Risikovurdering

System:	Digital postkasse
Dato gjennomført:	Sommer 2018 til januar 2019
Ansvarlig for gjennomføring:	Produktsjef Ellen Marie Kurås Langen
Sak	18/00746

Bakgrunn

Risikovurderingene av digital postkasse ble utført i 2014 og journalført på sak 14/00681 i Difis arkiv og tilgjengeliggjort på samarbeid.difi.no. Risikoregisteret for digital postkasse dokumenteres og vedlikeholdes fortløpende. Siden det er fire år siden en fullstendig risikovurdering, ønsket Difi å få gjennomført en ny omfattende gjennomgang av risikoregisteret i år.

For å gjøre denne risikovurderingen sammenlignbar med tidligere risikovurdering, ble det valgt å legge til grunn det samme rammeverket. Det er tatt med mindre utdrag fra tidligere risikovurdering i dokumentet, men ønsker man å gå ytterligere i dybden i rammeverket vises det til ovennevnte risikovurdering.

I arbeidet har følgende roller i Difi vert representert:

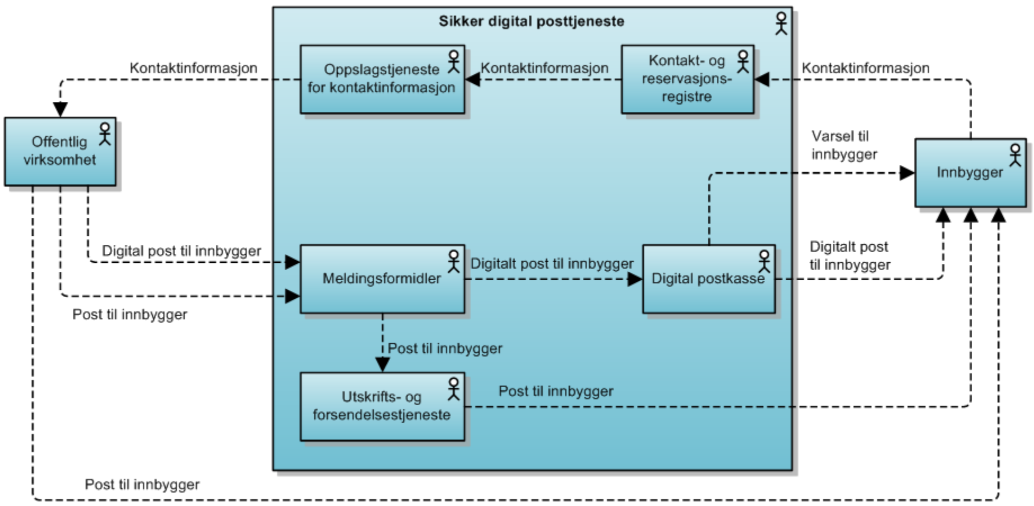
- Arkitekt: Martin Normann Michelsen
- Driftsleder: Sture Domaas Førre
- Incident Manager: Anne Lise Breidvik
- IT-sikkerhet: Arild Bjørk
- Produktsjef: Ellen Marie Kurås Langen
- Service Manager: Karin Furuli

Beskrivelse
For å gjøre det enkelt for forvaltningen å kommunisere digitalt, har Difi etablert en sikker digital postkasse for innbyggerne. Innbygger velger selv postkasse for å motta digital post fra det offentlige, blant markedsaktørene Posten og e-Boks.

Løsningen er egnet for å sende taushetsbelagt og annen beskyttelsesverdig informasjon. Digital post sendes og lagres kryptert i innbyggers postkasse. Innbygger logger seg inn via ID-porten for å lese posten sin fra det offentlige. Den enkelte virksomhet må i henhold til regelverket om behandling av personopplysninger gjennomføre en risiko- og sårbarhetsvurdering før digital postkasse tas i bruk, på samme måte som for andre løsninger. Utskrift og forsendelse er en del av tjenesten, slik at virksomhetene kan ekspedere både digital post og papirpost til innbyggerne i samme kanal.

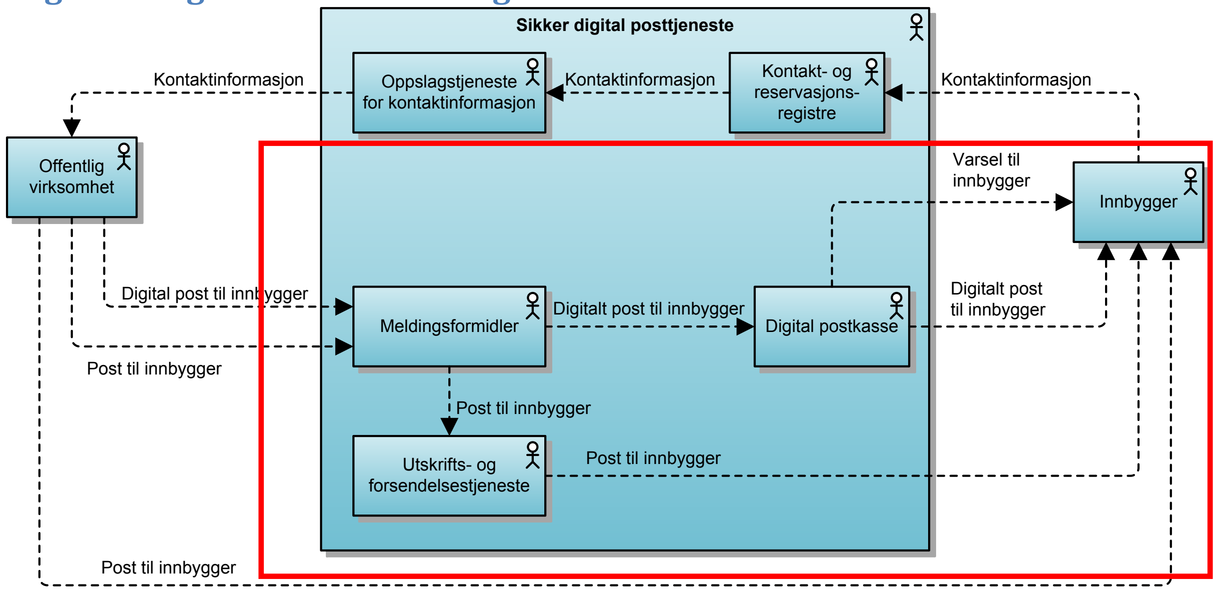
Digital postkasse er sist verdivurdert 12.03.18. Konsekvensene for Difi ved en hendelse innenfor konfidensialitet, integritet eller tilgjengelighet ble vurdert til nest høyeste nivå 3 av 4. Man antar at det for en hendelse innenfor konfidensialitet og integritet vil kunne slå mest ut på omdømmet til Difi. Årsaken er at produktet fremdeles er omdiskutert. Om systemet blir utilgjengelig er vurderingen at konsekvensene blir størst i forbindelse med virksomhetsmål og prosesser i Difi. Det vil medføre vesentlig arbeid å få reetablert en tilsvarende løsning.

Beskrivelse av informasjonssystemet
Se http://begrep.difi.no/SikkerDigitalPost/



Figur 1 Overordnet konsept og informasjonsflyt for digital postkasse til innbyggere

Avgrensning av risikovurdering



Risiko internt hos avsendervirksomheten inngår ikke i analysen, herunder at meldinger adresseres til feil person eller at utro tjenere i avsendervirksomheten kopierer meldinger. Noen av risikoene som avdekkes i rapporten bør håndteres med tiltak hos avsendervirksomhetene. Dette vil komme klart frem av tiltakslisten.

Prosessuell, organisatorisk og avtalemessige risiko relatert til avtaleforhold mellom Difi, postkasseleverandør, avsendervirksomheten, utstedere av e-ID og andre er ikke inkludert i analysen.

Sluttbrukers risikoappetitt er ikke inkludert. Vurderingen av risiko knyttet til angrep hos/via sluttbruker gir særlige utfordringer på grunn av at miljøet varierer fra sluttbruker til sluttbruker og det i hovedsak ligger utenfor postkassetjenestens kontrollsfære. Denne risikoen ble derfor vurdert for seg i risikovurderingen i 2014, kapittel 4.2, og ikke ytterligere vurdert nå i gjennomgangen i 2018.

Vi har sett bort fra at omkringliggende systemer som ID-porten og kontakt- og reservasjonsregister som helhet er kompromittert. Dette er omtalt i systemenes egne risikoanalyser.

Analyse av trusler, sårbarheter, sannsynlighet, konsekvens, og uønskede hendelser, samt forslag til tiltak

Samlet sett består risikoregisteret til digital postkasse av 142 risikoer ved start. Oppgaven har vært:

1. Revidere risikoene i risikoregisteret,
2. Finne nye risikoer,
3. Vurdere risikoer knyttet til utskrift- og forsendelsestjenesten.

Utdrag av risikoregister følger som **vedlegg 1**.

Trusselaktører

Trusselaktører er ikke like, og det finnes mange metoder for å kategorisere ulike trusselaktører. Her har vi valgt å fokusere på de samme egenskapene som i risikohåndteringsguiden til NIST, SP 800-30[1], og lagt til utholdenhet:

- Evne - En aktørs tilgang på kompetanse og ressurser.
- Vilje - En aktørs grad av motivasjon for å angripe.
- Målrettethet - En aktørs grad av målrettethet mot brukere eller brukergrupper. Målrettethet vil øke risikoen for individene angrepet rettes mot, pga økt frekvens og tilpasning av angrepene.
- Utholdenhet - En aktørs evne til å opprettholde et angrep over tid og evnen til å utføre flere angrepsforsøk over tid.

Evne, vilje og utholdenhet	Målrettethet
5 Meget høy	**5** Et spesifikt individ
4 Høy	**3** En eller flere individer
3 Middels	**1** Generisk angrep ikke spesielt rettet mot bestemte individer
2 Lav	
1 Meget lav	

De viktigste trusselaktørene vurderes slik:

Trusselaktør	Evne	Vilje	Målrettet	Utholdende
Fremmed makt	5	2	5	5
Organisert kriminalitet	4	3	5	4
Hacktivister	4	3	1	2
Hacker	4	3	3	4
Media	3	3	5	4
Utro tjener i virksomheten	3	3	5	3
Utro tjener hos Difi	3	3	5	3
Utro tjener hos tredjepart/databehandler	3	3	5	3
Nærstående med fysisk tilgang	3	4	5	4
Nærstående uten fysisk tilgang	2	4	5	4

[1] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Trusselaktør	Evne	Vilje	Målrettet	Utholdende
Forfølgere av trusselutsatte	2	3	5	4

Sannsynlighet

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
Sannsynlig at hendelsen inntreffer 4	Hendelsen inntreffer daglig eller oftere	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	- sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
Mulig at hendelsen inntreffer 3	Hendelsen inntreffer en gang i måneden	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
Mindre sannsynlig at hendelsen inntreffer 2	Hendelsen inntreffer årlig	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer 1	Hendelsen inntreffer omkring hvert 5. år eller sjeldnere	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

Konsekvens

Konsekvens-matrise	Ubetydelig	Moderat	Alvorlig	Kritisk
	1	2	3	4
Innbygger	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom kompromittering av følsomme opplysninger	Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av opplysninger den registrerte oppfatter som krenkende. Fare for skade eller helsetap.	Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet	Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.
Virksomhet Omdømme	Kun mindre diskusjon i organisasjonen	Avsender må forklare seg for kundene om saken. Enkeltstående presseoppslag.	Offentlig debatt, ledelsen må forklare seg for eierne eller myndigheter	Politisk debatt, betydelig økonomisk erstatning/tap
Virksomhet Økonomisk	Ubetydelige økonomiske tap	Mange små kostnader. Reduserte besparelser.	Stort økonomisk tap. Stor engangskostnad.	Betydelig økonomisk erstatning/tap

Risikomatrise og aksept

Konsekvens/ Sannsynlighet		Ubetydelig	Moderat	Alvorlig	Kritisk
		1	2	3	4
Sannsynlig Hendelsen inntrer daglig eller oftere	4	4	8	12	16
Mulig Hendelsen inntrer en gang i måneden	3	3	6	9	12
Mindre sannsynlig Hendelsen inntrer årlig	2	2	4	6	8
Sjelden Hendelsen inntrer omkring hvert 5. år eller sjeldnere	1	1	2	3	4

Nivåene for risikoaksept blir da som følger:

Lav risiko	1 – 3	Ingen tiltak nødvendig
Moderat risiko	4 – 9	Hendelsene skal vurderes nærmere og eventuelle tiltak implementeres eller risiko aksepteres
Høy risiko	10– 16	Tiltak skal iverksettes

Risikoevaluering

Lukkede risikoer

Under gjennomgangen av risikoregisteret var det behov for å rydde i registeret. Det medfører at en del risikoer lukkes. Det er flere årsaker til at disse risikoene lukkes, som f. eks.:

- risikoer registrert i forkant av anskaffelse som ikke er gyldige i dagens løsning,
- risikoer er utenfor scope/rammen for risikovurderingen,
- risikoer tilhører andre felleskomponenter,
- risiko er duplikat av annen registrert risiko,
- uklare risikoer.

6 Angriper sletter ulest post i postkassen
Risikoen knytter seg til ID-porten og ikke til digital postkasse.

14 Avsendervirksomheten sender mange meldinger med for lavt sikkerhetsnivå (eks. uten kryptering eller lavt krav til autentisering)
Risikoen er utenfor scope.

15 Avsenderadresse og emnefelt i meldinger, kan røpe en viss geografisk tilhørighet for kode-6 personer
Risikoen er dekket av risiko 137.

16 En bruker har fullmakt til å motta post på vegne av en annen bruker, men meldingen sendes likevel bare til fullmaktsgiver, og ikke til fullmektigen.
Risikoen er utenfor scope. Digital postkasse har ikke fullmaktsregister. Man kan ikke få brev på vegne av andre i sin egen postkasse fra virksomheter. Fullmaktsgiver må gi tilgang til sin postkasse for fullmektigen.

17 En bruker hadde fullmakt til å motta på vegne av en annen bruker, men fullmakten er trukket tilbake. Melding sendes likevel til fullmektigen.
Risikoen anses utenfor scope, se risiko 16 over.

18 En bruker blir feilaktig underlagt fullmakt og får ikke meldingene sine.
Risiko anses å være utenfor scope, se risiko 16 over.

19 Levering til meldingsformilder går sakte, men brevene blir levert innen gitte frister.
Ut ifra beskrivelsen anses dette ikke som en risiko siden brevene blir levert innen de frister som er satt.

21 Får ikke tak i kontaktinfo for mottaker
Risikoen er utenfor scope.

22 Får ikke tak i krypteringsnøkler for mottaker (meldingsformilder, postkasse, id-porten eller sluttbruker)
Risikoen er uklart formulert. Vi tolker det som det er avsender som ikke får tak i krypteringsnøkler. Risikoen hører til kontakt- og reservasjonsregisteret og er utenfor scope.

23 Brevet blir avvist av meldingsformilder (e.g for stort, ukjent format etc.)
Risikoen hører til avsender og er utenfor scope.

27 Stort tap av meldinger i meldingsformidleren, og avsender ikke i stand til å sende melding på nytt

Man mener at avsender skal greie å sende på nytt gitt informasjonen avsender får fra løsningen. Risikoen hører til hos avsender og er da utenfor scope.

29 Meldinger stoppes mellom avsender og meldingsformidler
For generisk hendelse. Risiko hører til avsender og er utenfor scope.

31 En avsender forfalsker tidspunkt for sending, for å etterleve sine lovpålagte tidsgaratiner.
Dette vil ikke kunne skje. Tidsstempler i løsningen vil avsløre dette raskt.

32 En aktivist sender meldinger til hele befolkningen, eks. trusler, tulle-selvangivelser eller barneporno. Avsender kan ikke oppspores/avsløres.
Alle avsendere er autentisert med org.nr og sertifikat. Utro tjener er behandlet i andre risikoer.

34 Brukeren tar sikkerhetskopi (dvs. meldinger ut av systemet). Lekkasje. Brukeren anklager virksomheten.
Tiltenkt funksjonalitet at bruker kan lagre meldinger fra tjenesten. Ikke risiko, men tiltenkt funksjonalitet.

35 Brukeren sletter utilsiktet meldinger fra brukerarkivet.
Det er brukers risiko. Bruker kan kontakte avsender for å sende på nytt.

36 Det blir begrenset (plass eller tid) til lagring av dokumenter i brukerarkivet; brukeren anklager virksomheten
Post fra det offentlige til innbygger er gratis å lagre for innbygger. Om bruker ønsker å lagre andre dokumenter/filer i løsningen, kan bruker kjøpe mer plass. Tydelig markedsført i løsningene. Anses ikke som reell risiko.

37 Et sensitivt brev blir synlig for en venn i tippelaget som følge av at manglende forståelse hos bruker av verdien av elektronisk identitetsbevis/e-ID; tippekort går på omgang i tippelaget
Risiko hører til ID-porten og omhandler forståelsen rundt hva en e-ID er og konsekvenser ved deling. Risiko er utenfor scope.

38 Et viktig brev leses av en som disponerer en annens e-ID (eks. tippelaget, ektefellen)
Dette er en generell risiko for flere fellesløsninger og vi har ikke kjennskap til konkrete hendelser knyttet til DPI. Større modenhet omkring håndtering av e-ID i befolkningen har redusert risiko. Vi vurderer risikoen utenfor scope da en brukers lempfeldige omgang med eIDene er en risiko som hører til ID-porten.

39 En bruker utsettes for ID-tyveri og angriper sletter svært viktige meldinger.
Dette er en risiko som er utenfor digital postkasse sin kontroll. Risikoen hører til ID-porten og eventuelle tiltak kommer inn under ID-porten sin risikostyring. Risiko er utenfor scope.

40 Lekkasje til offentligheten fra brukerarkivet som følge av ID-tyveri utenfor digital postkasse. Opplysningene som lekkes er svært følsomme for brukeren.
Risikoen knytter seg til ID-porten og ikke til digital postkasse og er utenfor scope.

41 Ondsinnet programvare hos brukeren fører til lekkasje. Brukeren anklager virksomheten
Tjenesten digital postkasse kan ikke løse dette. Det er en brukerrisiko.

42 Ondsinnet kode hos brukeren fører til ID-tyveri ved bruk av ID-porten; brukeren anklager virksomheten
Tjenesten digital postkasse kan ikke løse dette. Det er en brukerrisiko.

43 En bruker får ikke varsel fordi minnet i telefonen fullt, nytt nummer, brukeren er i utlandet, eller tilsvarende.
Det er brukers ansvar å vedlikeholde sine kontaktopplysninger og sitt utstyr. Tjenesten digital postkasse kan ikke løse dette. Risiko er brukers eller bør tilordnes kontakt- og reservasjonsregister og er i så måte utenfor rammene for digital postkasse sin risikovurdering.

46 En melding fra en privat avsender oppfattes som offentlig og brukeren agerer og bestiller tjenesten (e.g. tilbud om kontroll av bil fra Biltilsynet)
Risiko ligger hos bruker. Dersom bruker ønsker å bestille en tjeneste, spiller det heller gjerne ikke noen rolle for bruker om den leveres av privat eller offentlig virksomhet så lenge tjenesten er reell. (Biltilsynet er ikke privat avsender.) Ikke risiko.

47 En mottaker får en pdf med felter som skal fylles ut, og forstår ikke at papir er eneste måte å returnere dette på.
Det er vanlig er å ordne med elektronisk tilbakemelding. Alternativet er å sende på papir med medfølgende returkonvolutt. Uansett avsenders ansvar å kommunisere godt til mottaker. Risiko utenfor scope.

48 En mottaker får en pdf som skal fylles ut og sendes tilbake, men mottaker har ikke skriver.
Vanlig forvaltningspraksis tilsier mulighet for elektronisk tilbakemelding, alternativt sendes det på post med medfølgende returkonvolutt. Evt må avsender kommunisere til mottaker at han må henvende seg til avsender. Risiko utenfor scope.

50 Mottaker får sin e-ID revokert (på grunn av manglende betaling, for eksempel), og har ingen alternativ e-ID, og dette skjer like før en frist.
Mottaker er ansvarlig for håndtering av sin e-ID. Tilbakekalling av e-ID-er er en naturlig funksjonalitet for e-ID-leverandører og utenfor digital postkasse sin rekkevidde.

53 Innbygger mister rettigheter fordi postkasseleverandør/meldingsformidler avslører at han befant seg på feil sted/tid.
Det er ikke en konkret risiko som vil kunne konstateres. Dvs. avsender vil ikke få denne informasjon.

54 En bruker endrer postkasse i kontaktregisteret til en ugyldig adresse
Dette kan ikke skje siden bruker ikke kan endre adressen til postkassen i kontaktregisteret.

57 Media bekrefter at løsningen tar imot melding fra en ikke godkjent avsender; meldingen blir levert
Basert på løsningens utforming, lar dette seg ikke gjøre.

58 En godkjent avsender gir seg ut for å være en annen godkjent avsender (for eksempel ved at samme sertifikat blir brukt hos to virksomheter med samme leverandør)
Dette har aldri skjedd. En godkjent avsender kan ikke gi seg ut for å være andre avsendere. Må i tilfelle via Difi sin forvaltning for å etablere sending på vegne av. Risikoen er formulert som om en vilkårlig godkjent avsender kan gjøre dette uten hjelp. Dette er ikke mulig slik løsningen er utformet. Oppbevaring av sertifikat er avsenders risiko og utenfor scope.

59 En utro tjener sender melding til hele befolkningen fra en godkjent avsender (for eksempel politisk budskap, reklame el. l.)
Risikoen hører til avsender og er utenfor scope.

60 Sender bekreftelse på levert melding til feil avsender

Kvittering sendes ikke. Avsender må hente kvitteringer ved hjelp av eget sertifikat. Risiko ikke relevant.

62 Ved tilsyn blir meldingsformidler ikke godkjent
Det utføres ikke tilsyn på meldingsformidler. Risiko ikke relevant.

67 Rekkefølgen på meldinger endres mellom meldingsformidler og postkasse
Ikke relevant risiko.

71 Meldingsformidler avslører hvem som er kunde av hvilken postkasse
Risiko hører til kontakt- og reservasjonsregisteret, ikke digital postkasse til innbyggere. Risiko er utenfor scope.

72 Inneholder feil/Kennet-variant/etc.
Risiko hører til kontakt- og reservasjonsregisteret og er utenfor scope.

74 Bruker bytter postkasse, men hans gamle data slettes ikke.
Systemet er laget for at bruker kan beholde sine to postkasser. Data kan kopieres mellom postkassene, men bruker må evt slette postkassen sin.

75 Lekkasje som følge av single-sign-on (lekkasje hos en annen virksomhet gir lekkasjer hos virksomheten)
Risiko hører til ID-porten og er utenfor scope.

77 Ende-til-endekryptering svikter; meldinger passerer i klartekst gjennom systemet.
Dette har aldri skjedd. Meldinger som ikke har gyldig integritet (ved hjelp av sertifikat) blir avvist.

78 Kryptering til feil mottaker (meldingen kan ikke leses av mottaker)
Alt blir kryptert med postkasseleverandør sitt sertifikat per nå. Risiko er ikke relevant for dagens løsning.

79 En melding kommer på avveie, den er kryptert, men personnummer og avsender står som mottaker (dvs. det blir kjent at en melding er sendt til personen).
Det er postkasseadressen som står som mottaker, ikke personnummer og mottaker. Risiko vurderes ikke reell slik den er beskrevet. Tilstøtende risikoer relatert til feilsending tar for seg informasjon på avveie.

84 Bruker anbefales å deaktivere støtteprogramvare (Java, Acrobat Reader, etc.) som trenges for å lese meldinger.
Sluttbruker er selv ansvarlig for å sikre eget utstyr.

85 Programvarefeil hos meldingsformidleren, tap av SMS hos mobilselskapet, feil i kontaktregisteret (med vilje, glemt å oppdatere, bug)
For uspesifikk risiko/flere risikoer i èn. Den tar med risikoer for ID-porten og kontakt- og reservasjonsregisteret. Eventuelle tekniske feil i løsningen, håndteres via rutiner for feil/hendelseshåndtering.

86 Xml-tagging hos avsender
Risikoen anses for å være utenfor scope. Ligger hos avsender.

87 Programvarefeil hos meldingsformidleren.

Tittel og tekst på risiko er ikke i samsvar. Risikoen er også noe generisk og uklar da man ikke er konkret på hva som feiler eller skal være sårbarhet.

88 Feil i kontaktregisteret; brukeren oppført som død
Risiko vurderes utenfor scope, hører til kontakt- og reservasjonsregisteret.

89 Bruker misforstår varselet og tror det er meldingen. Meldingen er ikke kritisk.
Risikoen er utenfor scope. Det er vanskelig å ta ansvar for brukers leseferdigheter. Utformingen på varsel anses å være tydelig på at det er et varsel og ikke noe annet.

90 Avsender mottar feil info og sender elektronisk melding til en bruker som ikke har postkasse.
Personer som ikke har postkasse er det ikke mulig å sende til elektronisk. Erfaringer så langt er at det har hendt at melding sendes til feil person dersom avsender ikke bruker fødselsnummer til å søke opp person. Da er risikoen hos avsender og utenfor scope. Ingen erfaringer med at feil info fra kontakt- og reservasjonsregisteret har ført til feilsending.

93 Melding med taushetsbelagte opplysninger sendes til feil mottaker.
Kan skje dersom avsender ikke bruker fødselsnummer til å lokalisere mottaker. Risiko hører til avsender og er utenfor scope.

94 Melding uten taushetsbelagte opplysninger sendes til feil mottaker.
Risikoen hører til avsender er utenfor scope.

95 Brukeren videresender / får videresendt meldinger utenfor norsk jurisdiksjon (e-Boks i Danmark, for eksempel)
At bruker videresender er brukers valg og ansvar.

96 Lekkasje av informasjon på grunn av utro tjener hos de private leverandørene av postkassetjenester
Risiko er vurdert tidligere på meldingsformidler, risiko 56, og postkasseleverandør hver for seg, risiko 128. Risiko 103 er også en del av dette helhetsbildet for alle leverandøraktørene.

105 Det kommer mange e-ID-leverandører; en bruker velger en med lav kvalitet
Risiko vurderes utenfor scope siden dette en risiko som hører til ID-porten.

108 Tar imot melding fra en falsk meldingsformidler som inneholder trusler til befolkningen
Tatt hensyn til arkitektonisk for å sikre seg mot falske meldingsformidlere. Kan ikke se at det vil være mulig å integrere falske meldingsformidlere arkitektonisk eller forvaltningsmessig.

109 Metadata inneholder feil
Risikoer hører til avsendervirksomhet og er utenfor scope.

110 Manglende metadata hindrer levering av meldinger
Risiko hører til avsendervirksomhet og er utenfor scope.

112 Kjøling feiler
Anses for å være duplikat av risiko 68.

118 Postkasse ikke tilgjengelig på brukers utstyr (e.g. Java på nettbrett)
Det hender at brukerne har gammelt utstyr, f. eks. Windows XP som ikke kan oppdateres. Erfaringene er at det er et mindre problem for postkassebrukerne. Dagens brukere har flere typer

utstyr (PC, mobil eller nettbrett). Risiko hører til bruker og er ergo utenfor digital postkasse sin rekkevidde. Se for øvrig også bruksvilkårene til Digipost og e-Boks.

122 Manglende sikkerhet, rutiner, et cetera
Risikoen er for lite spesifikk.

125 Sertifikatfeil gjør at meldinger blir avvist
Risikoen er knyttet til rutiner som avsendervirksomheten er ansvarlig for. På lik linje med at man feiladresserer meldinger eller har utro tjener i virksomheten, er det virksomheten sitt ansvar at de har tilstrekkelig oppfølging av rutiner for å sørge for at integrasjonen fungerer som den skal. Risikoen er utenfor scope.

134 Fødselsnummer er identifikatoren i digital postkasse til innbyggere, mens i flere fagsystemer er saken registrert på navn.
Risikoen hører til avsender er utenfor scope.

136 Melding kan ikke sendes pga feil hos avsender
Risikoen hører til avsender er utenfor scope.

143 Gyldige avsendere kan ikke valideres
Det er ikke mulig å sende post gjennom systemet uten avtale. Risiko ikke reell.

Risikoer som har endret risikonivå

Basert på erfaringer og/eller tiltak etablert i løsningen, følger her en oversikt over de risikoene som har endret seg i forhold til tidligere. I hovedsak er det snakk om en justering av sannsynlighet knyttet til risikoene.

9 En privat aktør (med avtale i offentlig virksomhet) sender reklame
En privat aktør må tilegne seg rollen som saksbehandler i virksomheten sine systemer og dette er lite sannsynlig. Erfaringer viser at dette ikke har skjedd. Sannsynlighet reduseres fra 2 til 1.

11 Melding om virus
Hendelsen har aldri skjedd så lenge digital postkasse har vært i drift. Sannsynlighet reduseres fra 2 til 1.

12 En melding inneholder en link som er uriktig; en bruker får trojaner / virus / malware
En slik hendelse har aldri skjedd i løpet av årene løsningen har vært i produksjon. Dette tyder på at de tiltak avsendere og postkasseleverandører har etablert for å forhindre at skadevare spres fungerer. Sannsynlighet redusert fra 3 til 1.

13 Melding sendes til en mottaker som er død. Kontaktregisteret ikke oppdatert.
Daglig dødevask innført, men det tar noen dager før dødsfall registreres i Folkeregistrert. Sannsynlighet reduseres fra 4 til 3.

20 Kobler opp mot falsk meldingsformidler, SSL-spoofing. Blir oppdaget på grunn av manglende kvittering, men ikke kryptert informasjon blir eksponert.
Dette har aldri skjedd. Lite sannsynlig og evt. en risiko som hører til avsendervirksomheten. Snur om på sannsynlighet og konsekvens. Sannsynlighet settes til 1 og konsekvens til 4.

24 Meldingen blir avvist av postkassen
I utgangspunktet skal meldinger evt. bli avvist av meldingsformidler og dermed ikke komme frem til postkassen. Håndteres med kvitteringsflyt og god feilhåndtering. Sannsynlighet reduseres fra 4 til 3.

25 Får ikke bekreftelse på levert melding
Avsendere som har overvåkning melder dette inn. Difi har registrert noen hendelser på dette, men velger å redusere sannsynlighet fra 4 til 3 da det anses som et forbigående problem og ikke generelt omfangsrikt.

49 Mottaker ikke i stand til å autentisere seg overfor postkassen i ett døgn (ID-porten er nede)
Har ikke skjedd at ID-porten har vært nede ett døgn. Ingen avsender setter frist på 1 døgn svarfrist. Virksomhetene må følge forvaltningsloven. Sannsynlighet og konsekvens endres fra 2 til 1.

52 Innbygger skifter postkasse, men brukerarkivet overføres ikke. Brukerarkiv slettes hos gammel leverandør.
Man kan overføre mellom postkasseleverandørene. Eneste måten å slette brukerarkivet er dersom brukeren sletter det. Sannsynlighet reduseres fra 2 til 1.

55 Innbygger mister tilgang til postkassen
Difi kjenner til én hendelse på de fire årene løsningene har vært i bruk, der 50 postkasser ble deaktivert som følge av en menneskelig feil. Sannsynlighet reduseres fra 2 til 1.

61 Postkasseleverandør følger ikke rutiner for begrensninger mht. hvilke personer som skal ha tilgang til sikret område, ev. taushetserklæringskrav (eks. renholdere).

Kjenner ikke til hendelse i løpet av 4 år i produksjon. Leverandørene har gode rutiner, sannsynlighet er lav. Sannsynlighet reduseres fra 2 til 1.

63 Postkasseleverandørene følger ikke rutiner for destruksjon av disker. Eksterne stjeler disker som er tatt ut av produksjon (vi har ikke kontroll på innholdet)
Både postkasseleverandørene og underleverandør har rutiner for å håndtere lagringsmedia som blir tatt ut av produksjon som inkluderer degaussing. I tillegg bør det nevnes at disker eller fastminne i store produksjonsløsninger kjører i RAID som gjør at data blir spredt på et lavnivå som gjør at det er umulig å gjenskape store mengder uten at man kan gjenskape det eksakte oppsettet. Sannsynlighet reduseres fra 2 til 1.

65 Meldinger endres mellom meldingsformidler og postkasse, og det oppdages ikke.
Kjenner ikke til bitfeil. Meldinger er krypterte i transport. Vil ikke validere og vil forkastes med feilkvittering. Meldinger kommer ikke fram som uleselige som følge av feil under transport. Konsekvens reduseres fra 3 til 1.

69 Strømforsyning feiler som medfører at systemet er utilgjengelig i tre dager.
Redundans i flere nivå. Konsekvens reduseres fra 3 til 2.

70 2-3 dager nedetid pga. manglende eller for liten bemanning i en feilsituasjon.
Har ikke skjedd. God erfaring med stabil drift hos leverandørene. Sannsynlighet reduseres fra 2 til 1.

73 Bruker bytter postkasse, men meldinger går likevel til hans gamle adresse.
Dersom avsender har sendt med utsatt tilgjengeliggjøring, vil post havne i gammel postkasse. Bruker får varsel om ny post og vil oppdage dette. Konsekvens reduseres fra 2 til 1.

76 Lekkasjer av informasjon som følge av programvarefeil (Kenneth-saken)
Har ikke skjedd. Sannsynlighet reduseres fra 2 til 1.

82 Det har blitt akseptert risiko i digital postkasse som avsender ikke ville ha akseptert
Virksomhetene som må ta stilling til om de vil bruke tjenesten. De må risikovurdere sine tjenester, jf. bruksvilkår for digital postkasse. Konsekvens reduseres fra 3 til 1 og sannsynlighet fra 2 til 1.

83 En avsender ønsker å ta ned løsning pga. uavklart feil. Leverandør/sentralforvalter etterkommer ikke ønske.
Har ikke skjedd. Var en større risiko i starten. Stabil drift og forvaltning samt god tillit til løsningen hos avsendere gjør at risiko kan tas ned. Sannsynlighet og konsekvens reduseres fra 2 til 1.

91 Avsender mottar feil info og sender fysisk utsendelse til bruker som forventer å få sine meldinger elektronisk.
Erfaring er at det aldri er feil på info fra kontakt- og reservasjonsregisteret, men ikke alltid full synkronisering mellom postkasseleverandørene og registeret. Sannsynlighet reduseres fra 4 til 3 basert på erfaringene med web-services som kan ha stoppet hos postkasseleverandør.

Jevnlige, ca 2 ganger i året, manuelle tiltak for kontrollere at postkasseleverandørene og kontakt- og reservasjonsregisteret er ajour. Sannsynlighet reduseres fra 4 til 3.

92 Melding til en bruker som har reservert seg blir likevel sendt elektronisk
Får ikke sendt til brukere som har reservert seg. Når noen reserverer seg, vil statusen medføre at systemet ikke kan sende elektronisk til vedkommende. Kan skje dersom avsender benytter lokal kopi av kontaktregisteret som ikke er oppdatert. I tilfelle avsenders risiko. Det er seks virksomheter som har lokal kopi. Disse oppdateres hvert 1. til 10. minutt. Sannsynlighet reduseres fra 3 til 1.

98 Kryptert backup kommer på avveie.
Har aldri skjedd. Sannsynlighet reduseres fra 2 til 1.

99 Kryptert backup, med noen opplysninger (metadata) i klartekst, kommer på avveie.
Har ikke skjedd. Løsningen baserer seg på skyteknologi. Mulig gammeldags risiko fra den tiden man kjørte backup til tape eller separate disker. Må vurderes å lukkes neste gang. Sannsynlighet reduseres fra 2 til 1.

103 Én eller flere aktører i digital postkasse har ikke tilfredsstillende avtaler med sine ansatte
Krav til personalssikkerhet i ISMS. Nordiske leverandører - norsk og dansk. Gode arbeidsmiljølover. Sannsynlighet reduseres fra 2 til 1.

104 Én eller flere aktører i digital postkasse har ikke tilfredsstillende rutiner for «outsourcing» og informasjon havner utenfor avtalens rammer
Avtalene avgrenser handlingsrommet til EU/EØS. Det er avtalefestet at Difi må godkjenne skifte av underleverandør. Sannsynlighet reduseres fra 2 til 1.

106 Digital postkasse blir utilgjengelig for avsender som følge av strømbrudd eller tilsvarende ytre påvirkning
Tilstrekkelig med redundans i løsningen. Avsendere mottar feilmelding dersom meldingsformidler har vært nede i en time. Avsender bes om å sende på nytt. Avtalen stiller krav til tilstrekkelig oppetid i SLA med prikking og prisavslag. Konsekvens reduseres fra 3 til 1.

107 Digital postkasse blir utilgjengelig for bruker som følge av strømbrudd eller tilsvarende ytre påvirkning
Tilstrekkelig med redundans i løsningen. Avtalen stiller krav til tilstrekkelig oppetid i SLA med prikking og prisavslag. Konsekvens reduseres fra 3 til 1.

111 Postkasseleverandør presenterer melding til tilfeldig feil mottaker
Har aldri skjedd. Sannsynlighet reduseres fra 2 til 1.

113 Strømforsyning feiler
Avtalen inneholder omfattende krav til oppetid. Tilstrekkelig redundans ivaretar dette. Sannsynlighet reduseres fra 2 til 1.

114 Melding endres mellom postkasse og mottaker
TLS mellom bruker og tjenesten. Kvalitet kan sjekkes ved hjelp av SSLlabs. Brukerstøtte har aldri hørt om hendelser fra brukerne på dette. Har heller ikke registrert slike hendelser i media. Sannsynlighet reduseres fra 2 til 1.

115 Melding stoppes mellom postkasse og mottaker
Det er ikke registrert slike hendelser. Systemene ligger bak DDoS-beskyttelse. Sannsynlighet settes ned fra 4 til 1 basert på erfaringene i årene som har gått siden løsningen ble etablert.

116 Postkasseleverandør får ny eier
Omfattende avtale som binder leveransen og krav uansett eier. Intet i markedet som tilsier at dette vil skje på overskuelig fremtid. Sannsynlighet reduseres fra 2 til 1 og konsekvens fra 3 til 2.

117 Postkasseleverandør avslutter sin kontrakt med Difi

Det er regulert i avtalene hva som skal skje om en av partene sier opp kontrakten. Det skal være tilstrekkelig med ressurser for at kunden kan overføre til andre leverandører. Sannsynlighet reduseres fra 2 til 1.

123 Melding med taushetsbelagte opplysninger mottas av feil mottaker (sendt riktig)
Systemets arkitektur tilsier at det ikke skal være mulig å sende riktig til feil bruker. Riktig bruker vil få meldingen. Brukerstøtte har aldri opplevd slike hendelser. Sannsynlighet reduseres fra 2 til 1.

124 Melding uten taushetsbelagte opplysninger mottas av feil mottaker (sendt riktig)
Systemets arkitektur tilsier at det ikke skal være mulig å sende riktig til feil bruker. Riktig bruker vil få meldingen. Brukerstøtte har aldri opplevd slike hendelser. Sannsynlighet reduseres fra 2 til 1.

126 Mottaker ikke i stand til å lese melding
Risiko hører mest sannsynlig til bruker og brukers utstyr og er utenfor digital postkasse sin rekkevidde, se for øvrig bruksvilkårene til Digipost og e-Boks. Det er ikke kjennskap til andre årsaker til at mottaker ikke får lest melding. Sannsynlighet reduseres fra 4 til 1.

128 Svært følsom informasjon blir offentlig kjent på grunn av utro tjener hos postkasseleverandør
Konsekvensen på risikoen er knyttet til leverandør. Det er vanskelig å se at konsekvensen for en leverandør skal bli så høy. Leverandørene har strenge rutiner for tilgang til informasjon. Det er implementert sporing på handlinger som kan påvirke innbyggernes informasjon. For å bryte med regimet trengs det flere utro tjenere som samarbeider. På bakgrunn av leverandørenes etablerte rutiner og tiltak vurderes det derfor at omdømme ikke blir rammet i samme omfang. Konsekvens reduseres fra 4 til 3.

130 Varsel om feil i digital postkasse til innbyggere eller meldingsformidler blir ikke gitt til virksomhetene.
Har etablerte rutiner for dette. På bakgrunn av erfaringer med digital postkasse reduseres konsekvens fra 2 til 1.

135 Melding kan ikke sendes pga feil i digital postkasse til innbyggere
Konsekvenser er knyttet til opprydding og forsinkelser. På bakgrunn av erfaringer med digital postkasse reduseres konsekvensnivå fra 2 til 1.

144 Sporbare personopplysninger om reelle personer blir sendt inn i testmiljøet
Det gjennomføres periodisk sletting i testmiljøene etter 30 dager. Difi legger kun inn fiktive fødselsnummer i verifikasjonsmiljøet, så dette skal ikke kunne forekomme. Sannsynlighet reduseres fra 2 til 1.

145 Innbygger blir ikke logget ut fra tjenesten
Risikoen hører til personer som bruker offentlig utstyr eller felles utstyr. Har bruker digital postkasse, har også vedkommende mest sannsynlig utstyr privat. Det er også generelt økt bevissthet om ikt-sikkerhet i befolkningen. Sannsynlighet settes ned fra 2 til 1.

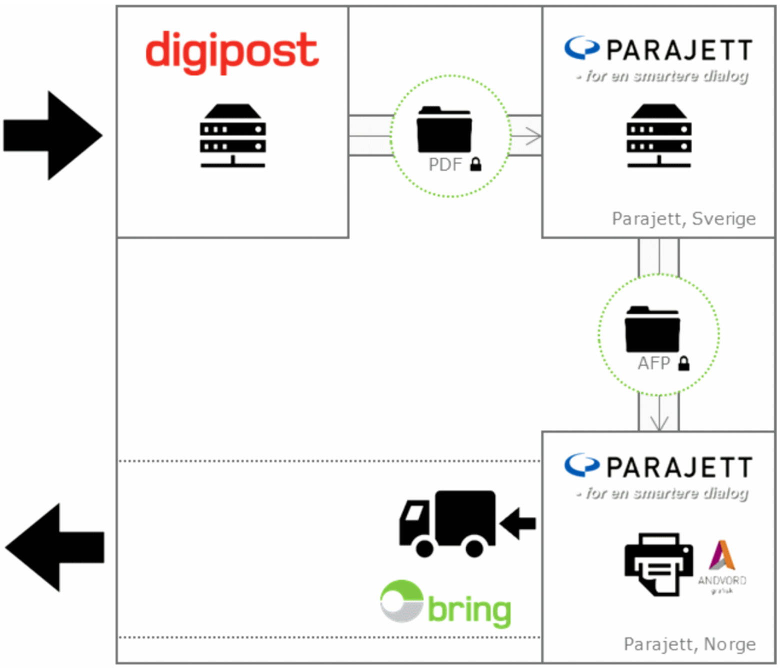
Risikonivå etter revidering av risikoregister

Konsekvens/ Sannsynlighet		Ubetydelig	Moderat	Alvorlig	Kritisk
		1	2	3	4
Sannsynlig Hendelsen inntrer daglig eller oftere	4				
Mulig Hendelsen inntrer en gang i måneden	3	13, 24, 25, 51, 80, 91			
Mindre sannsynlig Hendelsen inntrer årlig	2	8, 10 44, 73, 106, 107, 130		139	
Sjelden Hendelsen inntrer omkring hvert 5. år eller sjeldnere	1	5, 28, 49, 63, 65, 82, 83, 92, 98, 115, 126, 129	7, 9, 11, 12, 33, 52, 55, 61, 69, 70, 99, 103, 104, 111, 113, 114, 116, 117, 120, 121, 124, 135, 140, 144	26, 45, 66, 76, 97, 101, 102, 119, 123, 128, 131, 132, 141, 145	20, 56, 64, 68, 81, 100, 127, 137, 138, 142, 146, 147

Utskrifts- og forsendelsestjenesten

Gjennom infrastrukturen for digital postkasse til innbyggere, tilbyr Difi en opsjon for sikker utskrift, konvoluttering og frankering via en utskrifts- og forsendelsestjeneste for de virksomhetene som ønsker det. Det innebærer at all post til innbyggere kan sendes samme sted, også det som skal på papir i posten. Alt som sendes til utskrifts- og forsendelsestjenesten sendes kryptert gjennom løsningen. Det er Posten Norge AS som leverer utskrifts- og forsendelsestjenesten, mens Parajett utfører utskrift og forsendelse på vegne av Posten.

Prosess	Enhet	Lokasjon	Beskrivelse
Produksjon, **Norge**	Parajett Norge	Oslo, Norge	Produksjon og **levering** av print for Digipost.
Prosessering og produksjon, **Sverige**	Parajett (Sverige)	Landskrona, Sverige	Mottak og **prosessering** av print for Digipost. Ingen produksjon.



Difi har i slutten av oktober 2018 hatt møte med Posten ved direktør for produkt- og forretningsutvikling samt sikkerhetsansvarlig i Digipost. Difi fikk en gjennomgang av:

- Postens risikostyringssystem
- Prosessen til utskriftstjenesten
- Risikoer rangert høyest for utskriftstjenesten
- Risikoer som har vært vanskeligst å vurdere

Siden dette anses som intern informasjon i Posten, gås det ikke nærmere inn på de ulike punktene. De som ønsker en tilsvarende gjennomgang, må ta kontakt med Difi.

Difis vurdering er at Posten har et tilfredsstillende risikostyringssystem. De har god oversikt over prosessen til underleverandør og forståelse av risikoen, og har håndtert disse med tilstrekkelige tiltak. Informasjonssikkerhet hos underleverandør er tilstrekkelig ivaretatt med et styringssystem for informasjonssikkerhet sertifisert etter ISO 27001:2013 som dekker produksjon av fysiske dokumenter.

Innstikk og skanning

Det er gjennom utskrifts- og forsendelsestjenesten mulig å legge innstikk i konvoluttene som sendes ut. Et innstikk kan være et skjema med ferdigfrankert svarkonvolutt eller informasjonsmateriell. Innstikk og skanning er bygd opp på bakgrunn av krav og risikovurdering fra Helse Midt-Norge IT (Hemit), men er generisk funksjonalitet som kan tilbys andre.

Virksomheten kan enten bestille det aktuelle innstikket direkte fra utskriftsleverandøren eller fra en annen leverandør. Det avtales direkte med utskriftsleverandøren når forsendelsen skal sendes. Ved bestilling hos utskriftsleverandøren vil avsender få oppgitt en unik ID. Denne ID-en skal avsender legge inn i metadataene som sendes med den elektroniske forsendelsen til meldingsformidleren til avtalt tidspunkt. Denne ID-en vil bli sendt utskriftsleverandøren som da har oversikt over hvilket vedlegg som skal legges i som innstikk og utfører trykking og konvoluttering med vedlegg som avtalt.

Som en del av tjenesten for innstikk i forsendelser, tilbyr Difi muligheten for å digitalisere returnerte svarskjema. Dersom en virksomhet eksempelvis putter en svarkonvolutt i en forsendelse, kan svarkonvolutten åpnes, skannes og returneres til virksomheten. Tjenesten tilbys av utskriftsleverandøren.

Tjenesten vil innebære oppsett av tolkningsmal for papirskjema som skal fylles ut, sikker håndtering, skanning og makulering av utfylte papirskjema, bilder og data, samt sikker overføring av data og bilder fra utskriftstjenesten tilbake til virksomheten.

Alle skjemaene har en unik QR/strekkode som skanneren gjenkjenner slik at den benytter korrekt tolkningsmal og merker respektive XML og PDF med riktig metadata slik at dataene returneres rettmessig til avsender.

Avsender og utskriftsleverandør avtaler hvilken sikker kanal som skal benyttes for oversending av skannede data fra utskriftsleverandør til avsender. Det anbefales å bruke felles nasjonal infrastruktur til dette når den er tilgjengelig.

For ytterligere beskrivelse av innstikk og skanning, se https://samarbeid.difi.no/felleslosninger/digital-postkasse-til-innbyggere/dokumentasjon under Funksjonell dokumentasjon og Innstikk og skanning i utskrifts- og forsendelsestjenesten.

Difi har i oktober 2018 fått innsikt i risikovurdering av tjenesten som er i sluttfasen hos Hemit og på høring i helseregionene. Difi referer kun overordnet resultat av denne risikovurderingen. Dersom man ønsker innsyn i risikovurderingen, må man henvende seg til Difi.

Risikovurderingen er utført av en arbeidsgruppe bestående av personer fra både Hemit og Parajett Norge samt to uavhengige eksterne rådgivere. Dokumentunderlaget til risikovurderingen er omfattende. Det er identifisert 44 risikoer. Alle risikoer etter tiltak, med unntak av to, ligger på laveste risikonivå. To risikoer er vurdert til laveste nivå (4) av middels risikonivå. Begge risikoene har identifisert ytterligere risikoreduserende tiltak.

Nye risikoer

148 Sensitiv informasjon i varsel om post i digital postkasse (avsender)
Varsel (ukryptert e-post/SMS) inneholder sensitiv informasjon.

149 Avsender sender melding til feil mottaker og ønsker å trekke denne tilbake (avsender)
Avsender sender melding til feil mottaker og oppdager dette rett etter at meldingen er sendt. Ønsker å trekke meldingen tilbake.

150 Mottaker rammes av virus eller skadevare som følger varsel om post (avsender)
Data eller metadata som oversendes fra avsendervirksomhet til postkasseleverandør som danner grunnlag for varslene til mottaker inneholder enten skadevare eller (integrert) skript som kan utløses dersom mottaker klikker på lenke eller åpner e-posten/SMS-en. Mottaker får f.eks. filer slettet eller kryptert.

Leverandørene peker på at varsler på e-post eller SMS sendes i ren tekst og/eller utformes ved hjelp av et strengt malverk.

151 Mottaker rammes av virus eller skadevare som følger av varsel om post (postkasseleverandør)
Varslene om post i digital postkasse inneholder enten skadevare eller (integrert) skript som kan utløses dersom mottaker klikker på lenke eller åpner e-posten/SMS-en. Mottaker får f.eks. filer slettet eller kryptert.

Ser to alternative årsaker til trusselen:

- System for utsending av meldinger er infisert og henger på lenke til eller skadevare
- Misfornøyd ansatt med tilgang til systemet legger til rette for det

Leverandørene peker på tiltak som at varsler sendes i rent tekstformat, servere patcher jevnlig, overvåking av sårbarheter, HIDS/NIDS[2], strenge brannmurregler, sterk tilgangskontroll, begrenset antall personer med tilgang til produksjonsmiljø, hyppige tilgangsrevisjoner, sporbarhet i logging og sikring av logger.

152 Mottaker lures av falskt varsel om post i digital postkasse (ekstern aktør)
Ekstern aktør sender e-post som ser ut for bruker å være varsel om post i digital postkasse. Varselet inneholder lenke til skadevare, reklame eller annet urelatert.

Leverandørene har ulike tiltak som SPF, DKIM og ARC, men det er ikke etablert en DMARC-policy på utsendingsdomene.

153 Utro tjener(e) hos Postens utskriftsleverandør snoker og saboterer (utskriftsleverandør)
Brev på avveie, feil "pakking" etc. Difi krever styringssystem for informasjonssikkerhet tilsvarende ISO 27001 som dekker personellsikkerhet. Ansatte må signere taushetserklæring hos leverandørene. Det har ikke skjedd en slik hendelse så langt Difi er kjent med i løpet av perioden man har tilbydd utskrift.

154 Ved oversending av skannede data fra utskriftsleverandør til virksomhet benyttes en ikke sikker kanal (utskriftsleverandør)
Gjelder innstikkdelen av utskriftstjenesten. Skjema som er besvart på papir av mottaker og skannes av utskriftsleverandør.

[2] Host-based/Network Intrusion Detection System

Svar fra skjema digitaliseres og struktureres før de oversendes avsendervirksomhet. I dag har man bare krav om at det skal avtales en sikker kanal for returdata tilbake til virksomhet. Fare for at kravet glemmes og data sendes over usikker kanal. Informasjon kan leses av uvedkommende og tilliten til tjenesten påvirkes negativt. Det er avsenders ansvar å gjennomføre risikovurdering for bruken og tilstrekkelig sikkerhet på kanal tilbake. eFormidling, tilbyr sikker kanal, men er ikke klar ennå.

155 Mistillit til digital postkasse siden kryptering skjer med postkasseleverandørs sertifikat (ekstern aktør)

Meldinger til brukere av digital postkasse blir kryptert med offentlig nøkkel for postkasseleverandør. Meldingene vil da være leselig for de som har tilgang til privatnøkkel og evt. passord hos postkasseleverandør, som da kan dekryptere meldinger. Meldinger blir også dekryptert ved virus-skanning. Ved ekte ende-til-ende-kryptering ville det ikke vært mulig å beskytte brukere mot skadevare i postkassen.

Difi opplever av og til at brukere med teknisk bakgrunn stiller spørsmål ved sikkerheten i digital postkasse ved at de peker på risikoen ved bruk av postkasseleverandørenes krypteringsnøkkel og etterlyser ende-til-ende-kryptering. Sett i lys av hendelser med Facebook og Google+ der personopplysninger kommer på avveie, kan det være en økt risiko for at Difi kan oppleve at det kan skapes mistillit til digital postkasse.

156 Ansatt hos utskriftsleverandør kommer over et sensitivt brev til en høyt aktet personlighet (f.eks statsministeren), og presser vedkommende for penger eller truer med å gå ut i media, eller går faktisk ut i media (utskriftsleverandør)

Dette har aldri skjedd. Logging av digital aktivitet på utskriftsleverandørens systemer samt kontrollrutiner rundt og automatisering av produksjonsprosess gir ganske få muligheter for at dette kan skje uten å bli oppdaget.

157 Utro tjener putter et annet brev i konvolutten enn det som skulle sendes (utskriftsleverandør)

Prosessen for konvoluttering er fullautomatisert så det er svært liten mulighet for å gjøre dette.

158 Fysisk printutstyr stopper/går i stykker (altså et lengre avbrudd) (utskriftsleverandør)

SLA er avtaleregulert. Utskriftsleverandøren har rutiner og planverk om en slik situasjon skulle oppstå (mulighet for å produsere utskrift på annen lokasjon).

159 Selve innholdet i brevet pakkes i feil konvolutter slik at deler av innholdet (kan være sensitivt) vises i vinduskonvolutten (utskriftsleverandør)

Prosessen med pakking er lik på begge produksjonsmaskiner. Det er en strekkode i venstre marg. Strekkoden påføres når printfilene leses inn. Det har aldri skjedd feil med dette. Pakkemaskinen leser strekkoden og får dermed beskjed om rekkefølgen på dokumentsidene som skal skrives. Ingen erfaringer med feilpakking.

160 Dobbeltprint - innhold printes oppå annet innhold i et og samme brev (utskriftsleverandør)

Printfilene leses inn og printes i en sekvensiell bane på en stor rull, noe som tilsier at dobbelprint i utgangspunktet ikke kan skje. En rull omfatter en forholdsvis begrenset mengde brev avhengig av antall sider i brevet. Dobbelprint har forekommet én gang i forbindelse med en fastsatt tekst som skulle være med i alle brevene i en forsendelse.

161 Fysiske brev forsvinner i transport (transportør)

Uavhengig av hvilken utskriftsleverandør som benyttes. Risikoen er den samme som for vanlig post. Kvalitetskrav til Posten som måles sikrer at dette ikke kan skje for større mengder (etter sortering fordeles posten på x antall trailere, tog, fly).

162 Innstikk/skanning: Svar fra bruker skannes, men tolkes feil, f.eks forskyvning av felter i tolkningsmal eller forskyvning/skjevhet ved innskanning (utskriftsleverandør)
Bruker som fyller ut et skjema skal sette tydelig kryss, men feil kan skje. Skanner er satt opp til presisjonslesning og har erfaringsmessig høy pålitelighet. Skadet brev, f.eks. ved fuktighet, kan fremkalle feiltolkning.

163 Utro tjener leser i post under produksjon/utskrift og misbruker sin viten (utskriftsleverandør)
Fysiske brev eksponeres så lite som mulig for innsyn. Produksjonsprosessen er tilrettelagt på en sånn måte (automatisert, avskjermet og med få manuelle overganger), at det er ganske få muligheter for at få innsyn.

164 Uvedkommende får tilgang og leser post under produksjon/utskrift (utskriftsleverandør)
Produksjonshallene er avlåst og det er kontroll av hvem som går inn og ut. Det er installert overvåkningskameraer ved alle innganger og lokalene har adgangskontroll/adgangskort. Alle produksjonsenheter og prosedyrer er underlagt minimum samme sikkerhetsnivå som alminnelig fysisk post.

165 Utro tjener får tilgang til post under dekryptering av printfiler og misbruker sin viten (utskriftsleverandør)
Dekryptering og rutiner rundt dette adskiller seg ikke rent sikkerhetsmessig fra dekryptering av digital post. Kontrollfunksjoner, logging og håndtering av logg er på minst samme nivå. All lagring av filene skjer kryptert, med unntak av når filene prosesseres og klargjøres for print, og når filene overføres til produksjonsutstyret for fysisk utskrift. Pseudonymisering av data skjer dog i starten av bestillingsflyt, og det er ikke umiddelbart mulig senere å forbinde disse med kunde og person. Printfiler slettes etter printing.

166 Utro tjener leser i post under konvoluttering og misbruker sin viten (utskriftsleverandør)
Prosessen er som utgangspunkt fullautomatisert, og det er få muligheter for at få innsyn. Når det er få brev, kan manuell konvoluttering forekomme. Manuell konvolutteringen foregår etter fastsatte rutiner i leverandørens kvalitetshåndbok og forekommer i under 0,1% av totalvolum. Etter konvoluttering blir brevene oppbevart i lukkede kasser.

167 Uvedkommende får tilgang til printfiler i transitt mellom avsender og utskrifts- og forsendelsestjenesten (utskriftsleverandør)
Sikkerhetsmekanismene mellom avsender og meldingsformidler er de samme som for øvrig digital post. All overføringen av data mellom Posten og underleverandør og overføringer internt hos utskriftsleverandør, skjer over sikre forbindelser. Filene er i tillegg er krypterte og kan kun dekrypteres ved hjelp av utskriftsleverandørens privatnøkkel.

168 Feil under konvoluttering, for eksempel at to brev havner i samme konvolutt (utskriftsleverandør)
Det benyttes et kontrollsystem som sikrer at alle ark havner i konvolutten. Oppstår feil vil det konkrete brev og en andel av brevene før og etter i rekken bli sendt til makulering og produsert på nytt. Det brukes en ANSI tekstfil som styrer konvolutteringen. Leverandøren har hendelseslogger og månedlige møter med alle kunder, og det er ingen rapporterte hendelser fra kunder og mottagere på feil utsendte brev.

169 Driftsavbrudd på grunn av strømsvikt (utskriftsleverandør)
Det er redundans på servere, nettverk og produksjonsmaskineri og sikring mot strømsvikt samt muligheten for failover til annet produksjonslokale. Ved kortere avbrudd avventes strømmens tilbakekomst. Ved lengere tidsavbrudd (katastrofe) kan konvolutter sendes til alternativ produksjonsfasilitet, hvor man kan printe og konvoluttere. Sistnevnte har aldri skjedd.

Risikonivå nye risikoer før tiltak

Konsekvens/ Sannsynlighet		Ubetydelig 1	Moderat 2	Alvorlig 3	Kritisk 4
Sannsynlig Hendelsen inntrer daglig eller oftere	4				
Mulig Hendelsen inntrer en gang i måneden	3		154		
Mindre sannsynlig Hendelsen inntrer årlig	2		148, 149, 152, 155, 162		
Sjelden Hendelsen inntrer omkring hvert 5. år eller sjeldnere	1	158, 161, 169	153, 157, 159, 160, 163, 164, 166, 168	150, 151, 156, 165, 167	

Risikonivå nye risikoer etter mulige tiltak

Konsekvens/ Sannsynlighet		Ubetydelig 1	Moderat 2	Alvorlig 3	Kritisk 4
Sannsynlig Hendelsen inntrer daglig eller oftere	4				
Mulig Hendelsen inntrer en gang i måneden	3				
Mindre sannsynlig Hendelsen inntrer årlig	2		149, 162		
Sjelden Hendelsen inntrer omkring hvert 5. år eller sjeldnere	1	148, 155, 158, 161, 169	152, 153, 154, 157, 159, 160, 163, 164, 166, 168	150, 151, 156, 165, 167	

Fordeling av samlet risikobilde