Sikkerhetsarkitektur
Digital postkasse til innbyggere

Versjon: 12. mars 2015

Direktoratet for
forvaltning og IKT

Innholdsfortegnelse

1. Innledning

Digital postkasse til innbyggere er en tjeneste med høye krav til sikkerhet. Digital post kan inneholde følsom informasjon og posten skal kunne arkiveres i tjenesten så lenge innbyggerne ønsker.

Sikkerhetsarkitekturen er en integrert del av arkitekturen som sørger for at posten behandles og oppbevares på en betryggende måte, og passer på at uventede hendelser håndteres kontrollert. Sikkerhetsarkitekturen dekker hele spennet fra katastrofeøvelser med ledelsen og ned til kodelinjene som krypterer posten før den lagres.

Arbeidet med sikkerhetsarkitektur har vært systematisk for å sikre at digital postkasse til innbyggere er egnet for å sende og oppbevare digital post som i dag sendes på papir.

Forankring av sikkerhetsvalg underveis i utviklingen er viktig for å lage en tjeneste med god sikkerhet. Å heve sikkerheten etter en løsning er ferdig er erfaringsmessig dyrt og vanskelig. Sikkerhetsarbeidet har regelmessig vært forankret i sikker post programmet, og viktige tema har vært tatt opp i referansegruppen og styringsrådet for Difis felleskomponenter.

Arbeidet med sikkerhetsarkitektur har tatt utgangspunkt i TOGAF 9 standarden med leveranser som beskrevet i kapittel 21 - Sikkerhetsarkitektur og ADM. Se http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html for detaljer.

Som en del av sikkerhetsarbeidet har det vært gjennomført risiko- og sårbarhetsanalyse i en tidlig fase, før tjenesten var ferdig spesifisert. Dette arbeidet ble blant annet brukt til å skrive en kravspesifikasjon som ble sendt på høring. Resultatet fra risiko- og sårbarhetsanalysen ble sammen med høringssvarene brukt til å jobbe videre med sikkerhetsarkitekturen og lage en endelig kravspesifikasjon. Etter tjenesten var ferdig spesifisert ble det gjennomført en ny risiko- og sårbarhetsanalyse for å forsikre seg om at den ferdige tjenesten kunne settes i produksjon.

Sikkerhetsarkitekturen er som nevnt en integrert del av arkitekturen, og dette dokumentet er en beskrivelse av sikkerhet i forretnings- og informasjonsarkitekturen i tjenesten slik den er i dag.

Formålet er å gi leserne innsikt i tjenestens sikkerhet, slik at de kan få bedre forståelse for hva tjenesten er egnet til. For å få et mer helhetlig bilde kan dette dokumentet leses sammen med arkitekturbeskrivelsen, kravspesifikasjon og risiko- og sårbarhetsanalysene.

Beskrivelse av sikkerhetsarkitekturen er skrevet for de som jobber med digital postkasse til innbyggere internt i Difi, leverandører og de som skal benytte tjenesten til å sende post.

Hvis det er uoverensstemmelser mellom beskrivelsene i dette dokumentet og kontrakter og avtaler, så er det kontraktene og avtalene som gjelder.

2. Forretningsarkitektur

Forretningsarkitekturen beskriver tjenesten på et overordnet nivå, der det forretningsmessige hos aktørene fremheves, uten å gå i detaljer på hvordan tjenesten skal utformes. Sikkerhetsarkitekturen, som beskrevet her, har fokus på det som kan gå galt, og hvilke konsekvenser dette kan ha for aktørene som benytter tjenesten.

2.1. Fysisk miljø

De fysiske miljøene for drift av digital postkasse til innbyggere er hos tredjeparter i Norge og Danmark. Systemene er plassert i datahaller sammen med andre systemer og driftes av leverandører hvor kjernevirksomheten er drift av slike systemer. Krav til og kontroll over driftsmiljøene er ivaretatt i kravspesifikasjonen, og inkluderer områder som:

- Adgangskontrollsystem
- Inntrengningsbeskyttelse
- Alarmsystem og utrykningstid
- Personellsikkerhet
- Strømforsyning
- Kjøling
- Alternativ lokasjon

Driftsmiljøene skal blant annet ha regelmessige katastrofeøvelser og sikkerhetstester. Dette følges opp av sentralforvalter.

2.2. Forretningsmiljø

Avsendervirksomhetene er offentlige virksomheter eller private virksomheter som opererer på vegne av det offentlige. Antall virksomheter som benytter tjenesten er lavt i starten, men tjenesten er klargjort for å håndtere et stort antall avsendervirksomheter. Difi er sentralforvalter og inngår avtale (bruksvilkår) med avsendervirksomhetene. Store virksomheter kan ha flere tekniske integrasjoner mot tjenesten. Det er anledning til å benytte underleverandører for å sende digital post i tjenesten, og da kan flere små virksomheter benytte samme tekniske integrasjon mot systemet.

Mottakerne i systemet er innbyggere som kan identifiseres og autentiseres i ID-porten. Det kreves autentisering på nivå fire for opprette en postkasse. Nedre aldersgrense er begrenset av de e-ID-er som er tilgjengelig i ID-porten. Det er gratis for innbyggerne å motta post, og de kan velge mellom flere kommersielle postkassetilbydere. Det er frivillig for en innbygger å registrere sin postkasse for mottak av offentlig post, og i tillegg kan en innbygger reservere seg mot å få viktig post digitalt fra forvaltningen. Reservasjon gjelder alle digitale postløsninger, og ikke bare digital postkasse til innbyggere.

Meldingsformidleren er et sentralt punkt som alle avsendervirksomheter integrerer seg mot for å benytte tjenesten. Meldingsformidleren tilbys av Posten A/S.

Kommunikasjon mellom meldingsformidler, postkasser og innbyggere foregår over Internett.

Kostnader forbundet med tilpasning av egne systemer og bruk av tjenesten dekkes av avsendervirksomhetene.

Utgifter til investering og drift av løsningen for digital postkasse dekkes innenfor Kommunal og moderniseringsdepartementets gjeldende budsjettrammer.

Avsendervirksomhetene beholder kopi av informasjon som sendes igjennom digital postkasse til innbyggere, slik at dokumenter kan gjenskapes og sendes på nytt til innbyggere som ber om det.

Avsendervirksomhetene er ansvarlig for utsending av post, og må selv vurdere behovet for alternativ utsending, for eksempel på papir, dersom tjenesten skulle bli utilgjengelig.

Avsendervirksomhetene er ansvarlige for sine data. De må selv vurdere om digital postkasse til innbyggere tilfredsstiller deres krav til sikkerhet før de sender digital post igjennom tjenesten.

2.3. Sikkerhetsaktører

De viktigste aktørene er offentlige virksomheter som sender post og innbyggere som mottar post. Disse er igjen avhengig av flere andre aktører som påvirker sikkerheten til den digitale posten.

Aktør	**Beskrivelse**
Sentralforvalter	Den part som er ansvarlig for tjenesten og inngår avtaler med avsendervirksomheter, meldingsformidler og postkasseleverandører. Difi er sentralforvalter.
Avsendervirksomhet	Den som produserer den digitale posten som skal formidles til innbygger. Avsendervirksomheten er behandlingsansvarlig og har ansvar for å beskytte informasjon inntil den er gjort tilgjengelig for innbygger.
Meldingsformidler	Privat virksomhet som leverer teknologitjenester som legger til rette for kommunikasjon, har ansvaret for å sikre og levere data sendt av avsendervirksomhet til innbygger. Meldingsformidler leveres av Posten Norge A/S.
Postkasseleverandør	Private virksomheter som leverer teknologitjenester som legger til rette for kommunikasjon, har ansvar for å sikre, oppbevare og levere data sendt av avsendervirksomhet til innbygger. Postkasseleverandører er e-Boks A/S og Posten Norge A/S.
Innbygger	Mottaker av digital post, og eier av posten etter den er gjort tilgjengelig.
Tilsynsmyndigheter	Datatilsynet og Tilsynet for universell utforming. Disse kan føre tilsyn med løsningen innenfor sine områder.
Utstedere av virksomhetssertifikater	Virksomhetssertifikater benyttes for autentisering av virksomheter. Leverandører av virksomhetssertifikater er Buypass og Commfides.
ID-porten	Innbyggere autentiseres i ID-porten for tilgang til digital post.

2.4. Avtaleforhold

Digital postkasse til innbyggere er underlagt norske lover og regler, også der postkasseleverandører og underleverandører ikke er norske.

Avsendervirksomhetens bruk av digital postkasse til innbyggere er regulert gjennom avtaler (bruksvilkår) med sentralforvalter.

Postkasseleverandørene er regulert gjennom kontrakt med sentralforvalter.

Meldingsformidler er regulert gjennom kontrakt med sentralforvalter.

Innbyggers bruk av digital postkasse til innbyggere er regulert gjennom avtale med valgt postkasseleverandør. I tillegg vil sentralforvalter, i sin avtale med postkasseleverandøren, stille krav som postkasseleverandøren må holde overfor innbyggerne. For eksempel skal innbyggerne kunne lagre post fra det offentlige kostnadsfritt så lenge de ønsker.

Avsendervirksomheten er behandlingsansvarlig for personopplysninger i brev som kunden sender til digital postkasse frem til disse er gjort tilgjengelig for innbygger. Mer informasjon om behandling av personopplysninger er gitt i spesielle bruksvilkår for digital postkasse til innbyggere.

2.5. Sikkerhetspolicy

Difis sikkerhetspolicy, Informasjonssikkerhet i Difi, gir overordnet føringer. Målene for informasjonssikkerhet er:

Mål	**Betydning for digital postkasse til innbyggere**
Konfidensialitet, som innebærer å hindre at uvedkommende får tilgang til informasjon og systemer som skal skjermes.	Innholdet i digital post vedkommer bare avsender og mottaker, og alle andre må ses på som uvedkommende som skal hindres tilgang til innholdet. Det skal også hindres at uvedkommende får tilgang til en del metadata, som for eksempel hvem som er avsender og mottaker, og informasjon om når et brev ble åpnet.
Integritet, som innebærer å sørge for at informasjon og systemer ikke blir endret av uvedkommende og til enhver tid er riktige.	Innholdet i digital post skal ikke kunne endres av andre enn avsender og mottaker. Videre skal informasjon om når brevet ble sendt, når det ble mottatt og åpnet og lignende være korrekt.
Tilgjengelighet, som innebærer å sørge for at informasjon og systemer er tilgjengelige når vi trenger dem.	Avsendervirksomhetene skal kunne levere post til tjenesten når de har behov for det, og innbyggere skal kunne sjekke posten sin når de ønsker det. Videre må brukerstøtte være tilgjengelig når innbyggerne har behov for det, og integrasjon og testmiljø må være tilgjengelig for avsendervirksomhetene.

Meldingsformidler og postkasseleverandører har egne sikkerhetspolicyer for digital postkasse til innbyggere.

2.6. Regelverk og andre dokumenter

Gjeldene regelverk, veiledere og andre dokumenter som har vært relevant i sikkerhetsarbeidet for digital postkasse til innbyggere:

- LOV 1998-03-20 nr 10: Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).
- LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven).
- LOV 2001-06-15 nr 81: Lov om elektronisk signatur (esignaturloven).
- LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger (helseregisterloven).
- LOV 1992-12-04 nr 126: Lov om arkiv [arkivlova].
- LOV 2009-03-06 nr 11: Lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven)
- FOR 1972-03-17 nr 3352: Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen)
- FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger (personopplysningsforskriften)
- FOR 2001-06-29 nr 723: Forskrift om sikkerhetsadministrasjon.
- FOR 2001-07-01 nr 744: Forskrift om informasjonssikkerhet
- FOR 2004-06-25 nr 988: Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Felles løft for elektronisk ID i offentlig sektor.pdf
- Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor.pdf
- Norm for informasjossikkerhet
- Kravspesifikasjon for PKI i offentlig sektor
- På nett med innbyggerne
- Nasjonal strategi for informasjonssikkerhet
- Nasjonal strategi for informasjonssikkerhet - handlingsplan
- Nasjonale felleskomponenter i offentlig sektor

2.7. Verdier og eiere

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

Verdi	Eier	Beskrivelse
Digital post	Avsendervirksomhet	Offentlige virksomheter sitter på informasjon om innbyggere, og noe av denne informasjonen ønskes formidlet til innbyggere i form av digital post. Den offentlige virksomheten har behandlingsansvar for informasjonen, og er pålagt å beskytte informasjonen i henhold til lover og regler.
Digital post	Innbygger	Digital post fra det offentlige, etter den offentlige virksomhetens behandlingsansvar har opphørt. Den digitale posten er innbyggerens eierskap og skal kunne forvaltes deretter av innbyggeren selv.

2.8. Nivå for akseptabel risiko

På den ene siden bør sikkerhetsmekanismene i digital postkasse til innbyggere tilpasses aktørenes nivå for akseptabel risiko, og på den andre siden vil deres nivå for akseptabel risiko avgjøre i hvilken grad, og for hvilken informasjon de vil benytte løsningen. Noen avsendervirksomheter kan velge å ikke bruke løsningen dersom kostnadene og sikkerhetstiltakene overgår behovet de har for å beskytte informasjonen de ønsker å formidle.

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

Aktør	Nivå for akseptabel risiko
Sentralforvalter	Sentralforvalter har et overordnet ansvar for sikkerheten i digital postkasse til innbyggere, og er de som må stå til rette ovenfor innbyggere og resten av forvaltningen dersom det oppstår alvorlige sikkerhetshendelser. > Offentlige virksomheter skal kunne sende og motta dokumenter elektronisk på en sikker måte, slik at dokumentenes konfidensialitet, integritet og autentisitet kan garanteres. Denne uttalelsen fra Nasjonal strategi for informasjonssikkerhet antyder en lav risikovillighet, i alle fall innad i forvaltningen. Sentralforvalter har lagt opp tjenesten for å kunne håndtere særlig følsomme taushetsbelagte opplysninger, herunder de fleste sensitive personopplysninger, stigmatiserende opplysninger m.v. Kravspesifikasjonen til meldingsformidler og postkasseleverandører er tilpasset denne typen informasjon ved å stille krav basert

Aktør	**Nivå for akseptabel risiko**
	på en risiko- og sårbarhetsanalyse, tilbakemeldinger fra offentlige virksomheter og Datatilsynets veiledere.
Avsendervirksomhet	Nivå for akseptabel risiko varierer mye for de forskjellige avsendervirksomhetene. Helse er kanskje den sektoren som har kommet lengst i å spesifisere akseptabelt nivå ved sine beskrivelser i Norm for informasjonssikkerhet. Normen har et delkapittel, "Nivå for akseptabel risiko", som beskriver hva Helse definerer som akseptabel risiko. For konfidensialitet skriver de: > Personer utenfor *virksomheten* uansett ressurser og kunnskap skal ikke kunne få uautorisert *tilgang* til *helse- og personopplysninger*. De mest kompetente miljøene i dag har begrensninger i ressurser og kunnskap, og da er det naturlig å tolke teksten i retning at selv ikke disse skal være i stand til å skaffe seg tilgang. Teksten antyder et ekstremt lavt nivå for akseptabel risiko, der en skulle anta at helsesektoren var villig til å bruke store ressurser på TEMPEST-sikring og andre kostbare sikringstiltak for systemer som håndterer helseopplysninger. Imidlertid ser praksis ut til å være mer balansert og en villighet til å ta større risiko enn det som er uttalt. Hjemmekontor med nivå 4 autentisering er tillatt i Normen, og gir dermed en pekepinn på hvilken risiko som aksepteres.
Meldingsformidler	En privat aktør vil i stor grad sette nivå for akseptabel risiko utfra økonomiske vurderinger, og en offentlig virksomhet vil i stor grad sette nivå for akseptabel risiko utfra omdømmevurderinger. Meldingsformidleren er en privat aktør som har inngått avtale med sentralforvalter. Avtalen inneholder økonomiske sanksjoner dersom de ikke etterlever avtalt informasjonssikkerhet. Meldingsformidleren har tilgang til noe informasjon, slik som avsender og mottaker, men har ikke tilgang til dokumentene som formidles. For all post som sendes vil postkassen validere signaturen og kvittere tilbake til avsender. Brudd på formidlingens integritet eller tilgjengelighet vil derfor oppdages og følges opp.
Postkasse	Nivå for akseptabel risiko til postkassene vil i stor grad være gitt av de økonomiske konsekvensene ved et sikkerhetsbrudd. De økonomiske konsekvensene avhenger i stor grad av sentralforvalters avtalefestede sanksjonsmuligheter på den ene siden, og omdømmetap som fører til tap av kunder på den andre. Avtalen mellom sentralforvalter og postkasseleverandør inneholder økonomiske sanksjoner dersom ikke avtalt informasjonssikkerhet etterleves.

Aktør	Nivå for akseptabel risiko
Innbygger	Hos innbyggerne vil nivå for akseptabel risiko variere så mye at det er vanskelig å gi en dekkende beskrivelse. En innbygger vil ha mulighet til å reservere seg dersom de mener sikkerheten i dagens papirløsning er bedre.

2.9. Konsekvenser ved sikkerhetsbrudd

I utgangspunktet vil langvarig brudd på tilgjengelighet av tjenesten 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 papirutsending er et alternativ, og at ny vurdering gjøres før utskriftskapasiteten bygges ned.

Det er avsendervirksomhetene som best kjenner konsekvensene av sikkerhetsbrudd relatert til deres kommunikasjon med innbyggerne. Følgende informasjon er trukket ut i fra møter med noen avsendervirksomheter:

- Hvis systemet blir utilgjengelig over lengre tid så vil det føre til større kostnader for avsendervirksomhetene, ettersom de må gå over til en dyrere forsendelse på papir.

- Brev som ikke kommer frem, eller kommer frem noen dager for sent frem, gir store ulemper for mottageren. I tillegg krever det ekstra ressurser på brukerstøtte og gir et dårlig omdømme.

- Brev som endres eller ikke kommer frem kan føre til tap av liv og helse.

- Store mengder digital post på avveie vil gi et alvorlig tap av omdømme for forvaltningen, samt at både økonomi, liv og helse kan settes i fare hos innbyggere som får sine digitale brev eksponert.

2.10. Feilsøking og etterforskning

Når digital post er forsvunnet eller kompromittert vil det bli behov for å finne ut 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 eller feil hos meldingsformidler eller postkasseleverandører. Det er viktig å ha gode mekanismer for enkelt å kunne spore og søke etter feil ved slike hendelser. Ved mistanke om en kriminell handling skal logger, kvitteringer og annen informasjon ha tilstrekkelig sikring til å kunne benyttes i en rettssak.

Tiltak	Beskrivelse
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 ett og samme digitale brev over flere systemer. En slik identifikator muliggjør samkjøring av logger fra forskjellige systemer, og spo-

Tiltak	Beskrivelse
	ring av for eksempel feilsendt post. Typisk globale unike identifikatorer kan være IANA sine 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*, eller A Universally Unique IDentifier (UUID) URN Namespace av typen *e78a5770-7521-11e2-bcfd-0800200c9a66*. En digital postforsendelse består av flere elementer hvor hver av disse har sin unike identifikator.
Tilgangskontroll	For meldingsformidler og postkasser skal all tilgang til digital post være kontrollert av tilgangskontrollsystemer. Tilgang til digital post gis kun til personlige brukere og systemkomponenter som er identifisert, autentisert og autorisert for den operasjonen som utføres på den digitale posten.
Kryptografisk sikkerhet	Når digital post befinner seg utenfor et kontrollert miljø, for eksempel i transitt fra avsendervirksomhet til postkasse, er det kryptografisk sterke metoder for å ivareta konfidensialitet og integritet.
Systemkvitteringer	Når digital post leveres fra en databehandler til en annen returneres det signerte systemkvitteringer.
Sporing	All autorisert tilgang til digital post logges, og loggen er sikret mot uautorisert sletting og endring. Alle tidsangivelser har høy grad av nøyaktighet, slik at logger fra flere systemer kan samkjøres.
Hinder mot uautorisert tilgang	Det er sterke mekanismer som hindrer uautorisert tilgang til digital post. Slike tiltak er etablert og nødvendig for å sannsynliggjøre at det ikke har vært tilgang utover det som er logget.

2.11. Katastrofe- og kontinuitetsplan

Ved en katastrofe må sentralforvalter håndtere media og følge opp avsendervirksomheter og leverandørene av digital postkasse til innbyggere. Meldingsformidler og postkasseleverandører har katastrofe- og kontinuitetsplaner, og skal øve og revidere disse regelmessig i henhold til kontraktene. Sentralforvalter har ikke en egen katastrofe- og beredskapsplan for digital postkasse til innbyggere, men benytter felles rutiner for alle felleskomponentene.

Konkurs eller oppsigelse av kontraktene for meldingsformidler og postkasseleverandørene vil være en betydelig hendelse for sentralforvalter. Dette er regulert i kontraktene med økonomiske garantier og mulighet for å overføre arkivert post til andre leverandører.

2.12. Tillitskjeder

Avsendervirksomheter vil kun sende digital post igjennom digital postkasse til innbyggere dersom de har tillit til at den digitale posten blir tilstrekkelig beskyttet. På samme måte vil innbyggerne kun benytte tjenesten dersom de har tillit til løsningen.

Tjenesten vil kun ta imot digital post fra en avsendervirksomheter som er godkjent, og levere denne videre til mottaker dersom tjenesten har tillit til at det er riktig mottaker.

Avsendervirksomheter og innbyggere kan både anta og forvente at deres digitale post er godt sikret. Det er blant annet kommunisert i *På nett med innbyggerne*:

> Folk og bedrifter skal få post fra forvaltningen i en sikker, digital postkasse, og få varsling på sms og e-post når de har mottatt digital post.

Hva denne tilliten bygger på beskrives mer konkret i tabellen nedenfor.

Subjekt	**Objekt**	**Tillit**
Innbygger	Postkasseleverandør	En innbygger kan stole på at post fra det offentlige havner i postkassen ved informasjon gitt i media og på offentlige nettsider. Tillit til at digital post er tilstrekkelig beskyttet er delvis etablert igjennom lovverket, ved at digital postkasse til innbyggere er underlagt personopplysningsloven, og at datatilsynet kan føre tilsyn med løsningen. I tillegg vil avtalen som inngås med den valgte postkasseleverandøren inneholde elementer som kan gi tillit. Innbyggeren kan stole på at han befinner seg i sin postkasse ved den grønne bjelken i nettleseren (TLS med extended validation). Videre kan innbyggeren stole på at ingen andre kan logge seg inn på hans postkasse ved den tilliten som allerede er etablert i ID-porten og tilhørende e-ID-leverandører. Kjente angrep og dårlig kunnskap om hvordan beskytte sin egen datamaskin kan gi redusert tillit til løsningen.
Postkasseleverandør	Innbygger	Postkasseleverandøren kan stole på at det er riktig innbygger som logger seg inn ved den tillit som allerede er etablert ved bruk av ID-porten og tilhørende e-ID-leverandører.
Offentlig virksomhet	Kontakt- og reservasjonsregisteret	En offentlig virksomhet kan stole på informasjon fra kontakt- og reservasjonsregisteret på grunn av de avtaler (bruksvilkår) som er inngått med sentralforvalter.

Subjekt	Objekt	Tillit
Offentlig virksomhet	Meldingsformidler/ postkasseleverandør	En offentlig virksomhet kan stole på at posten kun gjøres tilgjengelig for riktig mottaker på bakgrunn av de avtaler, risiko- og sårbarhetsanalyser og øvrig sikkerhetsdokumentasjon som er gitt.
Meldingsformidler/Postkasseleverandør	Offentlig virksomhet	Meldingsformidler og postkasseleverandør kan stole på at digital post kommer fra en gyldig avsender ved å sjekke organisasjonsnummeret opp mot registrerte avsendere hos sentralforvalteren, og validere virksomhetssignaturen på forsendelsen.
Sentralforvalter	Postkasseleverandør	Sentralforvalteren etablerer tillit til postkasseleverandørene igjennom kontrakter og avtalt *Service Level Agreement*, og oppfølging av disse. Sertifiseringer, sikkerhetstester, katastrofeøvelser, befaringer, sikkerhetsmøter med mer har gitt, og vil gi tillit.
Sentralforvalter	Offentlig virksomhet	Ved registrering av offentlige virksomheter som avsendervirksomheter etableres tillit i samarbeidsportalen der den offentlige virksomheten aksepterer bruksvilkårene. Virksomhetens organisasjonsnummer kan sjekkes opp mot autorative registre.

2.13. Sikkerhetsrelaterte forretningsprosesser

Sentralforvalter har et overordnet ansvar for digital postkasse til innbyggere. Nedenfor er en liste over forretningsprosesser hvor sikkerhet inngår som et sentralt element.

Prosess	Beskrivelse
Tilsetting	Sentralforvalter følger statens regulativer når de ansetter folk for å håndtere oppgaver relatert til digital postkasse til innbyggere. Det er ikke identifisert oppgaver hos sentralforvalter som krever tilsettingsprosedyrer utover standard tilsetting i staten.
Ekspedere post	Detaljert under virksomhetsprosesser i arkitekturbeskrivelsen.
Formidle post	Detaljert under virksomhetsprosesser i arkitekturbeskrivelsen.
Oppbevare post	Detaljert under virksomhetsprosesser i arkitekturbeskrivelsen.
Lese post	Detaljert under virksomhetsprosesser i arkitekturbeskrivelsen.

Prosess	Beskrivelse
Bytte postkasse og flytte post	Detaljert under virksomhetsprosesser i arkitekturbeskrivelsen.
Forvaltning av sikkerhetskrav	Vedlikeholde krav til sikkerhet i tråd med beste praksis. Algoritmer og nøkkellengder må for eksempel endres over tid.
Forvaltning av krav til validering av post	Vedlikeholde krav til validering av postforsendelsen. Dokumenttyper og grensesnitt endres over tid, og tjenesten for å validere forsendelsen endres tilsvarende.
Godkjenning av avsendere	Vedlikeholde liste over avsendere, inkludert underleverandører, som er autorisert for å sende post.
Godkjenning av leverandører	Kontroll med meldingsformidler og postkasseleverandører, inkludert deres driftsleverandører og andre underleverandører de benytter.
Registrering av innbyggers kontaktinformasjon	Innbyggere oppdaterer epost, telefonnummer og reservasjonsstatus. Postkasseleverandørene oppdaterer postkasseadresse og sertifikat som en del av innbyggers kontaktinformasjon.
Avtaleoppfølging	Kontraktene mellom sentralforvalter, meldingsformidler og postkasseleverandører inneholder mange krav der det skal være regelmessig oppfølging. For eksempel penetrasjonstesting, katastrofeøvelser og lignende.
Integrasjon og test	Gode prosesser for integrasjon og test er viktig for at avsendervirksomheter skal kunne oppdage feil før de går i produksjon. Feilsøking i et produksjonsmiljø er utfordrende på grunn av svært begrensede tilganger for de som skal feilsøke. Dersom feilen kan gjenskapes i et testmiljø vil det kunne bidra til raskere feilretting.

2.14. Tilkoblede systemer utenfor tjenesten

Digital postkasse til innbyggere vil nødvendigvis avhenge av andre systemer, både private og offentlige, som er nødvendige for å levere tjenesten. ID-porten og kontakt- og reservasjonsregisteret er listet opp som systemer utenfor tjenesten, fordi de ikke er en del av digital postkasse til innbyggere, selv om de er kontrollert av Difi.

System	Beskrivelse
ID-porten	ID-porten og tilhørende e-ID-leverandører brukes til identifisering og autentisering av innbyggere. Kvaliteten på denne tjenesten er essensiell for digital postkasse til innbyggere. Ved utilgjengelighet på ID-porten vil innbygger miste tilgang til digital post. Feil autentisering kan gi uautorisert tilgang til digital post.
Oppslagstjeneste for kontaktinformasjon	Avsendervirksomhetenes grensesnitt mot kontakt- og reservasjonsregisteret. Ved utilgjengelighet i oppslagstjenesten vil avsendere være forhindret fra å sende post.
Kontakt- og reservasjonsregister	Kontakt- og reservasjonsregister holder varslingsadresser, og adresse for innbyggerens digitale postkasse, i tillegg til mottakers sertifikat (enten personlig eller postkassens virksomhetsserti-

System	Beskrivelse
	fikat). Videre inneholder registeret oversikt over innbyggere som har reservert seg mot digital post fra det offentlige. I registeret er innbyggere enten reservert eller ikke reservert. For å oppnå ønsket nivå av tilgjengelighet kan det, for noen avsendervirksomheter, være ønskelig å holde en lokal kopi av registret. Feil i registeret kan føre til at innbygger ikke varsles om post, eller at posten leveres til feil mottaker.
Navnetjenester (DNS)	Navneoppslag på Internett brukes til å rute trafikken til riktig mottaker (IP-adresse). Feil eller utilgjengelighet vil føre til at digital post ikke sendes til riktig aktør.
Sertifikattjenester	Virksomhetene identifiseres og autentiseres igjennom virksomhetssertifikater, og dermed er leverandørene av disse av betydning for digital postkasse til innbyggere. For eksempel vil mangel på OCSP og revokeringslister føre til at avsendervirksomhetene ikke kan validere mottakers sertifikat.
Tilbyder av Internett	Digital postkasse til innbyggere avhenger av Internett, både for levering fra avsendervirksomhet til meldingsformidler og postkasse, og fra postkasse til innbyggere. Nedetid på Internett fører til nedetid på digital postkasse til innbyggere.
Klokkesynkronisering (NTP)	Samkjøring av logger, alarmer og lignende krever korrekt tid på de involverte serverne. Feil tid kan føre til at digital post blir avvist, eller at post som skulle vært avvist kommer igjennom.
Oppdateringsservere	Anti-virus, IDS, IPS, sikkerhetspatcher og flere andre systemer er avhengig av regelmessig oppdatering for å holde optimalt sikkerhetsnivå. Utilgjengelighet eller manipulerte oppdateringer kan få alvorlige konsekvenser for digital postkasse til innbyggere.
Epost (SMTP/POP)	Epostserver for levering av varsel. Varsling utføres av postkasseleverandørene, men deler av infrastrukturen ligger utenfor deres kontroll.
SMS	Tekstmeldingstjeneste for levering av varsel. Varsling utføres av postkasseleverandørene, men deler av infrastrukturen ligger utenfor deres kontroll.

3. Informasjonsarkitektur

Informasjonsarkitekturen handler om hvilken informasjon som eksisterer i tjenesten og hvordan den behandles. Beskrivelse av sikkerhetsarkitekturen fokuserer på hva som kan gå galt om informasjonen kommer på avveie, blir endret eller utilgjengelig.

3.1. Klassifisering av informasjon

Informasjon i løsningen er klassifisert etter konfidensialitet, integritet og tilgjengelighet. Tilbakemeldingene fra avsendervirksomhetene har i stor grad vært rettet mot konfidensialitet og i mindre grad rettet mot integritet og tilgjengelighet. Papirpost som sendes i dag har sjelden integritetssikring i form av vannmerket papir eller lignende. Postgang på papir tar tid, og noe post forsvinner uten at avsender får tilbakemelding.

3.1.1. Konfidensialitet

Basert på tilbakemeldinger fra noen store avsendervirksomheter deles informasjon i fem kategorier:

Kategori	**Beskrivelse**
1	Opplysninger som er egnet til å oppspore trusselutsatte personer, samt andre opplysninger hvor kompromittering i særlig grad er egnet til å volde betydelig skade. Adressen til personer med adressesperring i folkeregisteret er gradert strengt fortrolig etter beskyttelseinstruksen, jf. folkeregisterforskriften § 9-5. Et tilsvarende beskyttelsesbehov må antas å gjelde også for andre opplysninger om den trusselutsatte, i den grad aktuelle trusselaktører (forfølgeren) vil ha nytte av opplysningene for å oppspore personen og realisere trussel.
2	Særlig følsomme taushetsbelagte opplysninger, herunder de fleste sensitive personopplysninger, stigmatiserende opplysninger m.v. Eksempelvis opplysninger om sykdom. Sensitive personopplysninger, jf. pol § 2 nr 8, vil i all hovedsak høre hjemme i kategori 2, selv om unntak finnes. Eksempelvis kan opplysninger om straffbare forhold være offentlige og omfattet av innsynsrett, jf. veileder til offentleglova s 53 annet avsnitt og s 81-83. Datatilsynet skriver i sin veileder i risikovurdering, pkt 4.3, følgende: «Til **hjelp** i arbeidet med å anslå taps- eller skadepotensial er det aktuelt å avdekke om personopplysningene er *sensitive*. Dette begrepet skal **ikke** oppfattes som en sikkerhetsgradering i seg selv.» (Difis uthevinger).
3	Andre taushetsbelagte opplysninger, eksempelvis opplysninger om økonomiske forhold, jf. forvaltningsloven § 13 og tilsvarende bestemmelser i særlover.
4	Opplysninger omfattet av taushetsrett (men offentlighet *kan* praktiseres), jf. offentleglova § 3, jf. § 11 og unntakshjemler i kapittel 3 (§ 14-27)

Kategori	Beskrivelse
5	Opplysninger omfattet av allmennhetens innsynsrett, jf. offentleglova § 3, hovedregelen

Det bemerkes at alle opplysninger i kategori 1, 2 og 3 er taushetsbelagte.

3.1.2. Integritet

For integritet brukes følgende kategorier:

Kategori	Beskrivelse
Høy	Sterk integritet som kan etterprøves av uavhengig part.
Middels	Middels sterk integritet der tillit mellom aktørene er tilstrekkelig for etterprøving.
Lav	Ingen særlige behov for integritetssikring.

3.1.3. Tilgjengelighet

Tilgjengelighet og levetid for informasjon gis ved tekstlig beskrivelse.

3.2. Informasjonselementer

Informasjon i digital postkasse til innbyggere er plassert i følgende kategorier:

Informasjonselement	Konfidensialitet	Integritet	Tilgjengelighet
Dokumentpakke (inkludert signatur og manifest)	1-5 (alle behandles som 2)	Høy	Så lenge innbygger har en konto, og ikke aktivt har slettet posten. I rimelig tid etter dødsfall eller avslutning av konto.
Kryptert dokumentpakke	4	Lav (feil vil oppdages)	Til den er dekryptert og lagret under annen beskyttelse. Maks levetid for kryptert dokumentpakke er gitt av sertifikatet den er kryptert med
Digital post (kryptert dokumentpakke, varslings informasjon, adressering med mer)	3 (Kombinasjon avsender og mottaker kan være følsom)	Høy	Under transport
Leveringskvittering	4 (Inneholder kun unik identifikator som knytter den til opprinnelig post)	Middels	Postkasse og meldingsformidler lagrer den til den er levert, mottaker av kvittering

Informasjonselement	**Konfidensialitet**	**Integritet**	**Tilgjengelighet**
			lagrer den så lenge de ønsker
Åpningskvittering	4 (Inneholder kun unik identifikator som knytter den til opprinnelig post)	Middels	Postkasse og meldingsformidler lagrer den til den er levert, mottaker av kvittering lagrer den så lenge de ønsker
Feil	3 (Meldingen inneholder feiltype og detaljer som kan inneholde følsom informasjon)	Middels	Postkasse og meldingsformidler lagrer den til den er levert, mottaker av kvittering lagrer den så lenge de ønsker
Varsling feilet	3 (Meldingen inneholder beskrivelse som er et tekstfelt som kan inneholde følsom informasjon)	Middels	Postkasse og meldingsformidler lagrer den til den er levert, mottaker av kvittering lagrer den så lenge de ønsker
Mottakskvittering	4 (Inneholder kun unik identifikator som knytter den til opprinnelig post)	Middels	Postkasse og meldingsformidler lagrer den til den er levert, mottaker av kvittering lagrer den så lenge de ønsker
Returpostkvittering	4 (Inneholder kun unik identifikator som knytter den til opprinnelig post)	Middels	Postkasse og meldingsformidler lagrer den til den er levert, mottaker av kvittering lagrer den så lenge de ønsker
Flyttet digital post	3 (Kombinasjon avsender og mottaker kan være følsom)	Høy	Inntil leveringskvittering er mottatt fra ny postkasse
Liste over gyldige avsendere	5 (Hvilke offentlige virksomheter som benytter tjenesten, og hvem de benytter som underleverandører er ikke taushetsbelagt)	Høy	Gyldige avsendere er tilgjengelig for meldingsformidler og postkasseleverandører. Historiske data gjøres ikke tilgjengelig.

Informasjonselement	Konfidensialitet	Integritet	Tilgjengelighet
Loggdata relatert til innbyggers bruk av postkassen	5	Middels	Avtale mellom innbygger og postkasseleverandør.Ikke kravsatt av sentralforvalter.
Loggdata relatert til sikkerhet og etterforskning	3 (Loggen inneholder ikke innbyggers post, men kan inneholde mye metadata, slik som avsender og mottaker, tidspunkt for åpning etc.)	Middels	Tilstrekkelig lenge. Eksakt lagringstid er ikke definert.
Loggdata relatert til fakturering	4	Middels	Tilstrekkelig lenge.
Sikkerhetskopi av digital post	2	Høy	Kravet var 30 dager, men det er akseptert lagring av sikkerhetskopi i 70 dager

3.3. Oppbevaring av verdier

I forretningsarkitekturen er digital post identifisert som eneste verdi av betydning. Digital post eies av avsendervirksomhet og innbygger, men behandles av flere aktører.

Verdi	Oppbevares av	Beskrivelse
Digital post	Avsendervirksomhet	Digital post opprettes av avsender for å leveres til innbygger.
Digital post	Meldingsformidler	Digital post oppbevares av meldingsformilder på vegne av avsender i den hensikt å transportere den videre. Meldingsformidler har kun behov for den informasjon som er nødvendig for å levere posten, samt nødvendig informasjon for fakturering og bruksstatistikk. Meldingsformidler har ikke behov, eller mulighet, for å se innholdet.
Digital post	Postkasseleverandør	Oppbevarer posten for avsender inntil den er gjort tilgjengelig for innbygger, og deretter oppbevares posten for innbygger, så lenge innbygger ønsker det.
Digital post	Innbygger	Innbygger eier posten etter den er gjort tilgjengelig, og kan da laste ned,

Verdi	Oppbevares av	Beskrivelse
		skrive ut og slette posten. Hva innbygger gjør med posten er utenfor det offentliges ansvar.

3.4. Logging

Det er viktig å kunne følge opp en hendelse der digital post ikke blir levert som forventet. Når det oppstår en feil er det viktig at ikke mange parter skylder på hverandre. Tjenesten er lagt opp slik at en alltid skal kunne identifisere hvor det feiler, og det skal ikke være mer enn to parter som er ansvarlig for å finne og rette feilen. Nedenfor er logghendelser relatert til sikkerhet i forbindelse med levering av digital post beskrevet.

Aktørene har i tillegg mange andre logger som er viktig for sikkerheten, slik som tilgangskontroll, autorisering av personell, sikkerhetsoppdatering, produksjonssetting, etc. Logging av slike hendelser er avtalt i kontrakt med leverandørene og beskrives ikke her.

Aktør	Hendelse
Sentralforvalter	Avsender aksepterer bruksvilkår for digital postkasse til innbyggere
Sentralforvalter	Avsender autorisert for bruk av digital postkasse til innbyggere
Sentralforvalter	Avsender mistet autorisasjon for bruk av digital postkasse til innbyggere
Sentralforvalter	Informasjon om autorisert(e) avsender(e) overført til meldingsformidler eller postkasseleverandør
Sentralforvalter	Faktureringsgrunnlag mottatt fra meldingsformidler
Sentralforvalter	Avsendervirksomhet fakturert
Sentralforvalter	Mottatt betaling fra avsendervirksomhet
Sentralforvalter	Mottatt faktura fra meldingsformidler eller postkasseleverandør
Sentralforvalter	Betalt meldingsformidler eller postkasseleverandør
Avsendervirksomhet	Kontaktinformasjon hentet fra kontakt- og reservasjonsregisteret
Avsendervirksomhet	Digital post levert til meldingsformidler
Avsendervirksomhet	Transportkvittering mottatt fra meldingsformidler
Avsendervirksomhet	Leveringskvittering mottatt fra postkasseleverandør
Avsendervirksomhet	Varsling feilet mottatt fra postkasseleverandør
Avsendervirksomhet	Feilmelding mottatt fra postkasseleverandør
Avsendervirksomhet	Åpningskvittering mottatt fra postkasseleverandør
Meldingsformidler	Digital post mottatt fra avsendervirksomhet
Meldingsformidler	Transportkvittering sendt til avsendervirksomhet
Meldingsformidler	Digital post levert til postkasseleverandør
Meldingsformidler	Transportkvittering mottatt fra postkasseleverandør

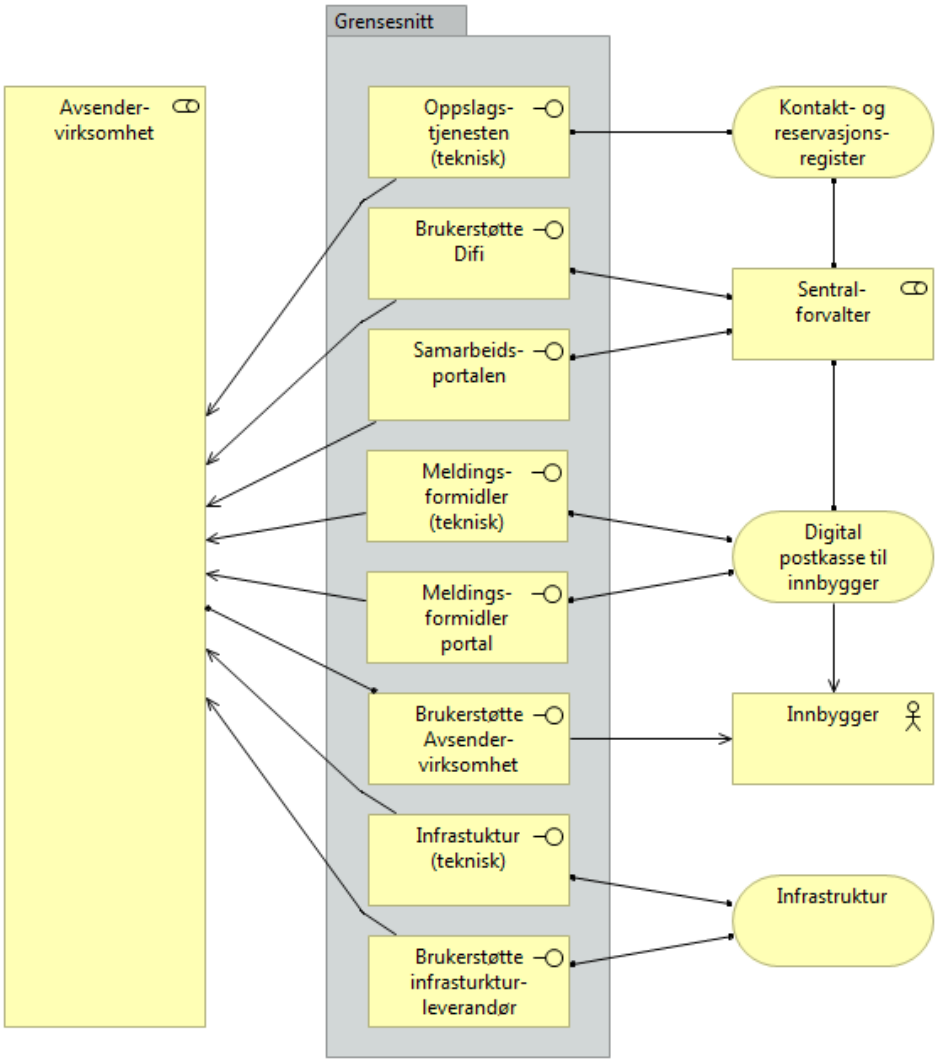
Aktør	Hendelse
Meldingsformidler	Melding til avsender mottatt fra postkasseleverandør (leveringskvittering, varsling feilet, feilmelding eller åpningskvittering)
Meldingsformidler	Transportkvittering levert til postkasseleverandør
Meldingsformidler	Melding levert til avsendervirksomhet
Meldingsformidler	Transportkvittering mottatt fra avsender
Postkasseleverandør	Digital post mottatt fra meldingsformidler
Postkasseleverandør	Transportkvittering levert til meldingsformidler
Postkasseleverandør	Melding til avsender levert til meldingsformidler (leveringskvittering, varsling feilet, feilmelding eller åpningskvittering)
Postkasseleverandør	Transportkvittering mottatt fra meldingsformidler
Postkasseleverandør	Innbygger autentisert i ID-porten
Postkasseleverandør	Brukerhendelse (logget inn, logget ut, åpnet post, slettet post, flyttet post, etc.)

3.5. Brukerscenarioer

Avsendere og mottakere av digital post er de som bruker tjenesten. Feil som oppstår i løsningen skal, så langt det lar seg gjøre, kunne identifiseres og følges opp av disse to aktørene. Deres grensesnitt mot tjenesten er beskrevet nedenfor.

3.5.1. Grensesnitt og feilsituasjoner hos avsendervirksomheten

Feil som oppstår i digital postkasse til innbyggere må oppdages og håndteres på en forsvarlig måte. Noen feil oppdages lett og kan håndteres automatisk, slik som feilet varsling av innbygger. Andre feil vil ikke oppdages før innbyggeren leser brevet, slik som for eksempel et feiladressert brev. Figuren nedenfor viser grensesnitt hvor avsendervirksomheten kan bli oppmerksom på feil. Interne feil hos avsendervirksomheten som oppdages og rettes uten ekstern kontakt er utelatt.

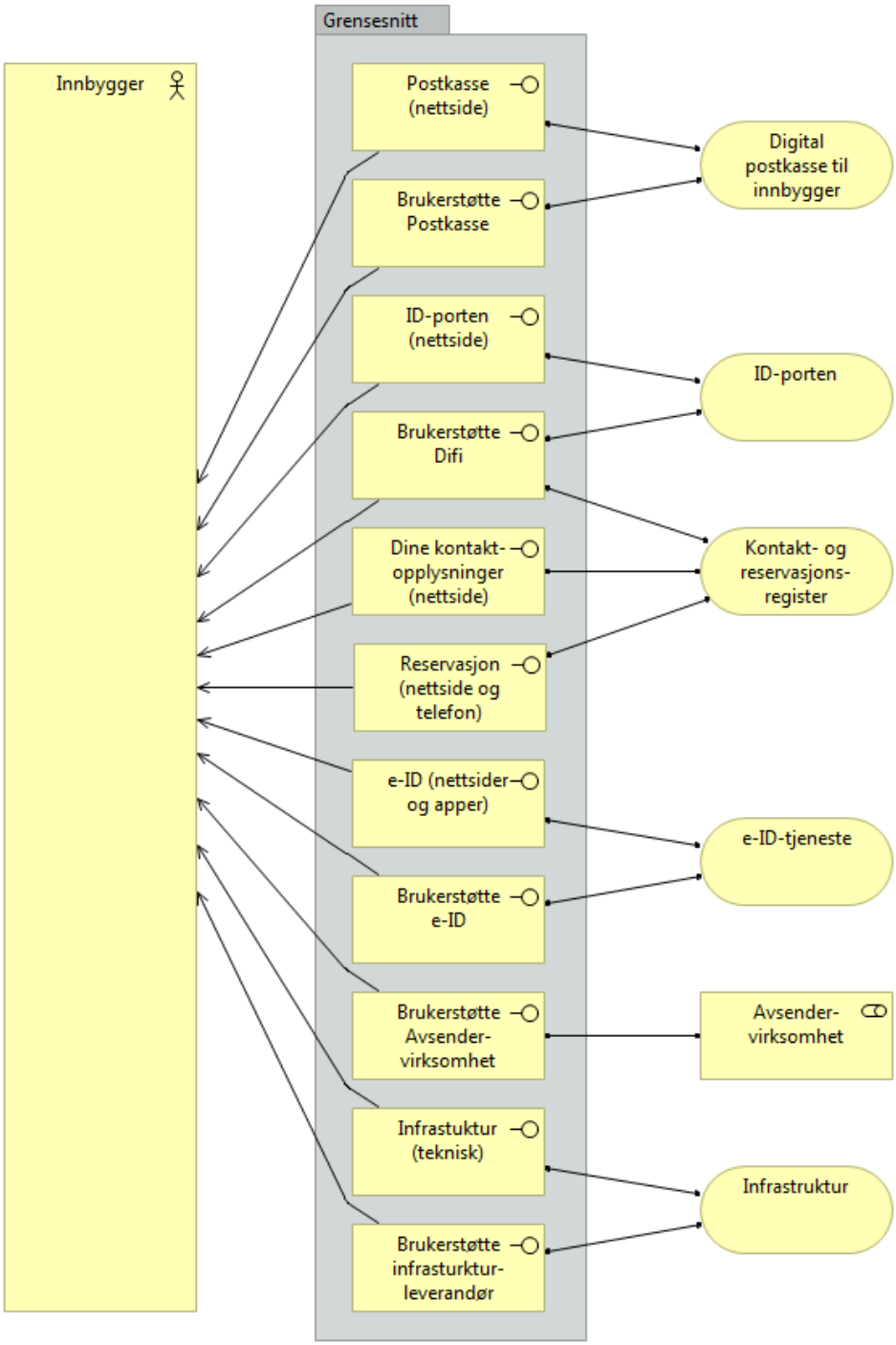


Grensesnitt	**Beskrivelse**
Oppslagstjenesten (teknisk grensesnitt)	Grensesnitt for å hente innbyggers kontaktinformasjon. Feil i informasjonen kan føre til at brev sendes til feil person, eller ikke blir varslet om mottatt post. Utilgjengelighet fører til at post ikke kan sendes.
Brukerstøtte hos Difi	Ved feil i tjenestene som avsendervirksomheten ikke kan håndtere selv skal de kontakte brukerstøtte hos Difi. For eksempel er manglende leveringskvittering noe som ikke skal forekomme, og grunn til å kontakte Difi.
Samarbeidsportalen	Difi tilbyr en samarbeidsportal hvor det vil informeres om feil i løsningene. For eksempel kan nedetid hos en av postkasseleverandørene kommuniseres her. Samarbeidsportalen gir mulighet til å legge inn kontaktinformasjon for virksomheten, slik at Difi kan ta kontakt ved alvorlige feil i løsningen.
Meldingsformidler (teknisk grensesnitt)	Digital post formidles i dette grensesnittet. Her er kan avsenderen motta melding om feil. For eksempel ugyldig signatur på forsendelsen, varsling feilet, intern feil hos leverandøren, etc. I til-

Grensesnitt	Beskrivelse
	legg må manglende transportkvittering og leveringskvittering anses som en feil og følges opp av avsendervirksomheten.
Meldingsformidler portal	Meldingsformidler har en portal hvor meldinger kan følges opp, og hvor det kan gis informasjon om feil. Det er ikke påkrevd at avsendervirksomheten må forholde seg til portalen for å bli informert om feil.
Brukerstøtte hos Avsendervirksomhet	Normalt tilbyr avsendervirksomheten en brukerstøtte for innbyggere de sender post til. Her kan innbygger ta kontakt i forbindelse med post de har problemer med. Brukerstøtte hos Difi kan også ta kontakt med brukerstøtte hos virksomheten på vegne av innbyggeren.
Infrastruktur (tekniske grensesnitt)	Avsendervirksomheten har en infrastruktur som er nødvendig for å sende digital post, slik som internett, navnetjenester (DNS), klokkesynkronisering (NTP) og sertifikattjenester (OCSP, CRL). Disse kan feile eller være utilgjengelig, og medføre feil i ekspedering av digital post. Andre tjenester kan også skape problemer dersom de er utilgjengelig eller ikke satt opp riktig, slik som brannmur, lastbalansering, viruskontroll, sikkerhetsoppdatering og så videre.
Brukerstøtte hos leverandør av infrastruktur	Leverandører av infrastruktur til avsendervirksomheten har diverse kontaktpunkt for feilmeldinger der avsendervirksomheten kan ta kontakt for informasjon og retting av feil.

3.5.2. Grensesnitt og feilsituasjoner hos innbygger

Innbygger kan oppleve flere situasjoner som fører til at digital postkasse til innbyggere ikke virker som forventet. Figuren under viser de grensesnitt innbygger forholder seg.



Grensesnitt	**Beskrivelse**
Postkasse (nettside)	Postkasseleverandøren har en nettside som gir innbyggeren tilgang til posten sin. Her kan innbyggeren oppleve at siden ikke er tilgjengelig, eller at han ikke er i stand til å lese post.
Brukerstøtte hos postkassen	Problemer ved bruk av postkassen kan rettes til postkasseleverandørens brukerstøtte.
ID-porten (nettside)	ID-porten benyttes ved innlogging til postkassen. Her kan innbyggeren oppleve problemer med å logge inn.

Grensesnitt	Beskrivelse
Brukerstøtte hos Difi	Problemer ved bruk av ID-porten eller dine kontaktopplysninger kan rettes til Difis brukerstøtte.
Dine kontaktopplysninger (nettside)	Dine kontaktopplysninger er en nettside hvor innbygger kan se og endre sin kontaktinformasjon. Ved feil kontaktinformasjon vil innbyggeren kunne miste varsel om digital post.
Reservasjon mot kommunikasjon på nett (nettside og telefon)	Innbygger kan reservere seg mot digital kommunikasjon. Hvis innbyggeren feilaktig blir reservert vil post som innbyggeren forventer å få digitalt sendes på papir.
e-ID (nettsider og apper)	Innlogging for å lese digital post fra det offentlige krever bruk av ID-porten. Uten en e-ID som virker med ID-porten vil innbygger ikke få tilgang til digital post fra det offentlige. Autentisering i ID-porten fungerer sammen med nettsider og apper levert av e-ID-leverandøren. Nettsidene og appene brukes sammen med smartkort, USB-pinner, SIM-kort, kodebrikker, kodebrev, og eller hva e-ID-leverandøren benytter i autentiseringen.
Brukerstøtte hos leverandør av e-ID	Problemer ved bruk av e-ID kan rettes til e-ID-leverandørens brukerstøtte.
Brukerstøtte hos avsendervirksomhet	Normalt tilbyr avsendervirksomheten en brukerstøtte for innbyggere de sender post til. Her kan innbygger ta kontakt i forbindelse med post de har problemer med.
Infrastruktur (tekniske grensesnitt)	Internett, navnetjenester (DNS), sertifikattjenester (OCSP, CRL), nettleser, pdf-leser med mer er nødvendig for å benytte digital postkasse for innbygger. Ved feil kan innbygger bli forhindret fra å lese digital post. For eksempel kan manglende pdf-leser føre til at innbyggeren ikke får lest digital post.
Brukerstøtte hos leverandør av infrastruktur	Stort sett er det internettleverandører, operativsystemleverandører og programvareleverandører som er aktuelle å kontakte for innbygger, og da gjerne på deres hjelpesider på nett.

3.6. Kritiske funksjoner

Funksjon	Kritikalitet
Hente innbyggers kontaktinformasjon	Avsender kan ikke sende digital post uten innbyggers kontaktinformasjon. Ved feil i kontaktinformasjon kan digital post ende opp hos ikke autoriserte personer.
Validering av innbyggers sertifikat	Avsender kan ikke sende digital post uten å validere innbyggers sertifikat. Ved feil sertifikat fra innbyggers kontaktinformasjon og feil ved valideringen av sertifikatet kan digital post bli tilgjengelig for ikke autoriserte personer.
Meldingsformidlertjenesten	Avsender kan ikke sende digital post dersom meldingsformidlertjenesten er utilgjengelig.

Funksjon	Kritikalitet
Postkassetjenesten	Meldingsformidler kan ikke levere post videre dersom postkassetjenesten er utilgjengelig. Innbygger kan ikke lese post dersom postkassetjenesten er utilgjengelig.
Validering av virksomhetssertifikater	Avsender, meldingsformidler og postkasseleverandører kan ikke utveksle informasjon på en tilstrekkelig sikker måte dersom validering av virksomhetssertifikater er utilgjengelig.
Validering av TLS-sertifikater	Innbygger, avsender, meldingsformidler og postkasseleverandører kan ikke kommunisere på en tilstrekkelig sikker måte dersom validering av TLS-sertifikater er utilgjengelig.
Liste over godkjente avsendere	Meldingsformidler og postkasseleverandører kan ikke formidle digital post dersom liste over godkjente avsendere er utilgjengelig. Ved feil på listen over godkjente avsendere kan ikke autoriserte avsendere sende digital post.

3.7. Risiko- og sårbarhetsanalyse

Det gjennomføres jevnlig risiko- og sårbarhetsanalyser, både hos sentralforvalter, meldingsformidler og postkasseleverandører. Resultatet oppbevares hos hver enkelt aktør og gjøres tilgjengelig for sentralforvalter.

3.8. Risikostyring

Sentralforvalter tilbyr en tjeneste som skal være egnet til å formidle mesteparten av avsendernes post til innbyggere. Avsendervirksomhetene har ansvar for posten de sender og får ikke overføre denne risikoen til sentralforvalter. Sentralforvalter har ansvar for å synliggjøre risiko ved bruk av tjenesten, slik at avsendervirksomhetene kan gjøre gode risikovurdering for posten de sender. Avsendervirksomhetene må selv vurdere hvilken post som kan sendes i tjenesten, og dersom de har post som tjenesten ikke er egnet for, så må de selv finne alternative leveringsmåter.

Posten som er levert er innbyggers eiendom og behandling av denne vil i hovedsak være et forhold mellom innbygger og postkasseleverandør. Avsenders ansvar og risiko for det enkelte brev opphører når posten er levert. Imidlertid er det ikke akseptabelt at det offentlige overfører risiko til innbyggere som disse ikke har forutsetninger for å håndtere. Avsendervirksomheter har altså et ansvar for at post kan håndteres forsvarlig av mottaker, selv om det er mottakeres eiendom etter levering. Dette ansvaret tas ved at sentralforvalter har avtale med postkasseleverandørene om hvordan de skal oppbevare post fra det offentlige på en sikker måte.

Innbyggere har mulighet til å laste ned post til eget utstyr, og da har det offentlige ikke noen innvirkning på hvordan innbyggeren velger å beskytte informasjonen.

Trusselbildet vil endre seg over tid, både på grunn av en generell utvikling av angrepsmetoder hos trusselaktørene, og fordi mengden informasjon i løsningen vokser og blir mer verdifull for angripere. Endring i risiko kartlegges ved jevnlig risiko- og sårbarhetsanalyse, og håndteres ved å tilpasse løsningen slik at risikoen holdes på et akseptabelt nivå.

3.9. Sikkerhetsstandarder og protokoller

Digital postkasse til innbyggere benytter blant annet standardene og protokollene listet her:

Standard	Beskrivelse
X.509	Definerer et rammeverk for digitale sertifikater. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (http://tools.ietf.org/html/rfc5280) Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (http://tools.ietf.org/html/rfc6818) Recommendation ITU-T X.509 ISO/IEC 9594-8
OCSP	En protokoll for å bestemme status på et digitalt sertifikat. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (http://tools.ietf.org/html/rfc2560)
TLS	En protokoll for å sikre kommunikasjonen mellom klient og server på internett. The Transport Layer Security (TLS) Protocol Version 1.2 (http://tools.ietf.org/html/rfc5246)
PKCS #1	Standard for kryptering og signering med offentlig nøkkel kryptografi. PKCS #1 v2.1: RSA Cryptography Standard
SAML	Security Assertion Markup Language (SAML). En standard for å utveksle autentisering- og autoriseringsinformasjon mellom parter. http://saml.xml.org/saml-specifications
NTP	Network Time Protocol Network Time Protocol Version 4: Protocol and Algorithms Specification (http://tools.ietf.org/html/rfc5905)
XML Schema	XML Schema
XML Signature	XML Signature Syntax and Processing (Second Edition)
XML Encryption	XML Encryption Syntax and Processing Version 1.1
UUID	A Universally Unique IDentifier (UUID) URN Namespace (http://tools.ietf.org/html/rfc4122)
SOAP	Simple Object Access Protocol (SOAP)

Standard	Beskrivelse
	http://www.w3.org/TR/soap/
Web Services Security	En sikkerhetsutvidelse til SOAP som spesifiserer hvordan konfidensialitet og integritet kan bli ivaretatt for Web Services. https://www.oasis-open.org/standards#wssv1.1.1
ETSI TS 102 918	Electronic Signatures and Infrastructures (ESI); Associated Signature
ETSI TS 103 174	Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile
ETSI TS 101 903	Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures
ETSI TS 103 171	Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
IETF, RFC 5652	Cryptographic Message Syntax (CMS)
IETF, RFC 3560	Use of the RSAES-OAEP Key Transport Algorithm in the Cryptographic Message Syntax (CMS)
IETF, RFC 3565	Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)
IETF, RFC 5084	Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)
IETF, RFC 5083	Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type
Standard Business Document	Standard Business Document
AS4 Profile of ebMS 3.0 Version 1.0	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.pdf
OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf

4. Kryptografisk beskyttelse av digital post

Digital postkasse til innbyggere skal etablere tillit 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 overordnet løsning for å sikre integritet og konfidensialitet i overføringen av digital post fra avsendervirksomhetene til innbyggernes digitale postkasser.

Formatet på digitalt post er detaljert på http://begrep.difi.no/SikkerDigitalPost. Løsningen legger opp til at all post sikres på samme nivå, og er tiltenkt å kunne beskytte informasjon av særlig følsomme taushetsbelagte opplysninger, herunder de fleste sensitive personopplysninger, stigmatiserende opplysninger m.v. Eksempelvis opplysninger om sykdom. Det er hver enkelt avsendervirksomhet som må vurdere om løsningen er dekkende for deres informasjon, men det vil utarbeides risiko- og sårbarhetsanalyser som vil hjelpe avsendervirksomhetene i denne vurderingen.

4.1. 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.

Associated Signature Container er et pakkeformat som er designet for å ivareta integritet til innholdet over lang tid. Kort fortalt definerer standarden hvordan man skal sette sammen en zip-fil med en filstruktur der man lager en digital signatur over innholdet.

Avsendervirksomheten pakker dokumentene til mottakeren i en dokumentpakke og signerer den med sitt eget virksomhetssertifikat. (En avsendervirksomhet kan også benytte sertifikatet til en Databehandler etter nærmere avtale.)

I tillegg er det en signatur på formidlingen som dekker både ukryptert metadata som skal være tilgjengelig under formidlingen, inkludert avsenders virksomhetssertifikat, varslingsinformasjon og dokumentpakken som er kryptert.

Det vil være behov for å endre algoritmer og protokoller over tid, men i første versjon er signaturen i dokumentpakken http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (PKCS #1 v1.5) i henhold til XAdES-standarden.

For å sende digital post må en avsendervirksomhet være registrert med organisasjonsnummer hos sentralforvalteren av digital postkasse til innbyggere, og må inneha et virksomhetssertifikat som benyttes for å signere all digital post. Meldingsformidler og postkasseleverandører vil va-

lidere 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. Signaturen i dokumentpakken kan valideres av en tredjepart, eller avsender kan signerer dokumentene som legges i dokumentpakken helt uavhengig av digital postkasse til innbyggere.

4.2. 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 utsendelse 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 kan kostnadsfritt valideres opp mot en sertifikatutsteder. I første omgang har begge postkasseleverandørene valgt å beskytte posten med eget virksomhetssertifikat.

Avsendervirksomheten validerer sertifikatet og benytter dette for å kryptere den symmetriske nøkkelen som benyttes for å kryptere selve innholdet i den digitale posten. Krypteringen er i henhold til Cryptographic Message Syntax (CMS). Det vil være behov for å endre algoritmer og protokoller over tid, men i første versjon krypteres dokumentpakken med AES-CBC-PKCS5Padding og den symmetriske nøkkelen krypters med PKCS #1 v2.1.

Det sensitive innholdet i en digital forsendelse krypteres med symmetriske nøkler. Disse nøklene genereres tilfeldig og gjenbrukes ikke.

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 er den beskyttet under overføringen, fordi i tillegg til innholdskryptering er det også kanalkryptering i form av TLS mellom avsendervirksomheten og meldingsformidleren, og mellom meldingsformidleren og postkassen, og mellom postkassen og innbyggerne.

Direktoratet for
forvaltning og IKT (Difi)
Postboks 8115 Dep, 0032 Oslo
Telefon: 22 45 10 00
postmottak@difi.no
www.difi.no