Oppdatering av enkelte risikohendelser tilknyttet dokument 18/00746

System:	Digital postkasse til innbygger (DPI)
Dato gjennomført:	15. februar til 15. mars 2022
Ansvarlig for gjennomføring:	Petter Teie Hellum, Experis (innleid ressurs) og Ellen Marie Kurås Langen (DigDir)
Sak:	22/00059
Type dokument:	Vedlegg til risikovurderingen 18/00746 - Revisjon av enkelte risikohendelser, knyttet til endring i transportinfrastruktur.
Versjon:	1.0
Siste revisjonsdato:	14.03.2022

Bakgrunn

Risikovurderingene av digital postkasse ble utført i 2014 og journalført på sak 14/00681 i DigDirs arkiv og tilgjengeliggjort på samarbeid.digdir.no. Risikoregisteret for digital postkasse dokumenteres og vedlikeholdes fortløpende. I 2018 ble det gjennomført en ny gjennomgang, og denne ble journalført på sak 18/00746.

Om dette vedlegget til rapporten

I februar og mars 2022 ble det gjennomført nok en revisjon av risiko- og sårbarhetsvurderingen, og denne nye revideringen innebærer en oppdatering av risikohendelser knyttet til ny transportinfrastruktur i DPI. Det følgende dokumentet består av en sammenstilling av de endringer som er gjort i risikohendelsene. Dette dokumentet er ikke tenkt som en fullstendig risikovurderingsrapport, men skal sees i sammenheng med tidligere utført risikovurdering.

For å beholde det nødvendige sammenligningsgrunnlaget før og etter innføring av ny transportinfrastruktur, benytter denne siste revideringen det samme rammeverket for risikovurdering som ved forrige revisjon.

Arbeidsgruppesammensetning

I arbeidet som er gjennomført i februar og mars 2022 har følgende personer vært involvert:

Navn	Rolle/stilling	Virksomhet
Petter Teie Hellum	Prosessleder	Experis AS
Ellen Marie Kurås Langen	Produktsjef	Digitaliseringsdirektoratet
Arild Bjørk	IT-sikkerhetsrådgiver	Digitaliseringsdirektoratet
Sture Førre	Prosjektleder på transportinfrastruktur	Digitaliseringsdirektoratet
Martin Normann Michelsen	Virksomhetsarkitekt på transportinfrastruktur	Digitaliseringsdirektoratet
Steinar Henriksen	Arkitekt på eFormidling	Digitaliseringsdirektoratet

Beskrivelse

For å gjøre det enkelt for forvaltningen å kommunisere digitalt, har DigDir etablert en sikker digital postkasse for innbyggerne (DPI). 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. I forbindelse med revidering av risiko- og sårbarhetsvurderingen i februar og mars 2022 ble denne verdivurderingen gjennomgått på nytt, for å vurdere om det var behov for endringer. Det ble ikke gjort endringer i denne omgangen, og verdivurderingen fra 12.03.2018 ligger derfor til grunn for revideringen fra 2022.

Beskrivelse av løsningen

Beskrivelse av Digital postkasse til innbygger:
https://docs.digdir.no/resources/begrep/sikkerDigitalPost/innledning/
Beskrivelse av ny transportinfrastruktur:
https://docs.digdir.no/dpi_oversikt_index.html

Ny transportinfrastruktur

I gammel DPI-løsning var meldingsformidlingen (etter sending av brev, men før mottak) en sentralisert løsning. I ny transportinfrastruktur er det et uttalt mål at løsningen skal etterleve krav i PEPPOL-standarden[1], og at private aktører kan bidra som tjenesteleverandører i større deler av meldingsflyten. Ny transportinfrastruktur følger en fire-hjørners-modell,[2] hvor avsender og avsenders fagsystem befinner seg i hjørne 1, avsenders aksesspunkt (system avsender kobler seg opp mot for å sende melding) befinner seg i hjørne 2, mottakers aksesspunkt (system mottaker kobler seg opp mot for å hente ned melding) befinner seg i hjørne 3, og mottaker selv (postkasseleverandørene Digipost og E-boks, i tillegg til utskriftsleverandøren (Skatteetaten)) befinner seg i hjørne 4. Alle aktører som agerer som ledd i meldingsflyten, være seg avsender, aksesspunkt eller mottaker, er autorisert for slik interaksjon med løsningen, og dette bidrar til å minimere sannsynligheten for at uvedkommende kan utgjøre en trussel mot konfidensialitet, integritet og tilgjengelighet (KIT).

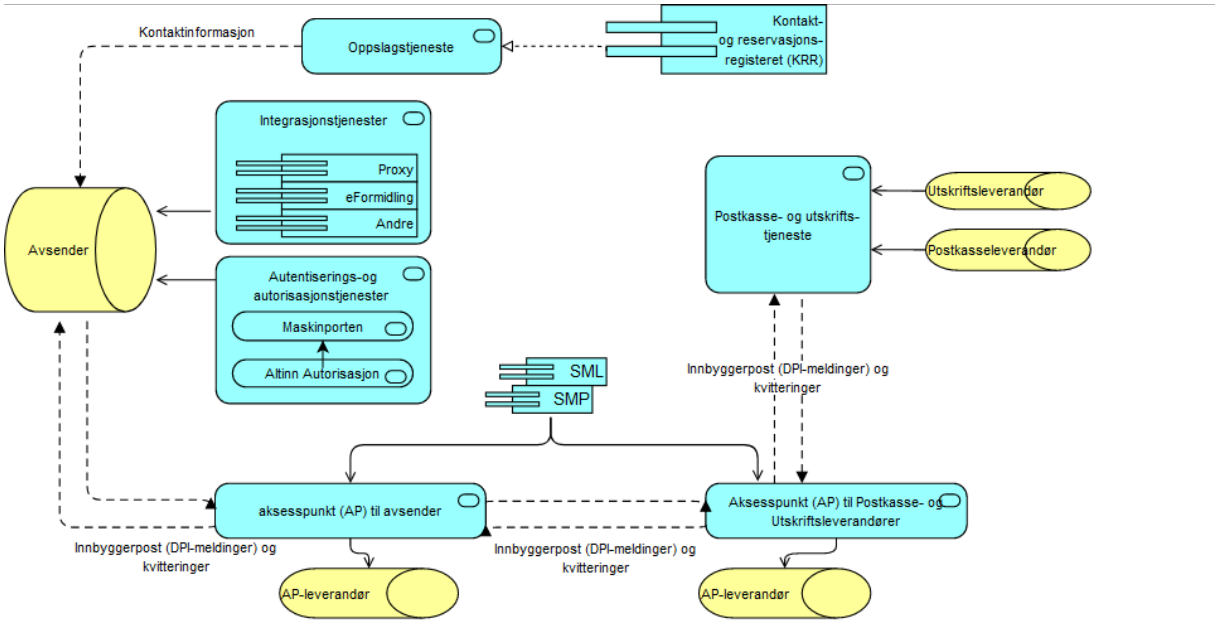
I tillegg til elementene som omtales som de fire hjørnene i avsnittet ovenfor, er nasjonale felleskomponenter tatt i bruk i løsningen. ID-porten benyttes som autentisering av sluttbrukere for lesing av brev hos sine respektive postkasseleverandører, Maskinporten leverer et token som avsender benytter mot sitt aksesspunkt, i tillegg til at Maskinporten kontrollerer at avsender og avsenders fagsystem har lov til å bruke DPI, og Kontakt- og reservasjonsregisteret (KRR) benyttes for å hente oppdatert informasjon om hvilken postkasseleverandør mottaker benytter. Den nasjonale felleskomponenten eFormidling benyttes som integrasjonspunkt for offentlige virksomheters fagsystemer mot avsenders aksesspunkt. På den måten har avsender anledning til å koble opp mot

[1] PEPPOL: https://peppol.eu/downloads/the-peppol-edelivery-network-specifications/
[2] Se arkitekturskisse på side 4.

aksesspunkt uten å sette opp egen API-integrasjon og håndtere pakking av meldinger etter godkjent standard. For andre avsendere som ikke benytter eFormidling må integrasjon settes opp selv.

Arkitekturskisse for ny transportinfrastruktur

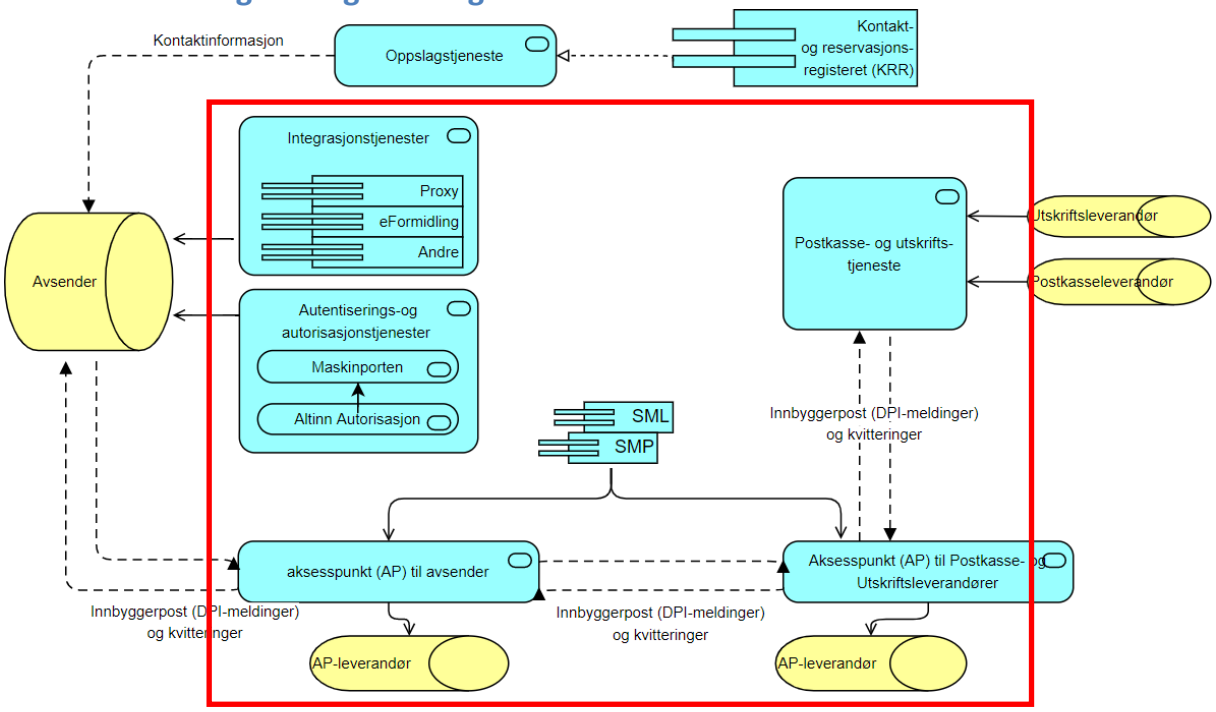
Skissen nedenfor viser den overordnede informasjonsflyten og integrasjonspunktene i DPI, i henhold til hjørnemodellen. Under skissen finnes en enkel beskrivelse av flere av de relevante komponentene i løsningen.



Proxy	Proxy-versjon av klientbibliotekene (java og .net) som brukes i infrastruktur som skal fases ut. Proxy-versjon sender til ny transportinfrastruktur via eFormidling. En enkel måte å komme over på ny infrastruktur på, men er tenkt som en midlertidig løsning da Digdir ønsker å kutte ut klientbiblioteker til fordel for REST. Krever at avsender tar i bruk eFormidling.
eFormidling	eFormidling er en fellesløsning for formidling av meldinger i offentlig sektor. Løsningen krever at avsender setter opp et integrasjonspunkt (komponent i eFormidling). Integrasjonspunktet kommuniserer med et aksesspunkt (AP). Det er laget et sett med REST-kall som avsendere og/eller fagsystemleverandører kan bruke for å sende via eFormidling.
Andre	Det er mulig for avsendervirksomheter å lage egne integrasjoner mot aksesspunktet (AP). Det er også mulig for avsendere og fagsystemleverandører å skaffe egne Peppol-sertifiserte aksesspunktleverandører, eller selv opptre som AP.
Maskinporten	Sikker autentisering og tilgangskontroll for utveksling av data mellom virksomheter. Avsender henter token fra Maskinporten og bruker dette mot sitt AP (Aksesspunkt). Maskinporten kontrollerer at avsender har lov til å bruke DPI. Dersom avsender bruker en databehandler sjekker Maskinporten mot Altinn at databehandler har lov til å sende på vegne av avsender. Token inkluderes i meldingen slik at Postkasse-leverandøren kan motta dette som bevis på tillatelse til å sende post.
Altinn Autorisasjon	Altinn Autorisasjon brukes dersom en avsendervirksomhet har en databehandler som skal sende post på deres vegne. Avsender delegerer tilgangen videre til databehandler i Altinn.
aksesspunkt (AP)	Tjeneste for formidling av elektroniske dokumenter. Aksesspunktet til avsender gjennomfører teknisk validering av Maskinporten-tokenet, identifiserer AP til postkasseleverandørene (ved oppslag i SMP/ELMA) og videreekspederer meldingen ihht Peppol regelverk. Ved returkvitteringer er det aksesspunktet til postkasseleverandør eller utskriftstjenesten som slår opp i SMP/ELMA for å identifisere AP til avsender.
SML	Service Metadata Locator. Sentralt Peppol-register for å finne rett SMP.
SMP	Service Metadata Provider. Register som inneholder data om mottakers dokumenttype, profil og aksesspunkt.

Figur 1 Overordnet konsept og informasjonsflyt for digital postkasse til innbyggere, med beskrivelse av komponenter

Denne revideringens avgrensninger



Det primære formålet med dette dokumentet og den vurderingen som er gjennomført er å avdekke endringer i risikoer etter innføring ny transportinfrastruktur. Risikoer knyttet til bruk av DPI generelt er omtalt i risikovurderingen 18/00746. Risiko som manifesterer seg grunnet avsendervirksomhetenes egne rutiner eller feilbruk, eller risiko for mottaker grunnet konfigurasjon av deres klienter eller mottakers handlinger med egne meldinger er ikke omtalt.

Prosessuell, organisatorisk og avtalemessige risiko relatert til avtaleforhold mellom DigDir, 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 hverken i vurderingen som ble gjort i 2018 eller i revidert versjon fra februar og mars 2022.

Vi har sett bort fra at omkringliggende systemer som ID-porten, maskinporten, Altinn Autorisasjon 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

Overordnet om endring i risikoer

DigDir gjorde i forkant av oppstart av revideringen et uttrekk fra risikoregisteret som er etablert for DPI. **Uttrekket resulterte i en liste på 30 risikohendelser** / scenarier som prosessleder ble bedt om å revidere i lys av ny transportinfrastruktur.

5 av de 30 risikohendelsene har blitt vurdert som ikke relevante etter endring i transportinfrastruktur, og er derfor fjernet. Årsakene til fjerningen er blant annet at hendelsen ikke omhandler informasjonssikkerhetsrisiko, f.eks. ved at de dreier seg om arbeidsforhold eller andre scenerier som ikke kan attribueres til informasjonssikkerhet, eller at hendelsen ikke er relevant etter endring av transportinfrastruktur.

2 av de 30 risikohendelsene er ikke berørt av endringer i transportinfrastruktur, og utelates derfor fra denne risikovurderingen. De kan dermed stå uendret i hendelsesregisteret.

De resterende 23 hendelsene som er behandlet er skrevet om og tilpasset ny transportinfrastruktur, enten ved å gjøre mindre endringer i språk og begrepsbruk, eller ved å gjøre større endringer i hendelsen og etablerte, risikoreduserende tiltak, tilpasset nåsituasjon.

Alle de resterende 23 hendelsene har fått tildelt ny hendelses-ID og har blitt risikovurdert på nytt i lys av endringene. Følgelig bør utfasede risikohendelser fjernes, og nye hendelser legges inn som erstatning for disse. **Noen av hendelsene er slått sammen eller blitt erstattet av færre hendelser. 17 nye risikohendelser erstatter de 23 reviderte**. Nederst i dette dokumentet finnes en fullstendig oversikt over hvilke hendelser som er fjernet, hvilke som er erstattet og hvilke hendelser som skal benyttes i stedet for de erstattede hendelsene.

Oversikt i listeform

Her følger et tabelloppsett over endringer i hendelsesregisteret. Opprinnelig hendelses-ID er listet opp i venstre kolonne. Hvorvidt hendelsen er erstattet av ny og revidert risikohendelse tydeliggjøres i kolonne to, og de hendelser som er slettet uten at de erstattes av en revidert hendelse er markert i kolonne tre. To av hendelsene skal hverken endres eller slettes i denne revideringen, og de er derfor uendret. Disse er markert i kolonne fire. Nye hendelser som erstatter de reviderte er listet opp i kolonne fem.

Opprinnelig ID	Dekkes av ny risikohendelse	Fjernes uten å bli erstattet	Holdes utenfor denne ROS	Ny risikohendelses-ID
11	X			N01
20		X		-
24	X			N02
25	X			N03
26	X			N03
28	X			N04
33	X			N05
56	X			N06
64		X		-
65	X			N04
66	X			N03
68	X			N07
69	X			N07
70	X			N08
73	X			N09
76	X			N10
80	X			N11
81		X		-
99		X		-
103		X		-
106	X			N07
114	X			N04
115	X			N02 og N03
120	X			N12
123	X			N11
130	X			N13 og N14
135	X			N15 og N16
137			X	-
144			X	-
167	X			N17

Trusselaktører

Trusselaktører er ikke like, og det finnes mange metoder for å kategorisere ulike trusselaktører. Her har vi valgt å benytte egenskapene som fremgår av risikohåndteringsguiden til NIST, SP 800-30[3], og lagt til attributten *utholdenhet.* I revideringen som er gjennomført i februar og mars 2022 er det også gjennomført noen endringer knyttet til hvilke trusselaktører man anser som relevante i 2022. Det er viktig å understreke at slike endringer i trusselbildet kun gir et øyeblikksbilde av situasjonen, at vektingen av trusselaktørene kun gjelder for det behandlede analyseobjektet, og at en full gjennomgang av relevante trusselaktører må gjøres ved hver revisjon og ved hver ny risiko- og sårbarhetsvurdering. Nedenfor følger en oversikt over de attributtene arbeidsgruppen anser som særlig relevante for å kunne vurdere hvilken trussel de ulike trusselaktørene kan utgjøre for analyseobjektet og DigDir:

- 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
2 Lav	spesielt rettet mot
1 Meget lav	bestemte individer

Særlig relevante trusselaktører

Nedenfor følger de trusselaktørene arbeidsgruppen anser som mest relevante for analyseobjektet:

Trusselaktør	Evne	Vilje	Målrettet	Utholdende
Fremmed makt	5	2	3	5
Organisert kriminalitet	4	3	1	4
Hacktivister	2	1	1	1
Hacker	2	1	1	1
Utro tjener hos DigDir	5	1	1	1
Utro tjener hos tredjepart/databehandler	5	1	1	1

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

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,
- risikoen stemmer ikke overens med nåværende tekniske løsning,
- risikoer er utenfor scope/rammen for risikovurderingen,
- risikoer tilhører andre felleskomponenter,
- risiko er duplikat av annen registrert risiko,
- uklare risikoer.

11 Melding om virus
Fjernes og erstattes av ny hendelse med ID N01, for å bedre samsvare med ny transportinfrastruktur.

20 Kobler opp mot falsk meldingsformidler, SSL-spoofing. Blir oppdaget på grunn av manglende kvittering, men ikke kryptert informasjon blir eksponert.
Løsningen inneholder ikke informasjon som ikke er kryptert slik risikoen beskriver. Fjernes.

24 Meldingen blir avvist av postkassen
Fjernes og erstattes av ny hendelse med ID N02, for å bedre samsvare med ny transportinfrastruktur.

25 Får ikke bekreftelse på levert melding
Fjernes og erstattes av ny hendelse med ID N03, for å bedre samsvare med ny transportinfrastruktur.

26 Får ikke feilmelding om at melding med særlig viktig informasjon ikke blir levert
Fjernes og erstattes av ny hendelse med ID N03, for å bedre samsvare med ny transportinfrastruktur.

28 En meldinger endres mellom avsender og meldingsformidler
Fjernes og erstattes av ny hendelse med ID N04, for å bedre samsvare med ny transportinfrastruktur.

33 Brukere nekter for å ha mottatt melding og SDP kan ikke opplyse saken
Fjernes og erstattes av ny hendelse med ID N05, for å bedre samsvare med ny transportinfrastruktur.

56 Svært følsom informasjon blir offentlig kjent på grunn av utro tjener i meldingsformidleren (offentlig)
Fjernes og erstattes av ny hendelse med ID N06, for å bedre samsvare med ny transportinfrastruktur.

64 Brev leveres til en falsk postkasseleverandør
Dette kan ikke inntreffe i nåværende løsning, og hendelsen fjernes derfor.

65 Meldinger endres mellom meldingsformidler og postkasse, og det oppdages ikke.
Fjernes og erstattes av ny hendelse med ID N04, for å bedre samsvare med ny transportinfrastruktur.

66 Melding stoppes mellom meldingsformidler og postkasse, og det oppdages ikke.
Fjernes og erstattes av ny hendelse med ID N03, for å bedre samsvare med ny transportinfrastruktur.

68 Kjøling feiler som medfører at systemet er utilgjengelig i en uke.
Fjernes og erstattes av ny hendelse med ID N07, for å bedre samsvare med ny transportinfrastruktur.

69 Strømforsyning feiler som medfører at systemet er utilgjengelig i tre dager.

Fjernes og erstattes av ny hendelse med ID N07, for å bedre samsvare med ny transportinfrastruktur.

70 2-3 dager nedetid pga. manglende eller for liten bemanning i en feilsituasjon.
Fjernes og erstattes av ny hendelse med ID N08, for å bedre samsvare med ny transportinfrastruktur.

73 Bruker bytter postkasse, men meldinger går likevel til hans gamle adresse.
Fjernes og erstattes av ny hendelse med ID N09, for å bedre samsvare med ny transportinfrastruktur.

76 Lekkasjer av informasjon som følge av programvarefeil (Kenneth-saken)
Fjernes og erstattes av ny hendelse med ID N10, for å bedre samsvare med ny transportinfrastruktur.

80 Levering av en kryptert melding til feil mottaker
Fjernes og erstattes av ny hendelse med ID N11, for å bedre samsvare med ny transportinfrastruktur.

81 Meldingsformidler eller postbokstjenesten forstår ikke alvoret i sikkerhetskravene som stilles til tjenesten, og har derfor svak etterlevelse av kravene.
Fjernes. De tjenesteleverandørene som i dag er involvert i tjenesten er svært seriøse aktører, og å skulle sannsynlighetsfeste hvor trolig det er at de ikke forstår kravene fremstår unødvendig.

99 Kryptert backup, med noen opplysninger (metadata) i klartekst, kommer på avveie.
Dette kan ikke inntreffe i nåværende løsning, og hendelsen fjernes derfor.

103 Én eller flere aktører i digital postkasse har ikke tilfredsstillende avtaler med sine ansatte
Fjernes. Krav til ansettelsesavtaler, arbeidsforhold og arbeidsmiljø hos leverandører faller utenfor scope i denne informasjonssikkerhets-risikovurderingen.

106 Digital postkasse blir utilgjengelig for avsender som følge av strømbrudd eller tilsvarende ytre påvirkning
Fjernes og erstattes av ny hendelse med ID N07, for å bedre samsvare med ny transportinfrastruktur.

114 Melding endres mellom postkasse og mottaker
Fjernes og erstattes av ny hendelse med ID N04, for å bedre samsvare med ny transportinfrastruktur.

115 Melding stoppes mellom postkasse og mottaker
Fjernes og erstattes av nye hendelser med ID N02 og N03, for å bedre samsvare med ny transportinfrastruktur.

120 Ved feil er det ikke mulig å følge opp sikkerhetsbrudd pga svak avtale mtp tilsyn/innsyn.
Fjernes og erstattes av ny hendelse med ID N12, for å bedre samsvare med ny transportinfrastruktur.

123 Melding med taushetsbelagte opplysninger mottas av feil mottaker (sendt riktig)
Fjernes og erstattes av ny hendelse med ID N11, for å bedre samsvare med ny transportinfrastruktur.

130 Varsel om feil i digital postkasse til innbyggere eller meldingsformidler blir ikke gitt til virksomhetene.
Fjernes og erstattes av nye hendelser med ID N13 og N14, for å bedre samsvare med ny transportinfrastruktur.

135 Melding kan ikke sendes pga feil i digital postkasse til innbyggere
Fjernes og erstattes av nye hendelser med ID N15 og N16, for å bedre samsvare med ny transportinfrastruktur.

167 Uvedkommende får tilgang til printfiler i transitt mellom avsender og utskrifts- og forsendelsestjenesten
Fjernes og erstattes av ny hendelse med ID N17, for å bedre samsvare med ny transportinfrastruktur.

Nye risikohendelser

Risikohendelsene nedenfor er omskrivninger eller erstatninger for tidligere risikohendelser. De er skrevet om og ny risikovurdering er gjennomført for samtlige hendelser, etter innføring av ny transportinfrastruktur i DPI.

N01 Melding med virus
Erstatter hendelse 11.

N02 Meldingen blir avvist av DPI, i aksesspunkt (hjørne 2), hjørne 3 eller annet ledd i meldingsløpet.
Erstatter hendelsene 24 og 115.

N03 Får ikke bekreftelse på levert melding
Erstatter hendelsene 25, 26, 66 og 115.

N04 Melding endres mellom avsender og mottaker
Erstatter hendelsene 28, 65 og 114.

N05 Brukere nekter for å ha mottatt melding og DPI kan ikke opplyse saken
Erstatter hendelse 33.

N06 Sensitiv informasjon blir offentlig kjent på grunn av utro tjener hos aksesspunktleverandør i hjørne 2 og/eller 3.
Erstatter hendelse 56.

N07 Infrastrukturfeil hos driftsleverandør medfører at systemet blir utilgjengelig i en lengre periode (dager, uker)
Erstatter hendelsene 68, 69 og 106.

N08 Lengre nedetid forårsaket av manglende eller for liten bemanning hos driftsleverandører i en feilsituasjon
Erstatter hendelse 70.

N09 Bruker bytter Digital postkasse, men meldinger går likevel til hans gamle digitale postkasse.
Erstatter hendelse 73.

N10 Lekkasje av informasjon som følge av programvarefeil
Erstatter hendelse 76.

N11 Levering av kryptert melding til feil mottaker
Erstatter hendelse 80.

N12 Ved feil er det ikke mulig å følge opp sikkerhetsbrudd, grunnet svake avtaler om tilsyn/revisjon/innsyn mellom DigDir og tjenesteleverandørene.
Erstatter hendelse 120.

N13 Varsel om feil hos leverandører I DPI, herunder aksesspunktleverandør i hjørne 2 og 3, samt feil hos KRR, maskinporte og Altinn formidles ikke til avsendervirksomhetene
Erstatter hendelse 130.

N14 Overbelastning på aksesspunktleverandører, KRR, maskinporten og/eller Altinn fører til utilgjengelighet på tjeneste.
Erstatter hendelse 130.

N15 Melding kan ikke sendes grunnet nedetid hos tjenesteleverandører i DPI, forårsaket av DDOS-angrep mot disse
Erstatter hendelse 135.

N16 Melding kan ikke sendes grunnet nedetid hos tjenesteleverandører i DPI, forårsaket av ikke-varslet patching eller oppgradering av servere, utenfor SLA.
Erstatter hendelse 135.

N17 Uvedkommende får tilgang til printfiler med opplysninger om meldingsinnhold og innhold I vedlegg.
Erstatter hendelse 167.

Risikonivå etter revidering av risikoregister

Den følgende oversikten viser de nye risikoen som er opprettet gjennom revisjonen i februar og mars 2022. NÅ-risiko for reviderte risikohendelser fremstår slik:

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				
Mindre sannsynlig Hendelsen inntrer årlig	2				
Sjelden Hendelsen inntrer omkring hvert 5. år eller sjeldnere	1	N02, N03, N09, N13, N14, N15, N16	N01, N04, N05, N10, N12, N17	N06, N07, N08, N11	

Risikonivå nye risikoer etter mulige tiltak

Etter fastsettelse av NÅ-risiko for nye hendelser har arbeidsgruppen kommet frem til at risikonivået ligger innenfor akseptabelt nivå, og at innføring av nye, risikoreduserende tiltak ikke er nødvendig. NÅ-risikonivå blir derfor lik REST-risiko, og tabellen på forrige side skal derfor anses som sluttført risikonivå.

Fordeling av samlet risikobilde

I arbeidsgruppens gjennomgang av risikonivå for endret transportinfrastruktur er det ikke gjort noen funn som tilsier at analyseobjektet har et risikonivå som krever ytterligere risikoreduserende tiltak. Alle de vurderte risikohendelsene anses å være innenfor akseptabelt risikonivå, som i DigDirs metodikk betegnes som lavt/grønt. Det er derfor ikke utarbeidet ytterligere tiltak, og NÅ-risiko kan derfor også anses som REST-risiko for denne vurderingen.