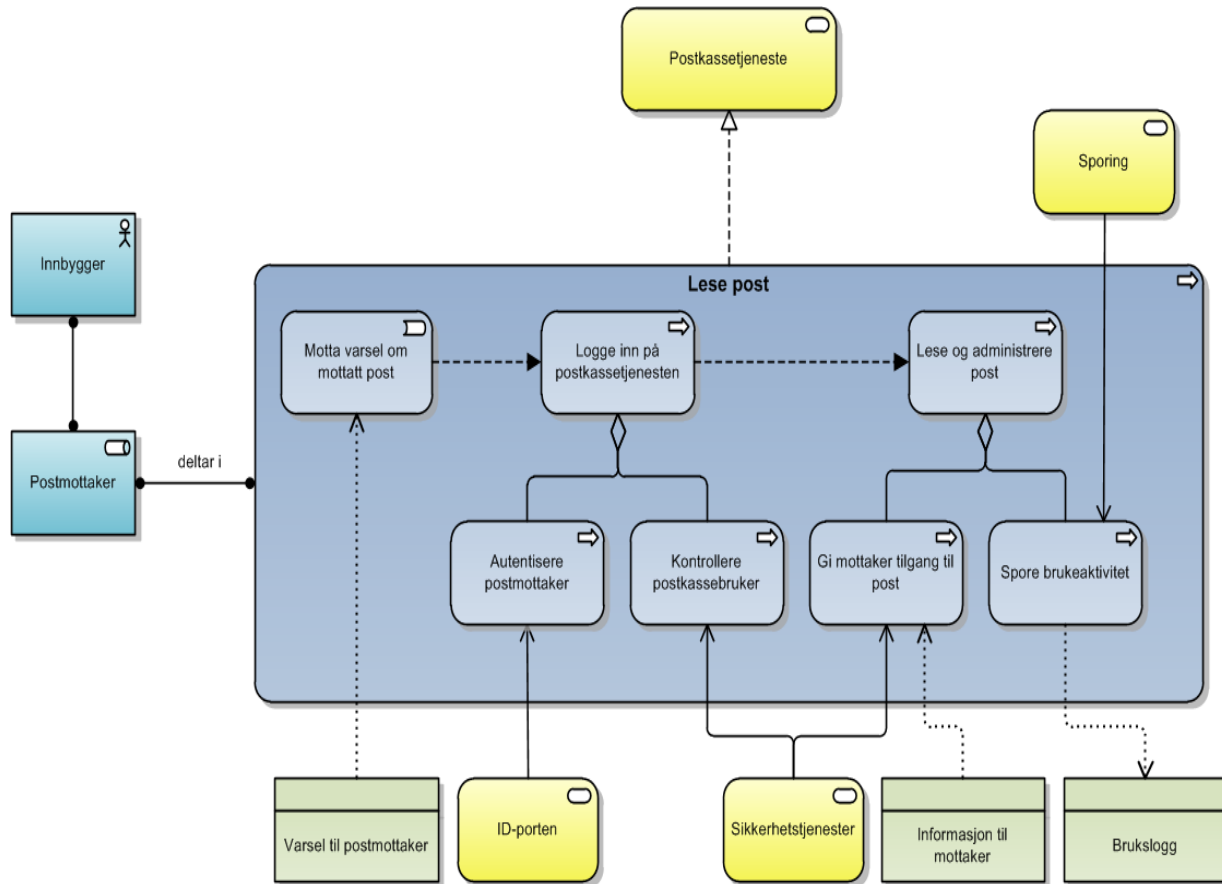
3.3.5 Detaljering av forretningsprosessen Lese post

Lese post består av følgende steg:

1. Postmottaker mottar varsel om ny post
2. Postmottaker logger seg inn på sin postkassetjeneste:
 - Postkassetjenesten autentiserer postmottaker med bruk av ID-porten
 - Postkassetjenesten kontrollerer autoriseringen til postmottaker (postmottaker må ha opprettet postkasse hos postkasseleverandøren)

3. Postmottaker kan lese, organisere, videresende og slette post:

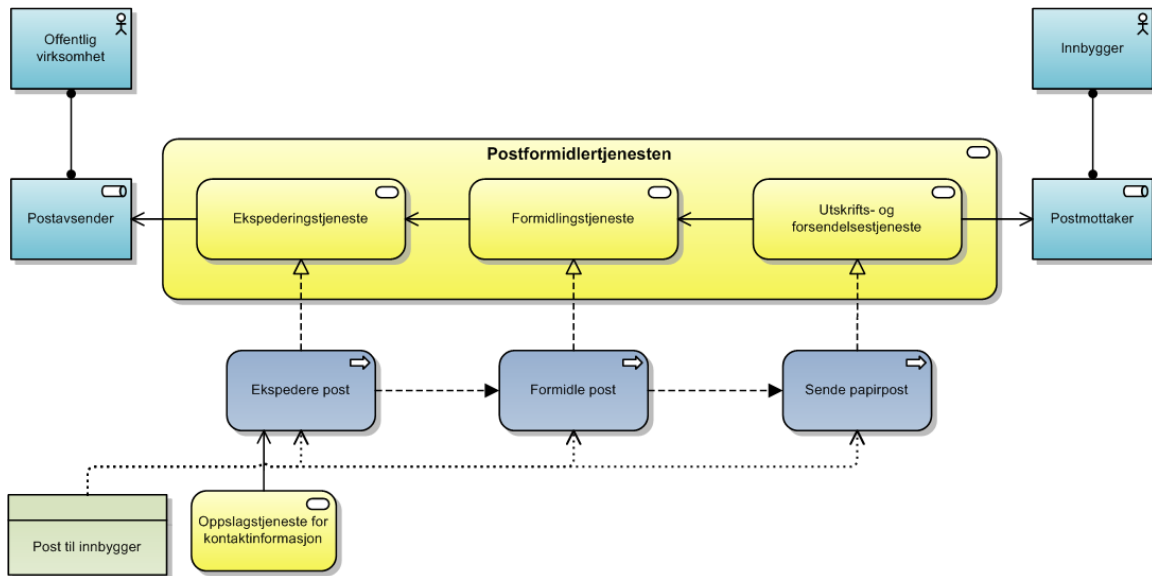
- Posten blir gjort tilgjengelig for postmottaker
- Postkassetjenesten logger brukerinteraksjon i bruksloggen. Aggregert informasjon fra bruksloggen vil gjøres tilgjengelig for statistiske formål.



Figur 21: Lese post

3.3.6 Sikker digital posttjenestens håndtering av papirpost

Prosessmodellen under beskriver de overordnede forretningsprosessene som vil realisere postformidlingstjenestens håndtering av papirpost.



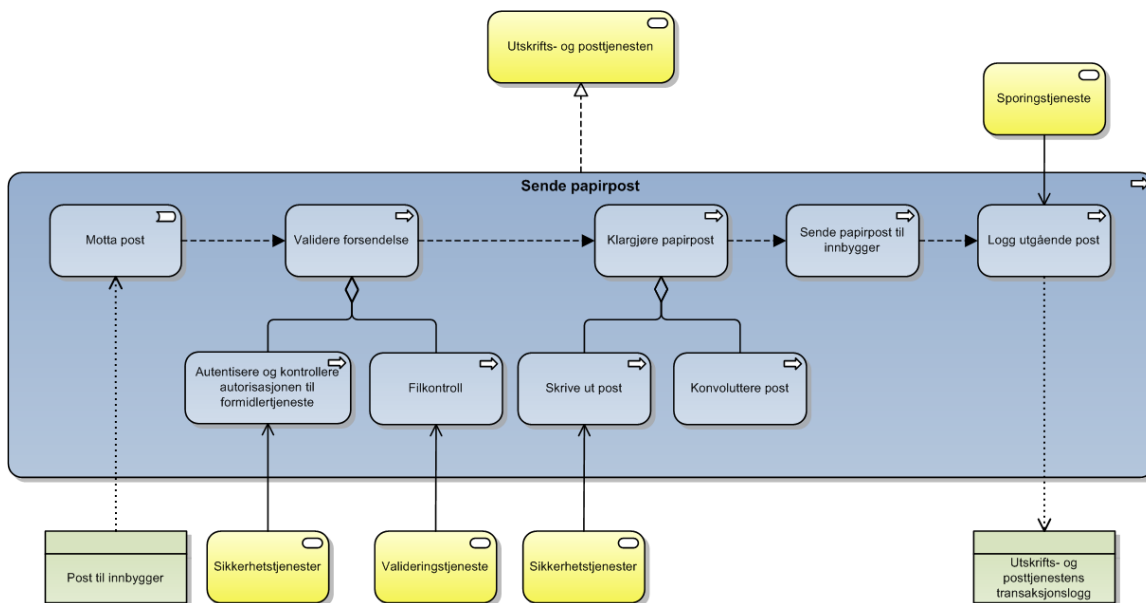
Figur 22: Håndtering av papirpost

Arkitekturen legger opp til at postavsender sender papirpost digitalt og på en sikker måte til utskrifts- og forsendelsestjenesten. Det vil si at ekspederingstjenesten og formidlertjenesten betrakter papirpost til innbygger som digital post.

Når innbygger skal få tilsendt post på papir, leverer oppslagstjenesten utskrifts- og forsendelsestjenestens kontaktinformasjon til ekspederingstjenesten. Offentlig virksomhet er selv ansvarlig for postadressen til innbygger. På sikt vil den kunne hentes fra oppslagstjenesten, når oppslagstjenesten blir knyttet til Folkeregisteret. Offentlig virksomhet klargjør en digital post i standardformat, inkludert konfidensialitetssikring med utskrifts- og forsendelsestjenestenes sertifikat. Ekspederingstjenesten sender så den digitale posten adressert til utskrifts- og forsendelsestjenesten til formidlingstjenesten.

Formidlertjenesten viderefremidler den digitale posten til utskrifts- og forsendelsestjenesten.

I figuren under vises forretningsprosessen Sende papirpost som realiserer utskrifts- og forsendelsestjenesten.



Figur 23: Sende papirpost

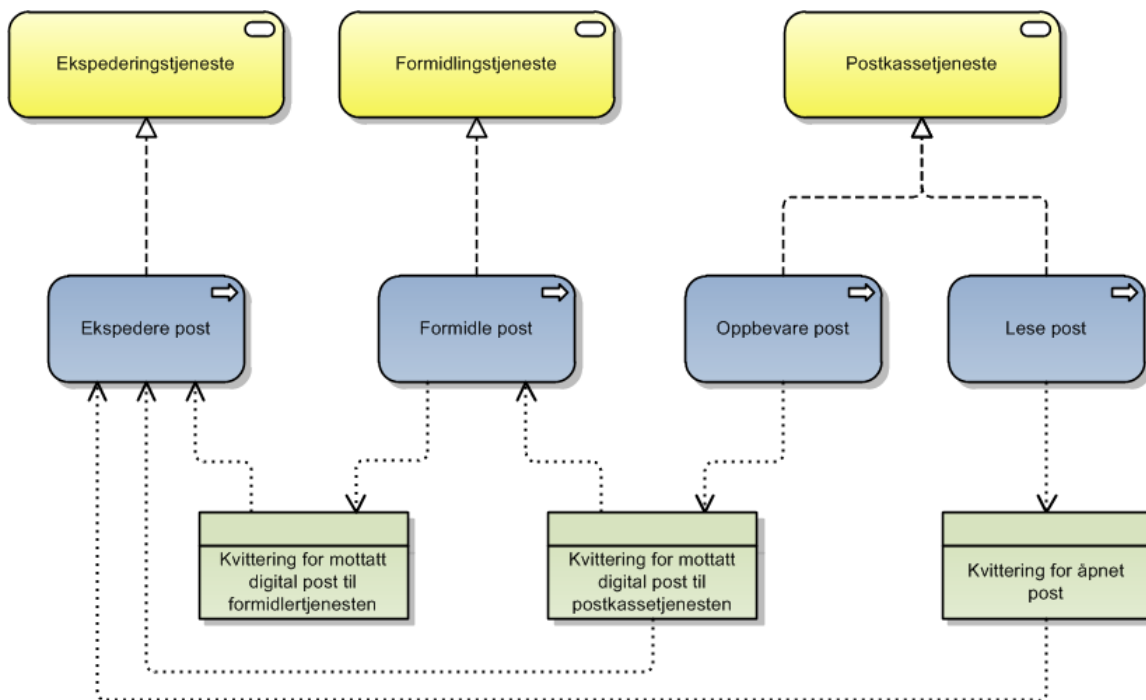
Sende post består av følgende steg:

1. Motta post fra formidlertjenesten
2. Validere forsendelsen
 - sikre at forsendelsen er sendt fra en autorisert formidlertjeneste
 - kontrollere postforsendelsen i henhold til definerte formatstandarder fra valideringstjenesten
3. Klargjøre papirpost
 - Skrive ut post på papir i sikrede omgivelser
 - Konvoluttere papirpost
4. Sende papirpost til innbygger, dvs. å distribuere papirpost til innbyggers postadresse
5. Prosessen avsluttes med å logge utgående post i utskrifts- og forsendelsestjenestens transaksjonslogg

Stegene beskriver normalsituasjonen. Feilsituasjoner, som for eksempel returpost, skal også logges og kvittering sendes til avsendervirksomheten via meldingsformidleren.

3.3.7 Kvittering i forbindelse med postformidling

Arkitekturen legger opp til at kvitteringer skal genereres og sendes, både når en hendelse har gått som forventet, og når noe har gått galt. I tillegg kan kvitteringer inneholde advarsler eller annen nyttig informasjon, som for eksempel at virksomhetssertifikatet som ble benyttet snart løper ut. Kvitteringene er tenkt formidlet mellom aktørene på samme måte som digital post formidles.



Figur 24: Kvitteringer i forbindelse med postformidling

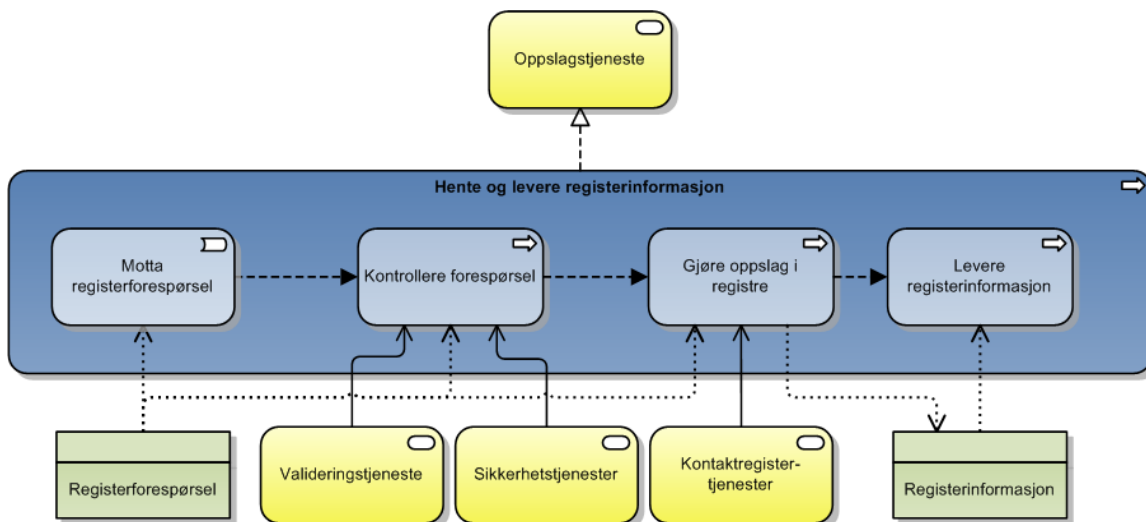
Formidlingstjenesten vil gi en kvittering til ekspederingstjenesten om at posten er mottatt og sjekket. Kvitteringen vil enten fortelle at alt er som forventet, eller den vil gi en feilmelding dersom posten ikke kan formidles videre.

Postkassetjenesten vil gi kvittering til formidlingstjenesten og ekspederingstjenesten (via formidlingstjenesten) om at posten er mottatt og gjort tilgjengelig for mottaker i mottakers postkasse, eventuelt at meldingen har feilet.

Kvitteringer for mottatt digital post kan være av ulike typer. For eksempel kan en kvittering inneholde informasjon om at varsling av mottaker feilet (e-post i retur), eller at mottaker ikke er aktiv bruker av postkassetjenesten. I tilfeller der avsendervirksomheten skal få bekreftelse på at mottaker har åpnet posten, vil postkassetjenesten levere kvittering til ekspederingstjenesten (via formidlingstjenesten) om at mottaker har åpnet posten. Dette kan skje med eller uten mottakers medvirkning, avhengig av hvordan regelverket utformes.

3.3.8 Detaljering av oppslagstjenesten

Figuren under viser hvilke virksomhetsprosesser som realiserer oppslagstjenesten.



Figur 25: Detaljering av oppslagstjenesten

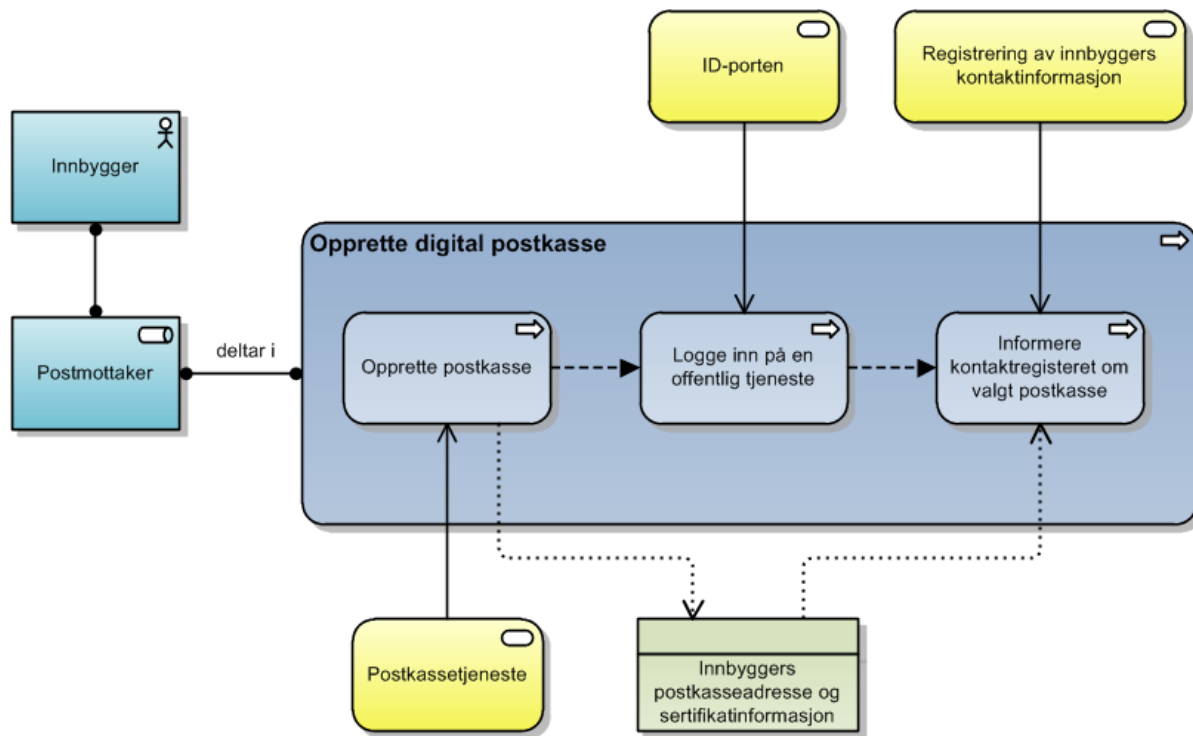
Prosessen starter ved en registerforespørsel fra en avsendervirksomhet. Det må valideres at forespørselen kommer fra en aktør som har rettigheter til å gjøre oppslag, og at forespørselen har riktig format. Oppslagstjenesten vil videre gjøre oppslag i de nødvendige registre, og levere registerinformasjon til avsendervirksomheten.

3.3.9 Opprette digital postkasse

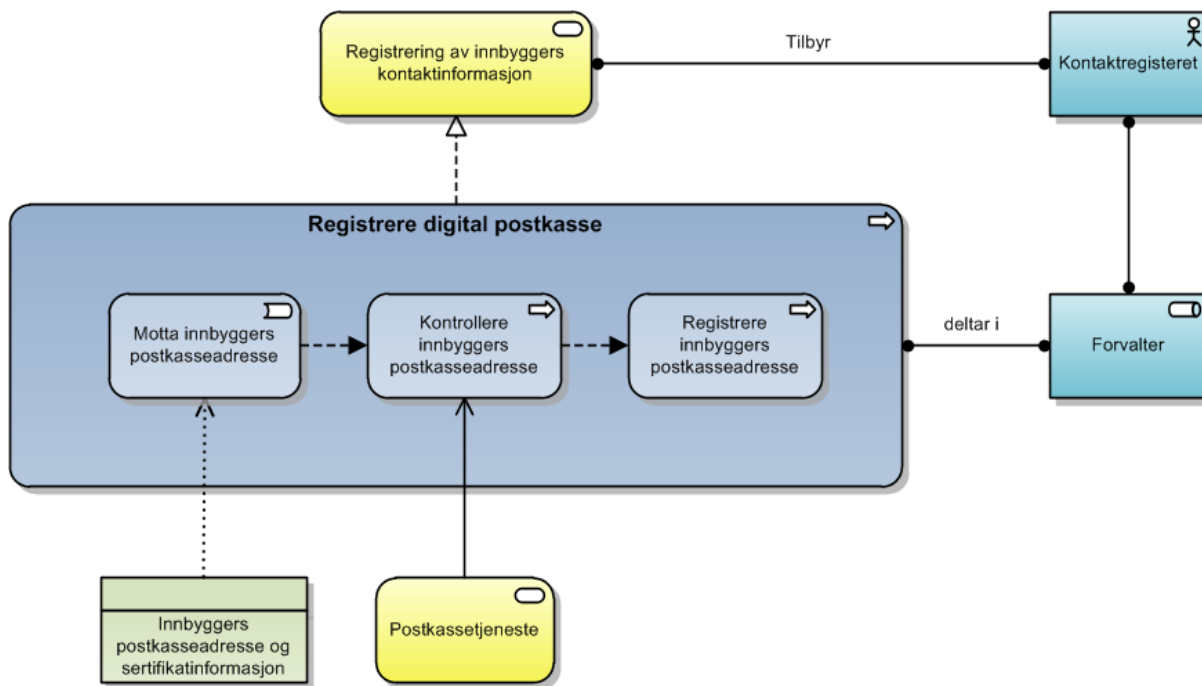
Postkasse opprettes hos en postkasseleverandør som innbygger selv velger, blant de postkasseleverandørene som har avtale med sentralforvalter. En innbygger kan opprette digitale postkasser hos flere leverandører, men kun én av disse kan til enhver tid være valgt som innbyggerens postkasse for post fra det offentlige.

3.3.10 Registrere digital postkasse

En innbygger må ha en postkasse før den kan registreres i kontaktregisteret. ID-porten benyttes for å autentisere innbyggeren ved registrering av postkasse i kontaktregisteret. Registrering skal være enkelt for innbyggeren, der det tilrettelegges for at postkasseadresse og sertifikatinformasjon leveres automatisk, fra postkasseleverandøren, på innbyggerens initiativ. Postkasseleverandøren informeres om at kunden har registrert postkassen for mottak av offentlig post, og en bekreftelse sendes til innbyggeren.



Figur 26: Innbyggers prosesser for å registrere digital postkasse



Figur 27: Kontaktregisterets prosesser for å registrere digital postkasseadresse

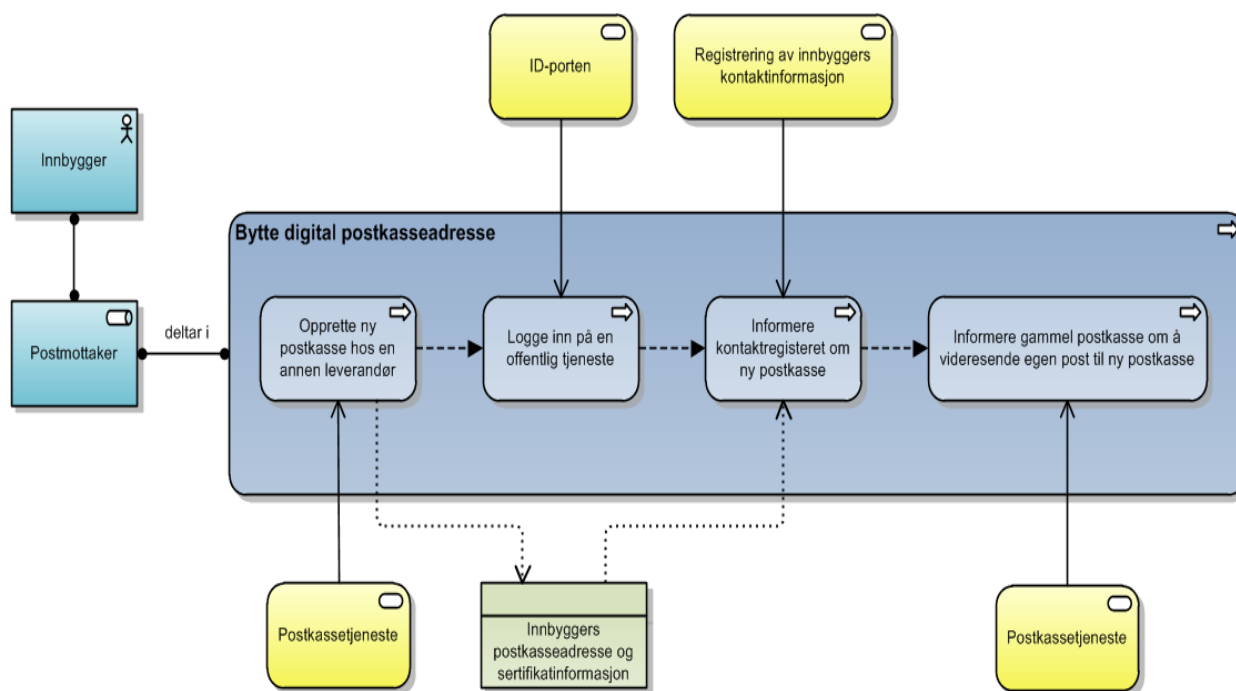
3.3.11 Bytte digital postkasse

Arkitekturen for Sikker digital posttjeneste skal legge til rette for at innbygger kan bytte digital postkasse på en enkel måte. Arkitekturen tar ikke stilling til hvilke aktører som skal belastes for byttekostnaden.

Innbyggeren må ha en postkasse å bytte til, og denne opprettes på samme måte som beskrevet ovenfor.

Kontaktregisterets prosess for å registrere at innbygger har byttet digital postkasse er lik kontaktregisterets prosesser for å registrere digital postkasseadresse. Kontaktregisteret informerer postkasseleverandøren om at postkassen ikke lenger er innbyggerens valgte postkasse for offentlig post.

Arkitekturen for Sikker digital posttjeneste forutsetter at postkassetjenesten kan videresende post til annen sikker digital postkasse. Det vil si at postkasseleverandøren opererer som en postavsender og må tilby og benytte en ekspederingstjeneste slik den er beskrevet i arkitekturen for Sikker digital posttjeneste. Ved bytte av postkasse skal postkassetjenesten tilby brukeren (postmottakere av offentlige post) en mulighet til å velge hvilken post fra det offentlige som skal flyttes til hans nye valgte postkasse. Detaljer omkring metadata og hvordan videresendt post skal vises i ny postkasse er ikke detaljert på dette nivået.



Figur 28: Innbyggers prosesser for å bytte digital postkasse

4. Informasjonsarkitektur

I beskrivelsene av informasjonsarkitekturen er det foreløpig fokusert på forretningsobjekter relatert til den digitale posten fra avsender til mottaker, og informasjonsmodeller for selve den digitale posten. Dette gir en forståelse for omfanget av informasjonen selv om detaljer rundt kvitteringer, registeroppslag og logging er utelatt.

Begreper innen domenet Sikker digital posttjeneste, som brukes mellom flere aktører, dokumenteres i en begrepskatalog hos sentralforvalter. Begrepskatalogen publiseres på nett i henhold til egnet standard (e.g. RDFa).

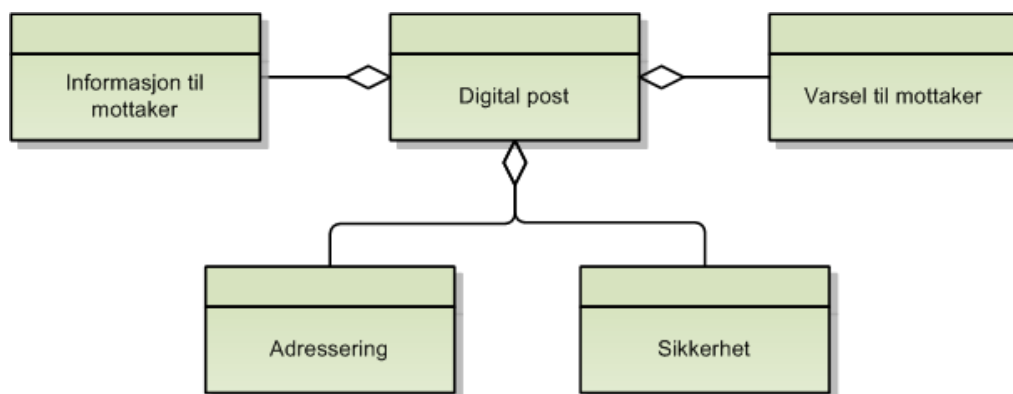
4.1 Forretningsobjekter

Forretningsobjektene identifisert i forretningsarkitekturen til Sikker digital posttjeneste er utgangspunktet for å identifisere og beskrive de sentrale dataobjektene.

Forretningsobjektene faller i fem hovedgrupper:

4.1.1 Digital post

Et eller flere digitale dokumenter med tilhørende metadata som sendes til en mottaker fra en avsendervirksomhet.



Figur 29: Digital post

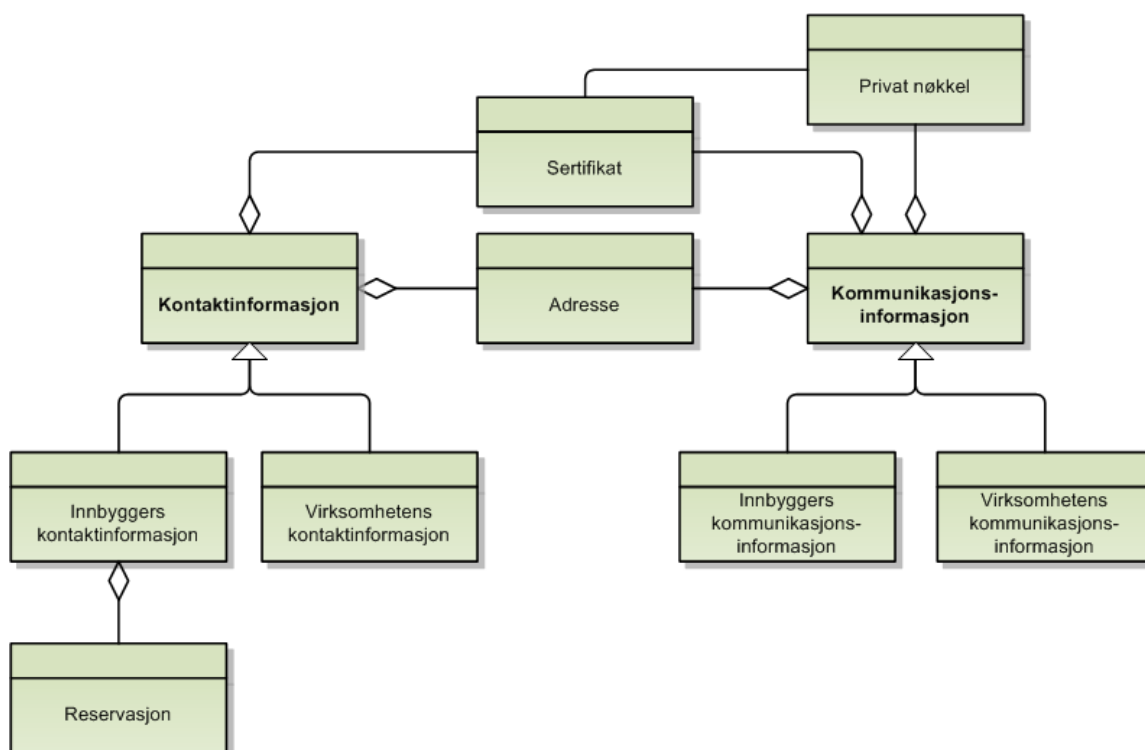
Forretningsobjekt	Beskrivelse
Informasjon til mottaker	Informasjon bestemt av postavsender som skal gis til postmottaker.
Varsel til postmottaker	Informasjon bestemt av postavsender eller postkassetjenesten som varsler postmottaker om ny digital post fra offentlig virksomhet.

Adressering	Nødvendig informasjon for å levere post og varsel til postmottaker.
Sikkerhet	Nødvendig informasjon for å sikre leveransen mellom avsender og mottaker.

4.1.2 Kontakt- og kommunikasjonsinformasjon

Kontaktinformasjon benyttes til å adressere og konfidensialitetssikre post til rett mottaker.

Kommunikasjonsinformasjon benyttes i å integritetssikre digital post til mottaker.



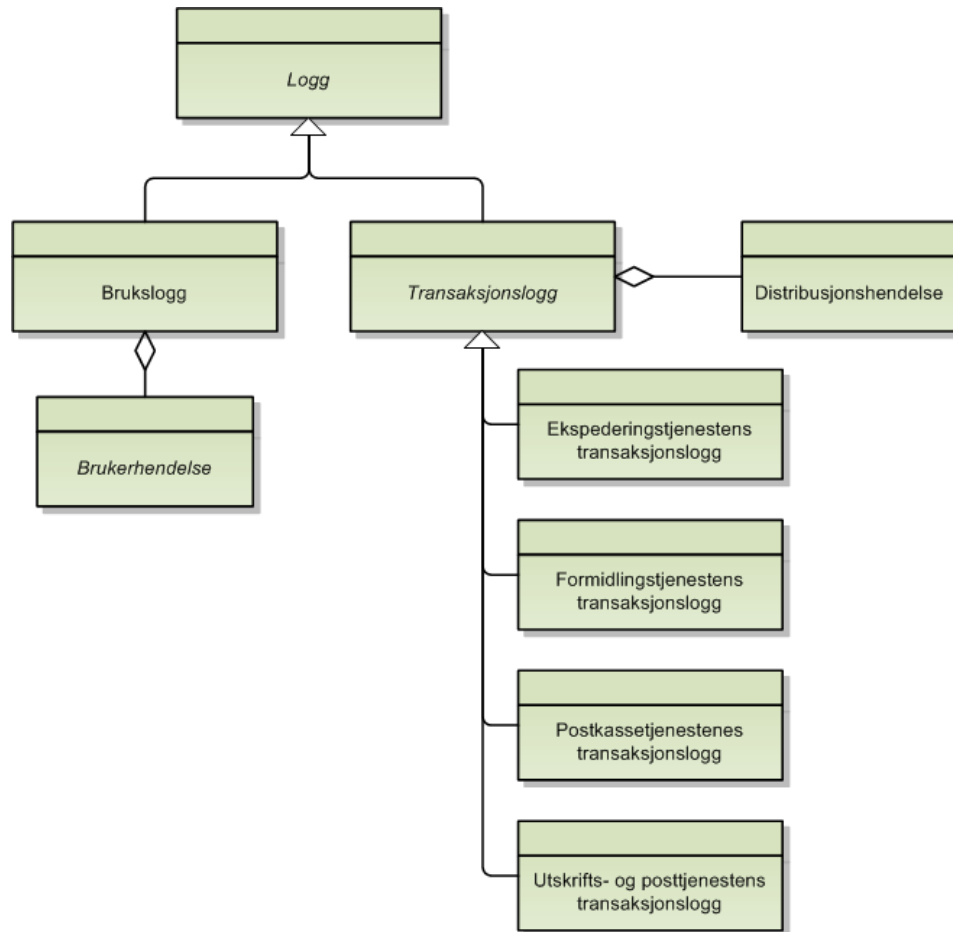
Figur 30: Kontakt- og kommunikasjonsinformasjon

Forretningsobjekt	Beskrivelse
Kontaktinformasjon	Nødvendig informasjon for å adressere post til rett mottaker. Mottaker av post er eier og forvalter av informasjonen, dvs. adresser, sertifikater og reservasjon.

Kommunikasjonsinformasjon	Informasjonsinnhold nødvendig for å sikre post til mottaker (sertifikater og private nøkler) og returadresser for tilbakemeldinger.
Adresse	Adresseinformasjon for å kunne sende digital post og papirpost
Sertifikat	Sertifikat for å kunne konfidensialitets- og integritetssikre digital postforsendelsen. I en digital kommunikasjon benyttes både avsenders og mottakers sertifikat.
Privat nøkkel	Kryptografisk nøkkel for elektronisk signering og dekryptering.
Reservasjon	Reservasjonsstatus som bestemmer om innbygger skal motta digital post. Innbygger eier og forvalter sin egen reservasjonsstatus.

4.1.3 Logg

Logg er informasjon som støtter opp om hendelsehåndtering, feilretting og statistikk.



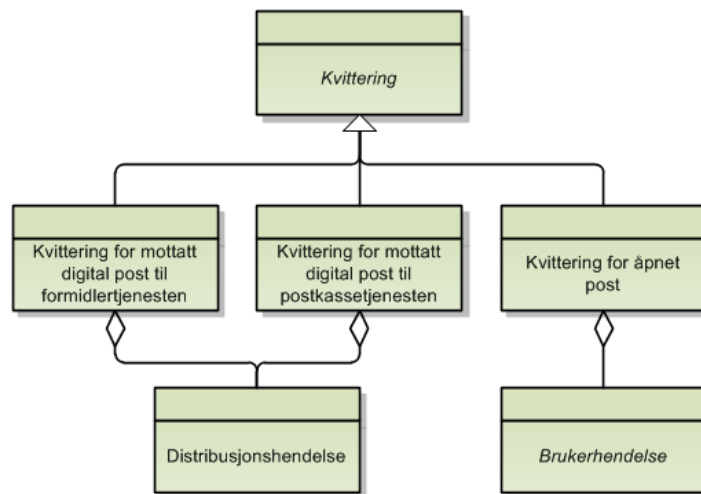
Figur 31: Logg

Forretningsobjekt	Beskrivelse
Ekspederingstjenestens transaksjonslogg	Logg av distribusjonshendelser for sporbarhet og statistikkformål.
Formidlertjenestens transaksjonslogg	Logg av distribusjonshendelser for sporbarhet og statistikkformål.
Postkassetjenestens transaksjonslogg	Logg av distribusjonshendelser for sporbarhet og statistikkformål.

Forretningsobjekt	Beskrivelse
Utskrifts- og forsendelsestjenestes transaksjonslogg	Logg av distribusjonshendelser for sporbarhet og statistikkformål.
Brukslogg	Logg av brukerhendelser i postkassen for sporbarhet, statistikkformål og brukskvalitet.
Distribusjonshendelse	Beskrivelse av hendelse for å kunne identifisere hva som hente når, i den digitale postforsendelsen.
Brukerhendelse	Beskrivelse av hendelse for å kunne identifisere hva postmottaker gjorde når, i sin administrasjon av den digitale posten.

Kvittering

Informasjon som kommuniseres mellom aktørene for å håndtere leveransen av digital post formidles igjennom kvitteringer.

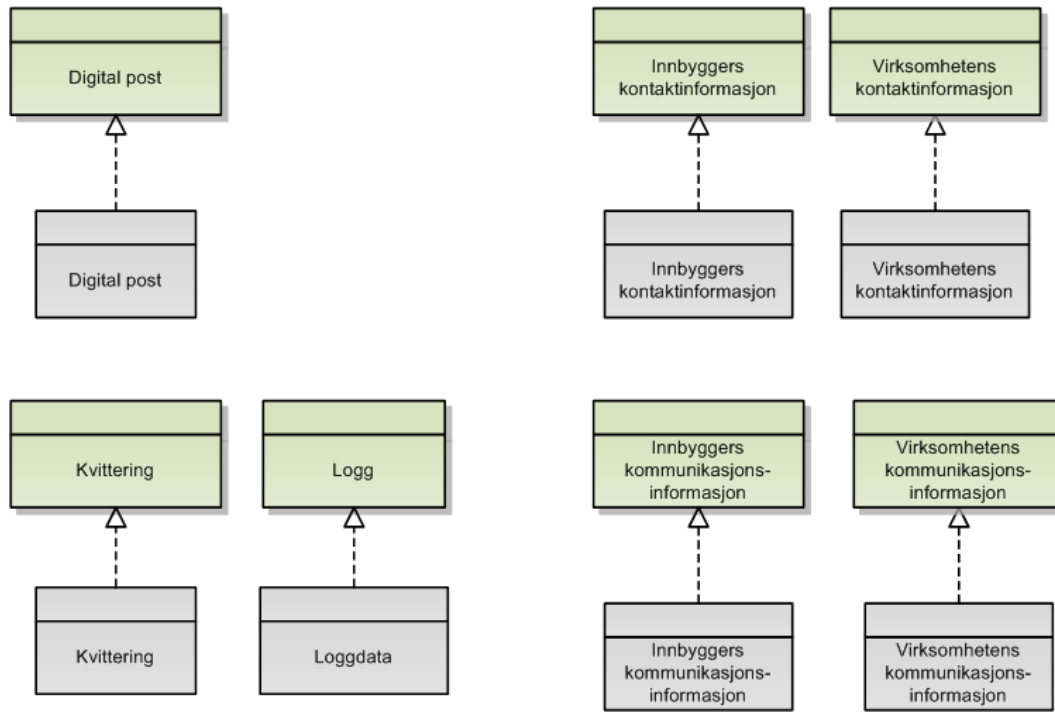


Figur 32: Kvittering

Forretningsobjekt	Beskrivelse
Kvittering for mottatt digital post til formidlertjenesten	Informasjon til avsender om at formidlertjenesten har tatt i mot en digital postforsendelse, og status på forsendelsen.
Kvittering for mottatt digital post til postkassetjenesten	Informasjon til avsender og formidlertjenesten om at postkassetjenesten har tatt i mot en digital postforsendelse, og status på forsendelsen.
Kvittering for åpnet post	Informasjon til avsender om at mottaker av post har åpnet denne. Det er ikke gitt at mottaker kan lese posten (e.g. PDF lastet ned til datamaskin uten PDF-leser)
Distribusjonshendelse	Se logg (over).
Brukerhendelse	Se logg (over).

4.1.4 Dataobjektene som realiserer forretningsobjektene

Figuren under illustrerer dataobjektene som realiserer de identifiserte forretningsobjektene i Sikker digital posttjeneste.



Figur 33: Dataobjekter

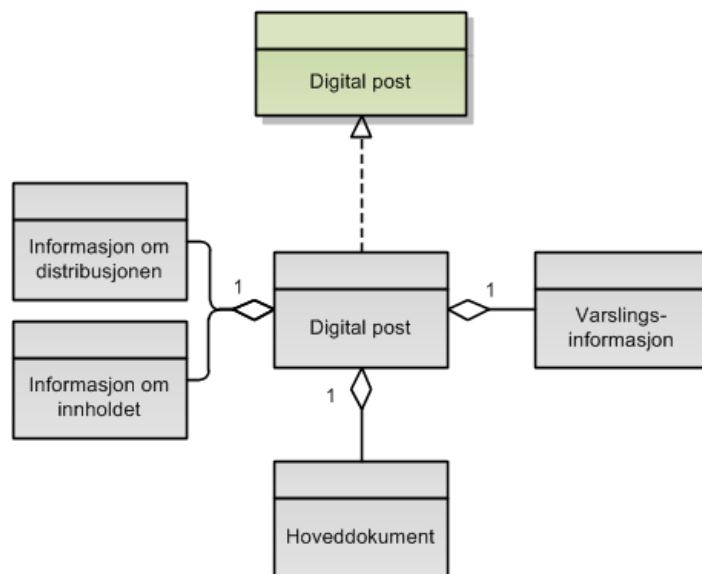
I det neste avsnittet detaljeres dataobjektene.

4.2 Informasjonsmodeller

Informasjonsmodellene presentert her er på et konseptuelt og logisk nivå. Difi som sentralforvalter av Sikker digital posttjeneste har ansvaret for å detaljere de logiske og operasjonelle modellene. Dette vil gjøres på et senere tidspunkt og i samarbeid med avsendervirksomheter og leverandører.

4.2.1 Digital post

Et eller flere digitale dokumenter med tilhørende informasjon om distribusjon og innhold som sendes til en mottaker fra en avsendervirksomhet.

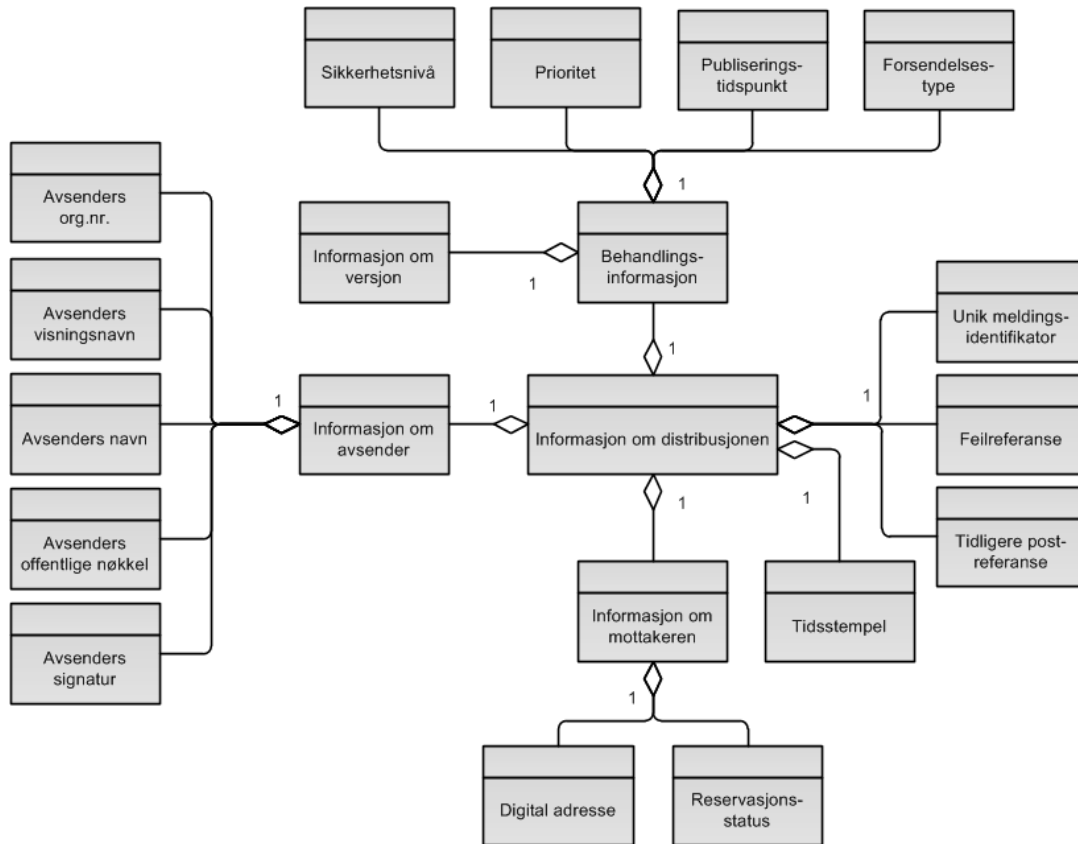


Figur 34: Digital post

Dataobjekt	Beskrivelse
Digital post	Et eller flere digitale dokumenter med tilhørende metadata som sendes til en mottaker fra en avsendervirksomhet.
Hoveddokument	Digital post består alltid av et hoveddokument, som er informasjon til postmottaker. Et hoveddokument kan ha flere vedlegg.
Varslingsinformasjon	Informasjon om brukeren skal motta varsel og på hvilken form. Varslingsinformasjon består også av varslingsstekst og varslingsadresse (se beskrivelse under).
Informasjon om distribusjonen	Adresseinformasjon og behandlingsregler
Informasjon om innholdet	Beskrivelse av type og innhold (hoveddokument)

Informasjon om distribusjonen

Informasjon om distribusjonen er informasjonen som er nødvendig for å flytte dokumenter fra avsender til mottaker.



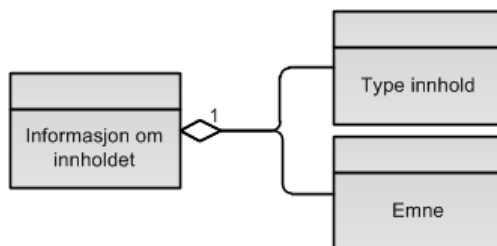
Figur 35: Informasjon om distribusjon

Dataobjekt	Beskrivelse
Unik meldingsidentifikator	All post skal ha en unik ID for sporing og behandling.
Feilreferanse	Referanse til bruk ved resending etter feil.
Tidligere postreferanse	Referanse til tidligere post.

Tidsstempel	Merking av tidspunkt digital post ble sendt fra avsender.
Informasjon om avsender	Informasjon om avsender for bruk ved autentisering, autorisasjon og integritetskontroll.
Informasjon om mottaker	Adresse og reservasjonsstatus ved sending.
Behandlingsinformasjon	Informasjon om hvordan aktørene skal behandle den digitale posten.

Informasjon om innholdet

Gode søkemuligheter og sortering av post er gir en bedre brukeropplevelse, og informasjon om innholdet gir nødvendig støtte for slik funksjonalitet.

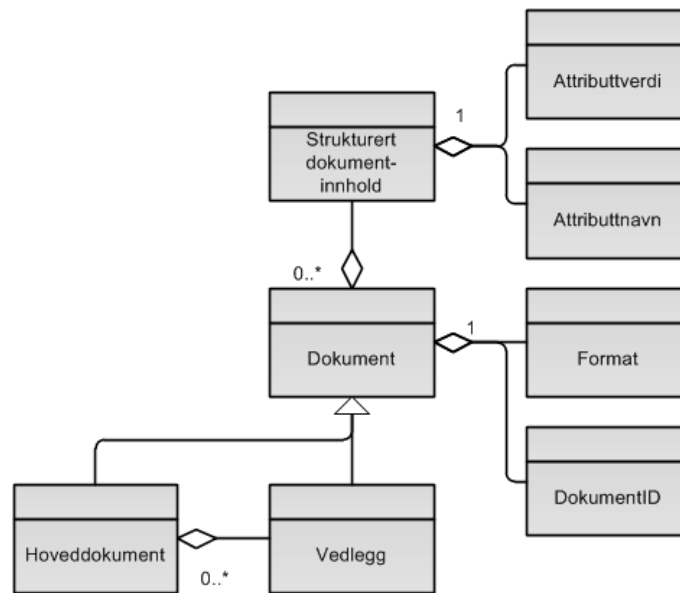


Figur 36: Informasjon om innholdet

Dataobjekt	Beskrivelse
Type innhold	Kategorisering av innhold, f.eks. vedtak, informasjonsbrev, prøvesvar.
Emne	Avsenders beskrivelse av innhold.

Dokument

Dokumenter er selve innholdet som skal flyttes fra avsender til mottager.

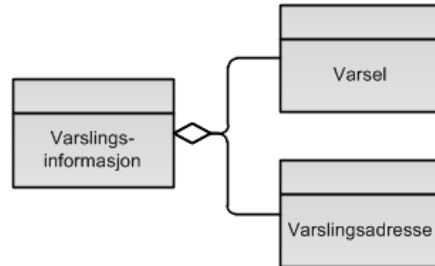


Figur 37: Dokument

Dataobjekt	Beskrivelse
Dokument	Informasjon til mottaker, hoveddokument eller vedlegg.
DokumentID	ID på dokument.
Format	Dokumentformat, eks. PDF, HTML etc.
Strukturert dokumentinnhold	Mulighet for avsender til å lage strukturert beskrivelse av innholdet i dokumentet.
Hoveddokument	Informasjon til mottaker.
Vedlegg	Informasjon til mottaker som avsender velger å ha i eget dokument, tillegg til hoveddokument.

Varslingsinformasjon

Det vil variere hvor ofte innbyggere kobler seg opp mot løsningen, og for å unngå at viktig informasjon kommer for sent frem er det lagt opp til at innbygger kan varsles om at det ligger post i postkassen.



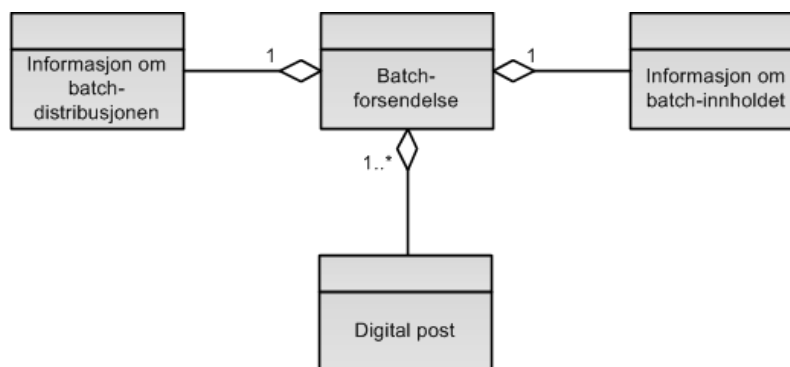
Figur 38: Varslingsinformasjon

Dataobjekt	Beskrivelse
Varsel	Varslingstekst fra avsender til mottaker.
Varslingsadresse	Adresse, eller kanal for varsling, eks. mobiltelefonnummer eller epostadresse.

4.2.2 Batch-forsendelse

Arkitekturen tar ikke stilling til om avsendervirksomhetene må sende digital post enkeltvis eller om de også skal kunne sende batcher til meldingsformidler. En batch vil inneholde en samling av digital post fra avsendervirksomhet til ulike postmottakere.

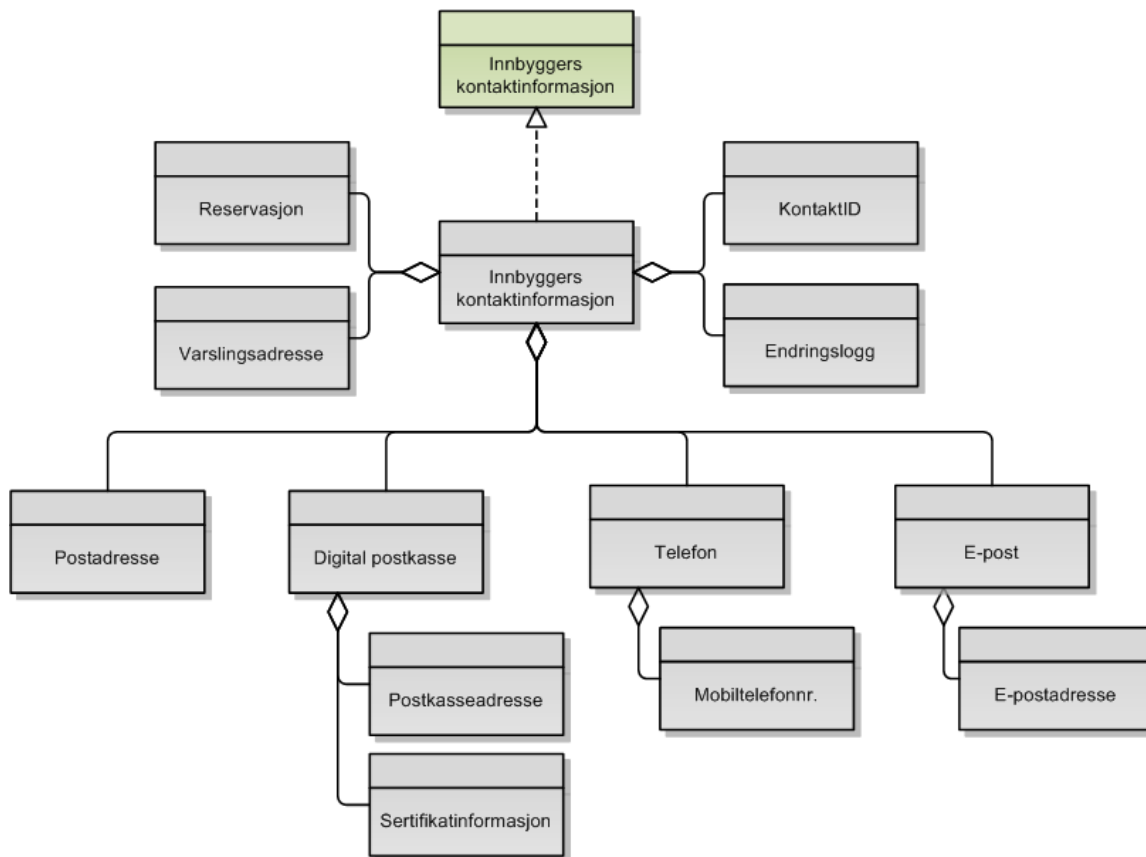
Informasjon om batch-distribusjon vil være informasjon om avsender og behandlingsregler for batch. Informasjon om batch-innholdet beskriver hva som inngår i og omfang av batch-forsendelsen (jf. figuren under).



Figur 39: Batch

4.2.3 Innbyggers kontaktinformasjon

Dataobjektet innbyggers kontaktinformasjon er en konseptuell og logisk samling av innbyggers adresseinformasjon, i tillegg til innbyggers reservasjonsstatus i forhold til digital kommunikasjon med det offentlige. For Sikker digital posttjeneste vil det være innbyggers reservasjonsstatus vedrørende mottak av digital post fra offentlige virksomheter.



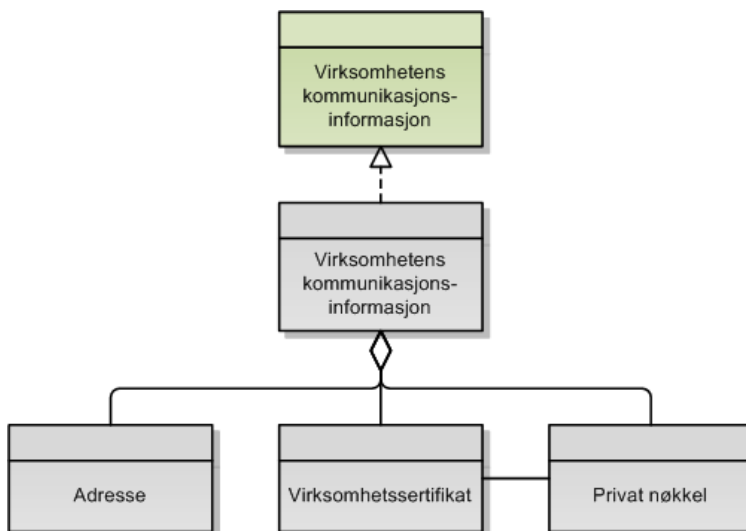
Figur 40: Innbyggers kontaktinformasjon

Dataobjekt	Beskrivelse
Innbyggers kontaktinformasjon	Innbyggers registrerte kontaktadresser og reservasjonsstatus.
KontaktID	Innbyggers unike identifikator. I førsteomgang vil det være fødselsnummer eller D-nummer.
Endringslogg	En logg på hvilke endringer innbygger har gjort med sin kontaktinformasjon.

Dataobjekt	Beskrivelse
Reservasjon	Innbyggers reservasjonsstatus i forhold til digital kommunikasjon med det offentlige.
Varslingsadresse	Innbyggers valgte varslingsform. I første omgang vil det være alternativene mobiltelefonnummer (sms) eller e-postadresse, men også apps og andre varslingsformer skal kunne benyttes dersom innbyggeren velger det.
Postadresse	Innbyggers postadresse for mottak av papirpost fra det offentlige.
Digital postkasse	Informasjon for å kunne sende sikker digital post til innbyggers digitale postkasse.
Postkasseadresse	Adressen til innbyggers valgte digitale postkasse for mottak av digital post fra offentlige virksomheter.
Sertifikatinformasjon	Innbyggers sertifikater for å konfidensialitetssikre digital post fra offentlige virksomheter.
Telefon	Innbyggers registrerte telefon. Denne består i utgangspunktet av mobiltelefonnummer som kan benyttes for sms.
E-post	Innbyggerens registrerte e-post. I utgangspunktet består denne bare av en e-postadresse, men kan utvides med sertifikatinformasjon eller lignende dersom det blir aktuelt på et senere tidspunkt.

4.2.4 Virksomhetens kommunikasjonsinformasjon

Dataobjektet virksomhetens kommunikasjonsinformasjon er en konseptuell og logisk samling av dataobjekter nødvendig for at virksomheten kan integritetssikre digital post til innbygger.

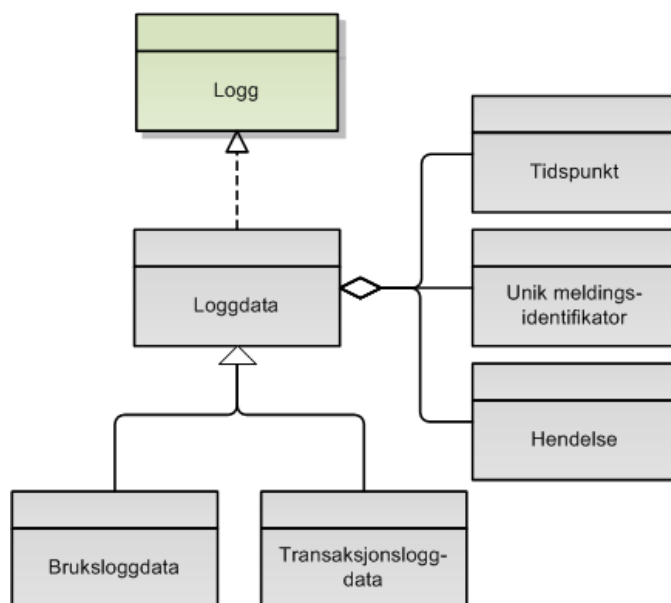


Figur 41: Virksomhetens kommunikasjonsinformasjon

Dataobjekt	Beskrivelse
Virksomhetens kommunikasjonsinformasjon	Nødvendig informasjon for integritetssikring og returmeldinger i forhold til Sikker digital posttjeneste.
Adresse	Adresser som brukes for kvitteringer og returmeldinger fra mottakere og distributører av digital post. (Innbyggeren kan ikke sende digital post til forvaltningen, selv om arkitekturen legger til rette for det.)
Virksomhetssertifikat	Sertifikater for å identifisere virksomheten. Sertifikatet inneholder virksomhetens navn og en unik virksomhetsidentifikator.
Privat nøkkel	Kryptografiske nøkler for å signere og dekryptere digital post.

4.2.5 Logg

Loggdata er informasjon som støtter opp om sporing, hendelseshåndtering, feilretting og statistikk.



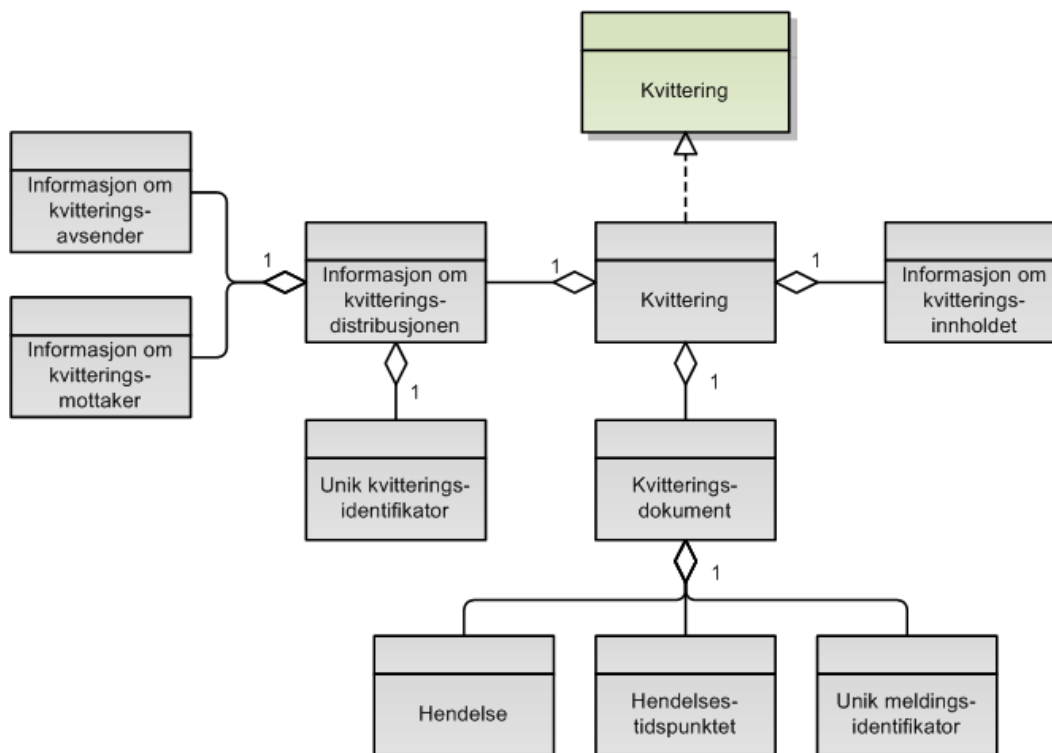
Figur 42: Logg

Dataobjekt	Beskrivelse
Loggdata	Informasjon om en hendelse som tas vare på
Tidspunkt	Tidspunkt for loggdata.
Unik meldingsidentifikator	Den unike meldingsidentifikatoren for meldingen som loggdata relateres til.
Hendelse	Beskrivelse av hendelsen som logges.
Bruksloggdata	Loggdata knyttet til brukerens handlinger i postkassen
Transaksjonsloggdata	Loggdata knyttet til formidlingen av post.

4.2.6 Kvittering

Kvitteringer benyttes til formidling av informasjon om leveransen av digital post. For eksempel at en melding er kommet frem, eller at en melding ikke kan leveres fordi mottakeren ikke eksisterer.

Informasjon som kommuniseres mellom aktørene for å håndtere leveransen av digital post formidles igjennom kvitteringer.



Figur 43: Kvittering

Dataobjekt	Beskrivelse
Kvittering	Informasjon som formidles mellom partene relatert til forsendelse av digital post.
Informasjon om kvitteringsinnholdet	Beskrivelse av kvitteringens innhold, som f.eks. om det er mottaks-, feil- eller advarselskvittering.
Kvitteringsdokument	Kvitteringens forretningsinnhold: beskrivelse av hendelse, hendelsestidspunkt og unik meldingsidentifikator
Informasjon om	Nødvendig informasjon for distribusjon av kvitteringen.

Dataobjekt	Beskrivelse
kvitteringsdistribusjonen	
Hendelse	Hendelsen som kvitteringen handler om, f.eks. melding mottatt eller postmottaker ukjent.
Hendelsestidspunktet	Når hendelsen fant sted.
Unik distribusjonsidentifikator	Postforsendelsens unike identifikator.
Unik kvitteringsidentifikator	Unik identifikator for kvitteringen. Benyttes for unik logging og sporing av kvitteringer.
Informasjon om kvitteringsavsender	Informasjon om hvem kvitteringen er fra.
Informasjon om kvitteringsmottaker	Informasjon om hvem kvitteringen er til.

5. Sikkerhetsarkitektur

TOGAF er benyttet som rammeverk for arkitekturarbeidet. Sikkerhetsarkitekturen omfatter mange områder, hvor utdrag fra noen av disse er gjengitt her.

5.1 Sikkerhetsforutsetninger og betingelser

- ID-porten skal brukes for identifisering og autentisering av innbygger i Sikker digital posttjeneste.
- Virksomhets sertifikater skal brukes for å identifisere og autentisere avsendervirksomheter, meldingsformidler og postkasseleverandører i Sikker digital posttjeneste.
- Avsendervirksomhetene skal beholde kopi av alt som sendes igjennom Sikker digital posttjeneste.
- Avsendervirksomhetene er ansvarlig for utsending av post, og må selv vurdere behovet for alternativ utsending, for eksempel på papir, dersom Sikker digital posttjeneste skulle bli utilgjengelig.
- Avsendervirksomhetene er ansvarlige for sine data. De må selv vurdere om Sikker digital posttjeneste tilfredsstillere deres krav til sikkerhet før de sender digital post igjennom tjenesten.

5.2 Tekniske tiltak for etterforskning

Når digital post er forsvunnet eller kompromittert vil det bli behov for å etterforske hvor feilen eller lekkasjen har oppstått. Innbyggers datamaskin vil trolig være den mest sårbare og sannsynlige komponenten for digital post på avveie, men det vil også være situasjoner der innbygger aldri har mottatt sin digitale post, som for eksempel ved feilsending fra avsender. Det er viktig å ha gode mekanismer for enkelt å kunne spore og søke etter feil ved slike hendelser.

5.2.1 Unik identifikator for digital post

En unik identifikator som følger en digital postforsendelse helt fra avsender til mottaker er nødvendig for å kunne referere til en og samme forsendelse av digital post over flere systemer. En slik identifikator muliggjør samkjøring av logger fra forskjellige systemer, og sporing av for eksempel feilsendt post. Typisk globale unike identifikatorer kan være:

- IANA Private Enterprise Numbers av typen 1.3.6.1.4.1.879 etterfulgt av egendefinerte nummer.
- Domenenavn som for eksempel no.difi.sdp.2013-02-12.msg1492854.
- A Universally Unique Identifier (UUID) URN Namespace av typen e78a5770-7521-11e2-bcfd-0800200c9a66.

5.2.2 Tilgangskontroll

For meldingsformidler og postkasser skal all tilgang til digital post være kontrollert av tilgangskontrollsystemer. Tilgang til digital post skal kun gis til personlige brukere og

systemkomponenter som er identifisert, autentisert og autorisert for den operasjonen som utføres på den digitale posten.

5.2.3 Kryptografisk sikkerhet

Når digital post befinner seg utenfor et kontrollert miljø, for eksempel i transit fra avsendervirksomhet til postkasse, skal det være kryptografisk sterke metoder for å ivareta konfidensialitet og integritet.

5.2.4 Systemkvitteringer

Når digital post leveres fra en databehandler til en annen skal det returneres signerte systemkvitteringer.

5.2.5 Sporing

All autorisert tilgang til digital post skal logges, og loggen skal være sikret mot uautorisert sletting og endring.

5.2.6 Hinder mot uautorisert tilgang

Det må være sterke mekanismer som hindrer uautorisert tilgang til digital post. Slike tiltak er nødvendig for å sannsynliggjøre at det ikke har vært tilgang utover det som er logget.

5.3 Nivå for akseptabel risiko

Sikkerhetsmekanismene i Sikker digital posttjeneste bør tilpasses avsendervirksomhetenes nivå for akseptabel risiko.

Nivå for akseptabel risiko avgjør i hvilken grad, og for hvilken informasjon avsendervirksomhetene vil benytte Sikker digital posttjeneste.

Akseptabel risiko sier noe om hvor mye ressurser en avsendervirksomhet er villig til å bruke på å forsikre seg om at det ikke vil forekomme brudd på informasjonssikkerheten.

En innbygger vil ha mulighet til å reservere seg dersom de mener sikkerheten i dagens papirløsning er bedre enn ved bruk av Sikker digital posttjeneste.

5.4 Verdier og eiere

Informasjon er den eneste verdien av betydning for avsender og mottaker, andre verdier er utelatt.

Den offentlige virksomheten er behandlingsansvarlig for informasjonen den sender fra seg, og er pålagt å beskytte informasjonen i henhold til lover og regler. Når den digitale posten er gjort tilgjengelig for mottaker vil behandlingsansvaret opphøre, og den digitale posten er innbyggerens eiendom og forvaltes deretter av innbyggeren selv.

5.5 Konsekvenser for brudd på tilgjengelighet

I utgangspunktet vil langvarig brudd på tilgjengeligheten føre til at avsendervirksomheter må sende brevene som ordinær post i stedet for digital post. Dette vil føre til økte kostnader, tap av omdømme, og mindre tillit til løsningen, men utover det vil det ikke være betydelige sikkerhetsmessige konsekvenser. Imidlertid vil utskriftskapasiteten trolig bygges ned over tid,

med den konsekvensen at utsending på papir ikke vil være et reelt alternativ. Vi legger til grunn at den løsningen som lanseres nå vil ha papiirutsending som et alternativ, og at ny vurdering gjøres før utskriftskapasiteten bygges ned.

5.6 Kryptografisk beskyttelse av digital post

Sikker digital posttjeneste skal etablere tillitt mellom avsender og mottaker, slik at avsender med rimelig sikkerhet kan stole på at posten som sendes havner i riktig postkasse, og innbygger kan vite hvem som har sendt posten, og stole på at den er autentisk. Begge parter ønsker å vite at ingen uvedkommende har lest eller endret den digitale posten som formidles mellom dem. Her beskrives løsningen for å sikre integritet og konfidensialitet i overføringen av digital post fra avsendervirksomhetene til innbyggernes postkasser.

Formatet på digitalt post er ikke bestemt, så detaljnivået på den kryptografiske sikringen er heller ikke endelig bestemt. Valg av format vil gi føringer for om signering og kryptering bør være en del av formatet, noe som vil være naturlig for XML-baserte formater, eller om en vil bruke andre protokoller som er helt uavhengig av formatet til det som skal beskyttes.

Beskrivelsen spesifiserer en av de sikringsmetodene som vil tilbys av Sikker digital posttjeneste. Det kan også etableres andre metoder, med høyere eller lavere krav til sikkerhet. Løsningen beskrevet her er tiltenkt å kunne beskytte informasjon av særlig følsomme taushetsbelagte opplysninger, herunder de fleste sensitive personopplysninger, stigmatiserende opplysninger m.v. Eksempelvis opplysninger om sykdom.

5.6.1 Konfidensialitet

Avsendervirksomheten benytter oppslagstjenesten for digital kontaktinformasjon for å få levert innbyggerens digitale postkasseadresse og tilhørende X.509 sertifikat. Postkasseleverandøren må gjøre sertifikatet tilgjengelig for oppslagstjenesten, og det kan enten være et unikt sertifikat tilhørende innbyggeren eller innbyggerens postkasse, eller det kan være postkasseleverandørens virksomhetssertifikat. Løsningen er valgt med tanke på fleksibilitet, der postkasseleverandørene kan konkurrere på sikkerhet, uten at avsendervirksomhetene må endre sine systemer for utsending av digital post. Postkasseleverandøren kan tilby beskyttelse under samme virksomhetssertifikat for alle sine kunder, eller de kan tilby unike sertifikater per innbygger, enten i egen kontroll, eller hvor innbyggeren selv sitter på den private nøkkelen som er nødvendig for å se innholdet. Sertifikatene postkasseleverandøren gjør tilgjengelig må kostnadsfritt kunne valideres opp mot en sertifikatutsteder.

Avsendervirksomheten validerer sertifikatet og benytter dette for å kryptere de symmetriske nøklene som benyttes for å kryptere selve innholdet i den digitale posten. Det vil være behov for å endre algoritmer og protokoller over tid, men i første versjon vil det være PKCS#1 v2.1 som benyttes for asymmetrisk beskyttelse av symmetriske nøkler.

Det sensitive innholdet i en digital forsendelse krypteres med symmetriske nøkler. Disse nøklene genereres tilfeldig og gjenbrukes ikke. Fra starten vil det være AES kryptering i en modus som vil bli spesifisert etter at formatet på den digitale posten er bestemt.

Noe metadata må være tilgjengelig under flytting av digital post fra avsender til mottaker, og denne kan ikke være innenfor det som er kryptert. Selv om denne informasjonen er utenfor det krypterte innholdet, så vil den delvis være beskyttet under overførselen, fordi i tillegg til innholdskryptering vil det være kanalkryptering i form av TLS mellom avsendervirksomheten og meldingsformidleren, og mellom meldingsformidleren og postkasseleverandøren.

5.6.2 Integritet

Det er flere forhold som ivaretas ved integritetsbeskyttelse. Meldingsformidler og postkasseleverandør vil kontrollere og verifisere identiteten til avsender for å hindre uautoriserte avsendere, og for å etablere et trygt sporings- og fakturaregime. Videre kan innbygger være trygg på at posten faktisk er fra den som har utgitt seg for å sende den.

God integritetssikring hindrer at postens innhold eller metadata endres underveis i transporten mellom avsender og mottaker, og sørger for at posten kommer frem til riktig postkasse.

Virksomhetssertifikater er den løsningen som har størst utbredelse og sikrer integritet på best måte, spesielt for autentisering av avsendervirksomheter.

Avsendervirksomheten signerer den digitale posten med sitt eget virksomhetssertifikat. Signaturen dekker både ukryptert metadata som skal være tilgjengelig under formidlingen, inkludert avsenders virksomhetssertifikat, og de skjermingsverdige delene som er kryptert. Det vil være behov for å endre algoritmer og protokoller over tid, men i første versjon vil signaturen være PKCS #1 v1.5 eller v2.1, enten i XML-format sammen med innholdet eller frittstående.

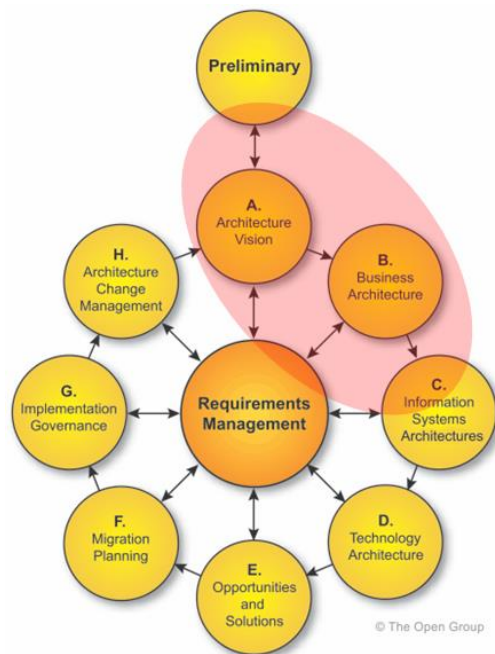
For å sende digital post må en avsendervirksomhet være registrert med organisasjonsnummer hos sentralforvalteren av sikker digital posttjeneste, og må inneha et virksomhetssertifikat som benyttes for å signere all digital post. Meldingsformidler og postkasseleverandører vil validere signaturen, og undersøke om avsendervirksomheten er registrert for utsending av digital post.

Innbyggere kan ha behov for å gjenbruke dokumenter utenfor postkassen, der en tredjepart ønsker å validere ektheten av dokumentet (jamfør eForvaltningsforskriften §10 nr. 5). Et slikt scenario anses som utenfor den digitale posttjenestens område, men kan løses ved at avsender signerer dokumentene som legges i den digitale posten.

Appendiks A. Metode og rammeverk

Arkitekturprosjektet tilstreber å arbeide mest mulig etter TOGAFs arkitekturmetoder og rammeverk, nærmere bestemt med deler av TOGAF som er relevant i denne sammenheng.

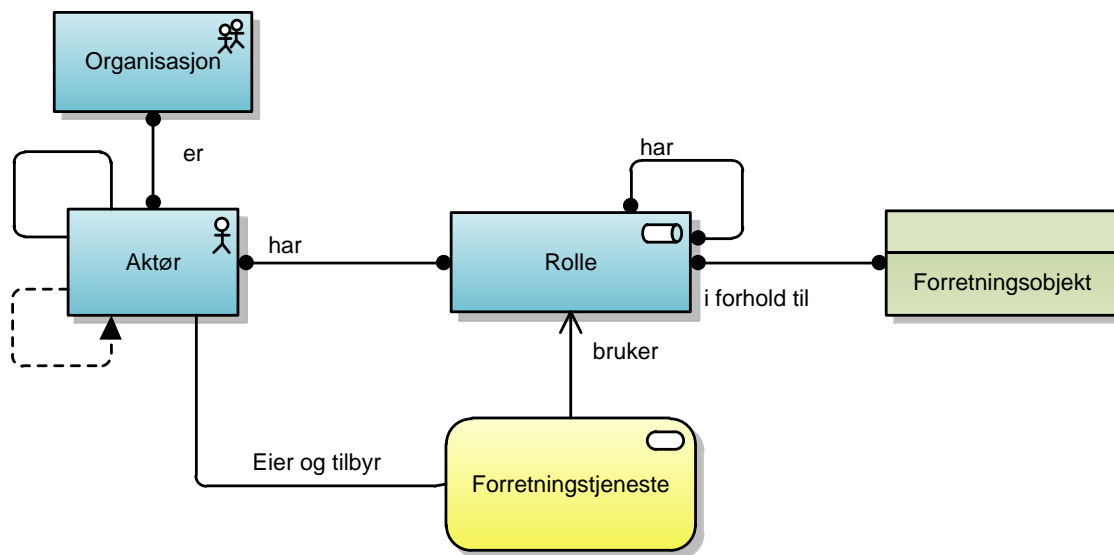
A.1.1 ADM – Architecture Development Method



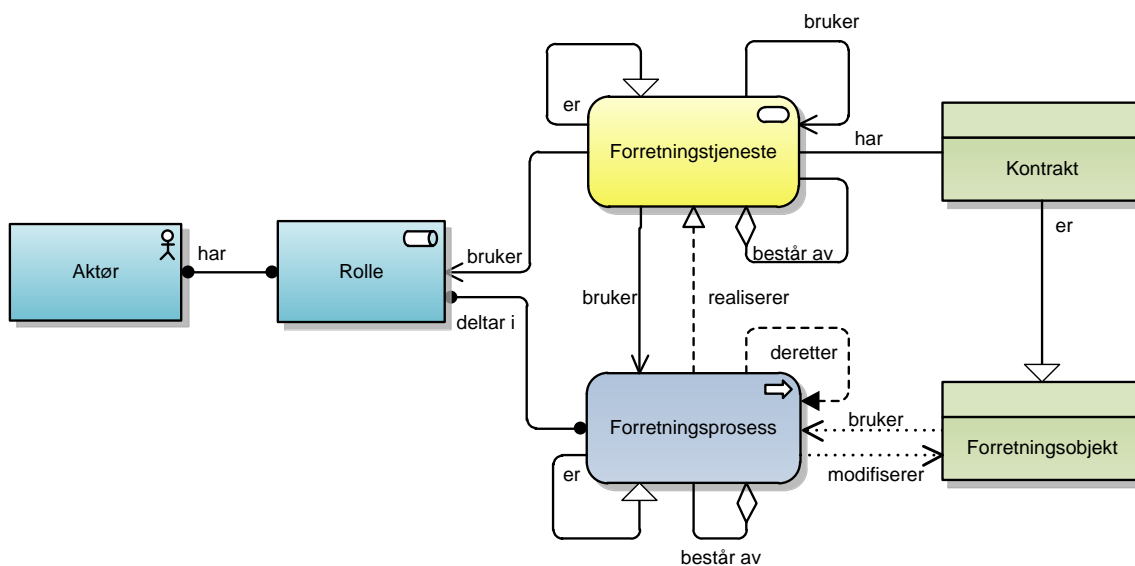
Figur 44: Architecture Development Method

A.1.2 Architecture Content Framework - Content Metamodel

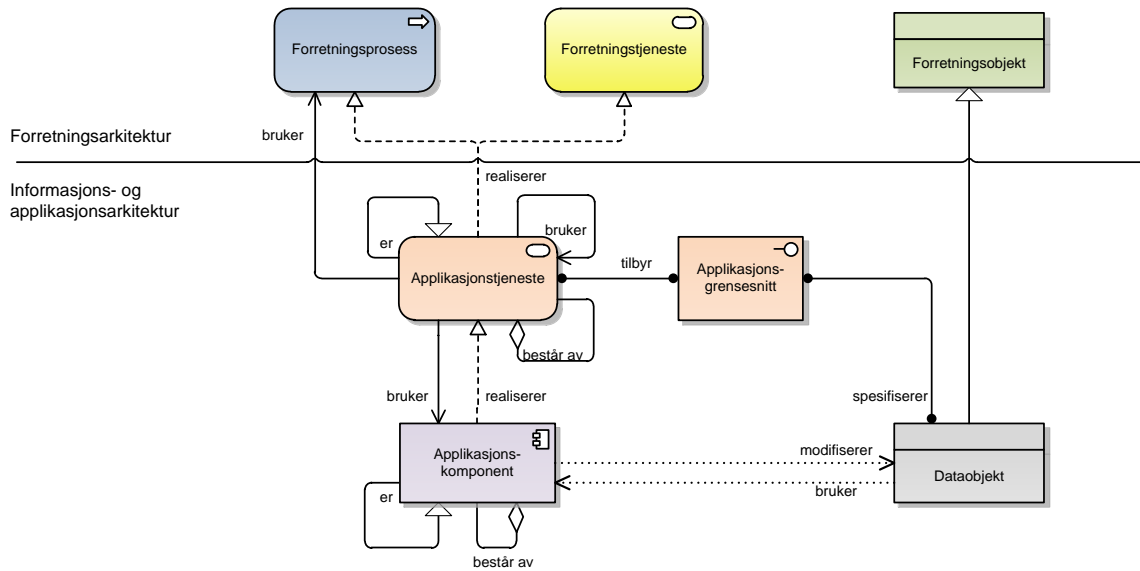
TOGAFs rammeverk har et omfattende modellverk for å beskrive sammenheng mellom komponenter i rammeverket.



Figur 46: Forenklet metamodel - Aktører og roller


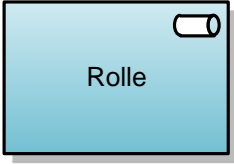
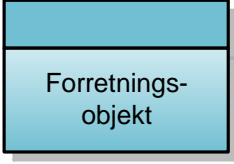



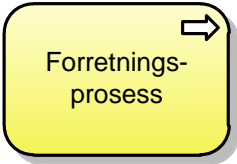

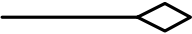
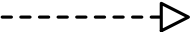
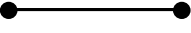
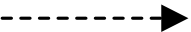

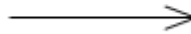

Figur 47: Forenklet metamodel - forretningstjenester og -prosesser



Figur 48: Forenklet metamodel - Informasjons- og applikasjonsarkitektur

A.1.4 Archimate – symbolforklaring

Symbol	Forklaring
 <p>Aktør</p>	An organizational entity that is capable of performing behavior.
 <p>Rolle</p>	The responsibility for performing specific behavior, to which an actor can be assigned.
 <p>Forretnings-objekt</p>	A passive element that has relevance from a business perspective.
 <p>Dataobjekt</p>	A data object is defined as a passive element suitable for automated processing

Symbol	Forklaring
 <p>Forretnings- prosess</p>	<p>A behavior element that groups behavior based on an ordering of activities. It is intended to produce a defined set of products or business services.</p>
 <p>Forretnings- tjeneste</p>	<p>A service that fulfills a business need for a customer (internal or external to the organization).</p>
	<p>The aggregation relationship indicates that a concept groups a number of other concepts.</p>
	<p>The realization relationship links a logical entity with a more concrete entity that realizes it.</p>
	<p>The assignment relationship links active elements (e.g., business roles or application components) with units of behavior that are performed by them, or business actors with business roles that are fulfilled by them.</p>
	<p>The flow relationship describes the exchange or transfer of, for example, information or value between processes, function, interactions, and events.</p>
	<p>The specialization relationship indicates that an object is a specialization of another object.</p>
	<p>The used by relationship models the use of services by processes, functions, or interactions and the access to interfaces by roles, components, or collaborations.</p>
	<p>An association models a relationship between objects that is not covered by another, more specific relationship.</p>