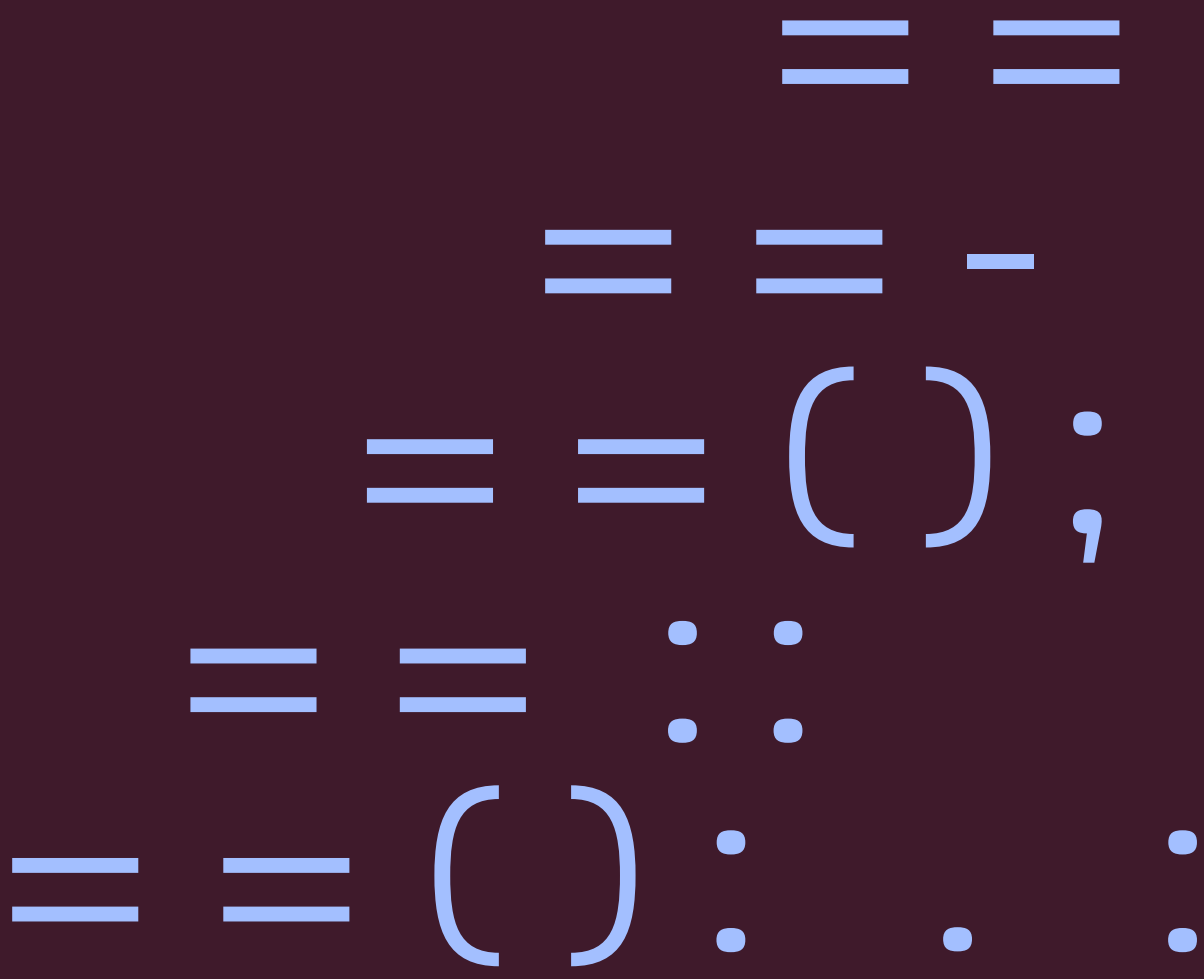
Digitaliserings-
styrelsen

Whitepaper

Sikkerhed i Digital Post-løsningen



Marts 2022

Indhold

1. Indledning 3
1.1 Digital Post-løsningens formål 3
2. Opbygning af Digital Post-løsningen 4
3. Sikkerhedsmekanismer 6
3.1 Sikkerhed for brugere- og myndigheder 6
3.1.1 Kvalitet af meddelelser 6
3.1.2 Sikring af at en meddelelse er modtaget og leveret 6
3.1.3 Uafviselighed 7
3.1.4 Tilgængelighed 7
3.1.5 Validering af afsendere 7
3.1.6 Sikkerhed i løsningens snitflader 8
3.2 Procesmæssig sikkerhed 8
3.2.1 Eksterne sikkerhedsreviews 9
3.3 Sikkerhed i driftsmiljøet 10
3.4 Sikkerhed i udviklingsprocessen 11
3.5 Løbende overvågning 11
4. Dataansvar 12
4.1 Dataansvarskonstruktionen 12
4.2 Lokationskravet og opbevaring af data 13
5. Visningsklienter 14
5.1 Tilslutningsaftale 14
5.2 Selvstændigt dataansvar 14
5.3 Godkendelsesproces 14
5.4 Ændringssproces 15
5.5 Ophør/afslutning af at være en udbyder af en visningsklient 15

1. Indledning

Formålet med denne hvidbog er at formidle et overblik over sikkerheden i Næste generation Digital Post. Sikkerheden skal beskytte fortrolighed, integritet og tilgængelighed af meddelelser og personoplysninger i Digital Post-løsningen.

Læsevejledning
Gennemgangen af sikkerheden i Digital Post-løsningen er opdelt i tre temaer, henholdsvis kontrakten, jura og visningsklienter.

- Kravene til sikkerheden i Digital Post-løsningen er fastlagt i en kontrakt med leverandørerne og efterlever standarden ISO 27001. Med udgangspunkt i kravene beskrives sikkerheden med fokus på teknik og processer i afsnit 2 og 3.
- Ud over kontraktlige sikkerhedskrav regulerer lovgivning dataansvaret for behandlingen af personoplysninger i Digital Post-løsningen, som beskrives i afsnit 4.
- Visningsklienterne, der udgør nye selvstændige indgange til Digital Post-løsningen, beskrives i afsnit 5.

1.1 Digital Post-løsningens formål

Digital Post-løsningens formål kan overordnet beskrives ved:

- Løsningens hovedformål er distribution af Digital Post, adviserings- og NemSMS'er fra offentlige afsendere (myndigheder) til borgere og virksomheder.
- Data der behandles i løsningen udgøres af både personoplysninger og data nødvendige for at distribuere meddelelser. Meddelelserne, der distribueres og opbevares i systemet, indeholder i udgangspunktet alle typer personoplysninger.
- Løsningen skal understøtte over 5 mio. borgere, over 600 myndigheder og over 700.000 virksomheder.

Alt sammen stiller høje krav til it-løsningens sikkerhed, således at data og personoplysninger indeholdt i løsningen behandles forsvarligt i overensstemmelse med gældende regler, lovgivning og kontrakter.

2. Opbygning af Digital Post-løsningen

I dette kapitel beskrives løsningen bag Næste generation Digital Post.

Næste generation Digital Post håndterer distributionen af meddelelser mellem myndigheders afsender- og modtagersystemer, opbevaringen af borgere og virksomheders digitale postmeddelelser i deres postkasser samt udstiller disse via visningsklienter. Løsningen omfatter ikke visningsklienterne, borger.dk, e-Boks, Mit.dk og Virk, der anvendes af borgere og virksomheder til at tilgå den digitale post. Læs nærmere om visningsklienter i afsnit 5.

Løsningen består af følgende 7 kernekomponenter med hver deres sikkerhedsniveau og -fokus:

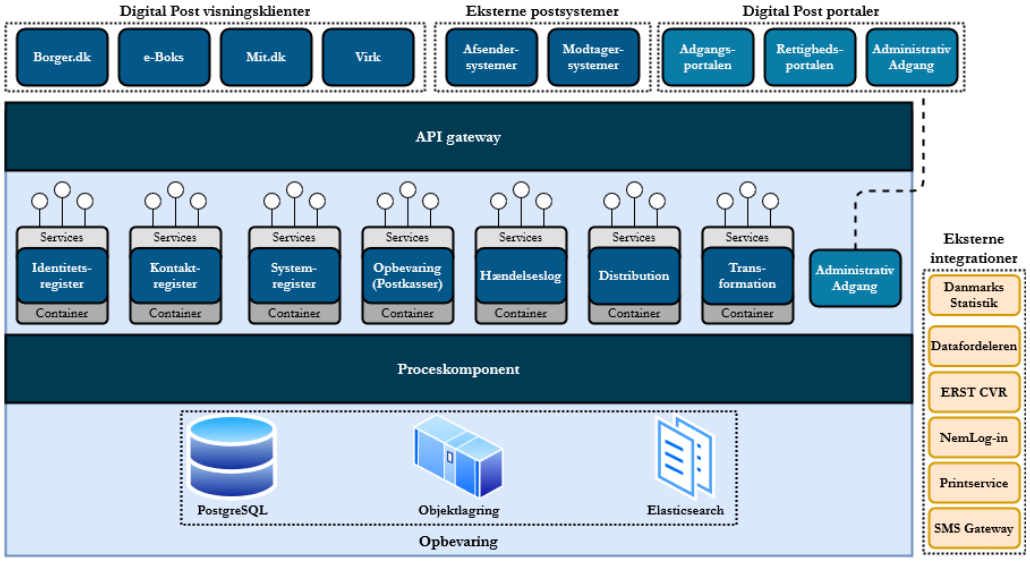
- *Distributionskomponenten*: Når en offentlig afsender ønsker at sende meddelelser til en borger eller en virksomhed, sker dette ved, at myndigheden via dennes afsendersystem sender postmeddelelsen til Digital Post-løsningens Distributionskomponent. Det sker via snitfladerne: REST m. https, SMTP med S/MIME og SFTP. Komponenten står derudover også for udsendelse af adviseringer via e-mail, SMS samt NemSMS og push beskeder.
- *Kontaktregisteret*: Digital Post-løsningen har et såkaldt Kontaktregister, der indeholder oplysninger om tilmeldingsstatus for både Digital Post og NemSMS for borgere og virksomheder samt deres kontaktoplysninger
    - Telefonnummer (valgfri)
    - Almindelige e-mail (valgfri)
    - personnummer eller CVR-nummer.
- *Opbevaringskomponenten*: Modtagelse og efterfølgende opbevaring af borgeres og virksomheders postmeddelelser vil ske i Opbevaringskomponenten, der udgør modtagernes postkasser. Meddelelserne bliver herfra vist via de kommercielle og offentlige visningsklienter, fx for borgere på borger.dk og for virksomheder på Virk. Tilsvarende bliver de meddelelser, som borgerne og virksomhederne sender, opbevaret i opbevaringskomponenten. Komponenten indeholder herudover også information om tilmeldte adviseringer og dertilhørende kanaler; e-mail og/eller SMS.
- *Systemregisteret*: Offentlige afsendere registreres i Digital Post-løsningens Systemregister, der har til formål at registrere, hvilke offentlige afsendere, der må sende og modtage meddelelser via Digital Post-løsningen. Hvis virksomheder ønsker at benytte sig af systemer til at afsende og/eller modtage meddelelser, registreres det også i denne komponent. Systemregisteret indeholder herudover også kontaktstrukturen for de enkelte offentlige afsendere.
- *Hændelseslog*s: Digital Post-løsningen indeholder en Hændelseslog, hvis funktion det er at registrere og udstille information om, hvornår en meddelelse er sendt og hvem der er afsender og modtager. Alle borgere og virksomheder har adgang til en hændelseslog, der vedrører og indeholder data og personoplysninger om dem selv.
- *Identitetsregisteret*: Identitetsregistret har til formål at opbevare alle de identiteter, som bruger Digital Post-løsningen eller som er en del af løsningen. Dette inkluderer systembrugere, eksterne systemer, medarbejdere i virksomheder og borgere samt deres rettigheder i Digital Post-løsningen. Rettigheder, som er tilknyttet de pågældende identiteter,

opbevares også i Identitetsregisteret. Rettighederne indeholder information om, hvad man må foretage sig i Digital Post-løsningen, samt hvilke data man kan få udstillet via en visningsklient.

- *Transformationskomponenten*: Transformationskomponenten har til formål at understøtte transformationen af meddelelser fra det tidligere Digital Post-format til det nye format, MeMo.

Komponenterne er bygget op omkring markedsudbredt standardprogrammel, der sikrer, at komponenterne er baseret på et fundament, der er velafprøvet, skalerbart og sikkert.

Digital Post-løsningen anvender integrationer til følgende tredjeparter: Printservice, Danmarks Statistik, NemLog-in, Datafordeleren (CPR-registeret) og Erhvervsstyrelsens CVR-register. Løsningen anvender også TDC SMS gateway til afsendelse af SMS notifikationer og NemSMS.
De 7 kernekomponenter og integrationsparterne er præsenteret i figuren nedenfor.



Udover Digital Post-løsningens kernekomponenter introduceres med Digital Post-løsningen MeddelelsesModel (”MeMo”), som er et nyt format til udveksling af digitale postbeskeder.

3. Sikkerhedsmekanismer

Dette kapitel indeholder en redegørelse for en række af de sikkerhedsmekanismer, der understøtter og sikrer et højt sikkerhedsniveau i Digital Post-løsningen.

3.1 Sikkerhed for brugere- og myndigheder

3.1.1 Kvalitet af meddelelser

Tillid til kvaliteten af meddelelser i Digital Post-løsningen er central for borgere og virksomheder, der modtager digital post såvel som de offentlige afsendere, der afsender digitale postmeddelelser, og som er afhængige af borgere og virksomheders fortsatte tillid til løsningen. For at sikre kvaliteten af alle meddelelser valideres og virusscannes meddelelserne, og der anvendes det nye MeMo-format, der er med at til at sikre et højt integritetsniveau. Dette er yderligere uddybet nedenfor.

Validering af indhold i meddelelserne

Indholdet af meddelelserne valideres for at sikre, at der ikke anvendes uhensigtsmæssigt indhold – fx HTML med referencer til eksternt indhold, der ikke findes i selve beskeden, og som Digital Post derfor ikke validerer. Der sker validering af de anvendte filtyper for alle vedhæftede filer, så der ikke anvendes filtyper, som er uhensigtsmæssige for modtageren af meddelelsen – fx direkte eksekverbare filer.

Virusscanning af indkommende filer

Ved at virusscanne indkommende filer sikres det i Digital Post-løsningen, at data, som modtages fra eksterne systemer, ikke indeholder malware, virus, eksekverbare filer og andet potentielt skadeligt materiale, inden det opbevares og distribueres. Derigennem beskyttes løsningen også mod kompromittering af eventuelt skadeligt indhold. Løsningen kan ikke bruges som distributionskanal for virus og malware til myndigheder, virksomheder og borgere.

MeMo-formatet

Det nye MeMo-format sikrer, at den digitale post er selvbærende. Det betyder i praksis, at når der sendes i det nye MeMo-format, modificeres meddelelsen ikke efter den er modtaget i løsningen og afleveret hos modtageren. På den måde sikres et højt integritetsniveau for posten, der formidles igennem Digital Post-løsningen, hvor modtageren kan være sikker på, at dét, der modtages, er det præcis samme, der er sendt.

3.1.2 Sikring af at en meddelelse er modtaget og leveret

Vished for at en meddelelse er modtaget og leveret af Digital Post-løsningen, er central for de offentlige afsendere, der har afsendt en postmeddelelse – ligesom vished for, at meddelelsen er modtaget er vigtig for den enkelte borger eller virksomhed. Borgeren og virksomheden kan via deres hændelseslog se hvornår og fra hvilken offentlige afsender, de har modtaget Digital Post.
For at skabe vished hos afsender har Digital Post-løsningen et kvitteringsflow, der sikrer, at der altid bliver kvitteret på for både modtagelse og levering af en afsendt meddelelse. Når en meddelelse er leveret markeres det med en forretningskvittering fra Digital Post-løsningen som betyder, at meddelelsen er lagt ned i borgeren eller virksomhedens postkasse – og dermed gjort tilgængelig for modtageren.

Derudover indeholder løsningen en gensendelsesmekanisme, der sikrer, at meddelelsen altid afleveres og forretningskvittering kan genereres i forlængelse heraf.

3.1.3 Uafviselighed

For at sikre uafviseligheden i Digital Post-løsningen er det et bærende princip, at man ikke gør noget, uden at det bliver registreret i en log.
Uafviseligheden sikres gennem en hændelseslog, der registrer, hvad alle brugere af løsningen foretager sig og samtidig registrer al modtagelse og afsendelse af meddelelser. Hændelsesloggen udstilles til brugerne af løsningen og sikrer dermed gennemskuelighed. For organisationer, der har tilsluttet systemer, er det også muligt at automatisere deres egne kontroller af hændelser foretaget i løsningen via systemintegration til deres hændelseslog.
Leverandørens handlinger i løsningen fx i forbindelse med teknisk vedligehold registreres i en systemlog. Systemloggen skaber sporbarhed og uafviselighed for de handlinger som kræver direkte adgang til løsningens komponenter.

3.1.4 Tilgængelighed

Såvel slutbrugere som myndigheder har behov for, at Digital Post-løsningen har en høj tilgængelighed, der sikrer, at offentlige afsendere kan afsende digitale postmeddelelser til borgere og virksomheder, og som samtidig sikrer, at borgerne og virksomhederne kan tilgå deres Digital Post rettidigt.
For at sikre maksimal tilgængelighed anvender løsningen en høj grad af redundans på alle niveauer fra datacenter-lokationer til infrastrukturkomponenter og videre til applikationskomponenter. Dermed sikres løsningen imod et single-point-of-falure, dvs. at selv hvis en lokation fejler, er det muligt at fortsætte driften via en anden lokation. Den høje grad af redundans sikrer, at myndigheder, virksomheder og borgere oplever en høj tilgængelighed, når de skal anvende løsningen.
Udover redundans er løsningen beskyttet af intrusion prevention-mekanismer og DDoS-beskyttelse som beskrevet i afsnit 3.3.

3.1.5 Validering af afsendere

Et andet centralt aspekt i tilliden til den digitale post er, at borgere og virksomheder kan stole på, hvem afsenderen af Digital Post meddelelsen er. Via autentifikation sikres den korrekte afsender ved hjælp af den fællesoffentlige sikkerhedsinfrastruktur og ved at anvende stærk kryptering og signering af kommunikation.

Anvendelse af den fællesoffentlige sikkerhedsinfrastruktur

Digital Post-løsningens sikkerhed er bygget op omkring den fællesoffentlige it-infrastruktur i form af NemLog-in, NemID og MitID og efterlever National Standard for Identiteters Sikringsniveauer (NSIS). På den måde sikres, at slutbrugere kan identificeres enten ved brug af OCES-certifikater eller Nem-/MitID nøglekort og –apps. Det betyder, at der kontinuerligt sikres viden om og dokumentation for, at afsendere af den digitale post er, hvem de udgiver sig for at være, og at posten kun kan tilgås af de tilsigtede modtagere borgere og virksomheder.

Rettighedsstyring og adgangskontrol

Administration af adgange og rettigheder til at kunne tilgå postkasser eller på anden måde agere i løsningen sker igennem Næste generation Digital Posts egen rettighedsstyring og dertilhørende komponenter. Denne fremgangsmåde er valgt for at kunne understøtte specifikke forretningsbehov som er unikke for Digital Post-løsningen, bl.a. understøttes mere findelte rettigheder og

adgangstyper og mulighed for mere fleksible tildelinger mellem virksomheder og borgere. Med implementeringen af rettighedsstyring er det også muligt at give visningsklienter mulighed for at bygge rettighedsadministration direkte ind i egne brugerrejser.

3.1.6 Sikkerhed i løsningens snitflader

I tillæg til den fællesoffentlige sikkerhedsinfrastruktur anvender Digital Post-løsningen sikre SSH-nøgler til filbaseret kommunikation og sikker API-nøglegenerering i forbindelse med kommunikation til visningsklienterne.

Kryptering og signering

For at sikre de oplysninger, løsningen indeholder, distribuerer og behandler, er den indgående og udgående kommunikation krypteret for derigennem at sikre fortroligheden. Krypteringen gælder indgående kommunikation fra offentlige afsendere, virksomheder og visningsklienter, og udgående kommunikation til integrationer og modtagersystemer. For at sikre en korrekt beskyttelse af informationer der opbevares i løsningen, anvendes stærk kryptering.
Digital Post-løsningen kan modtage meddelelser over forskellige protokoller som alle er krypterede. Konkret sikres de forskellige protokoller på følgende måder:

- Meddelelser der sendes via web service HTTPS (REST) krypteres via certifikater. Til autentifikation af afsender- og modtagersystemer anvendes der certifikater som er en del af den fællesoffentlige sikkerhedsinfrastruktur. Til transportkryptering anvendes der web-certifikater, der er tilknyttet de udstillede services.
- Meddelelser der sendes via filer over SFTP krypteres og sikres via SSH-nøgler. Der anvendes én SSH-brugernavn til unikt at identificere hvert afsender- og modtagersystem.
- Meddelelser der sendes via mail (SMTP) sikres både via transport (TLS) og S/MIME-kryptering for at sikre mod relay-situationer hvor transportkrypteringen i sig selv ikke garanterer end-to-end kryptering. Derudover verificeres det, at meddelelserne er signeret med det korrekte afsendercertifikat.

3.2 Procesmæssig sikkerhed

Digitaliseringsstyrelsen har kravstillet, at leverandørerne skal efterleve ISO 27001 standarden og herunder skal de vedligeholde et ledelsessystem for informationssikkerhed (ISMS).
Ledelsessystemet omfatter den kravstillede løsning dvs. de processer, teknologin og mennesker, der samlet udgør Digital Post-løsningen. Styringen af sikkerheden er baseret på en løbende risikovurdering af den samlede Digital Post-løsning.

Digitaliseringsstyrelsen har sikret, at kraven til ledelsessystemet for informationssikkerhed er forankret bredt i hovedkontraktens krav, illustreret ved følgende figur:

Ansvaret for processer er sikret i "1. Sikkerhedsgovernance", som stiller krav til ledelsesforankring og godkendelsesprocesser af sikkerhedsdokumentationen. Sikkerhedskrav til teknologien er fastholdt i "2. Driftssikkerhed" og "5. Sikkerhedskrav til løsningen". Sikkerhedskrav som vedrører mennesker, der anvender eller administrerer løsningen er fastholdt i "3. Brugerstyring" og "4. Persondatasikkerhed". Endeligt er kontrol og dokumentation af efterlevelse af sikkerhedskravene fastholdt i "6. Sikkerhedspolitik", "7. Audit og revisionserklæringer" og "8. Test af sikkerhed".

Ledelsessystemet for informationssikkerhed består af en række dokumenter som nærmere fastlægger best practise for hvordan, der for Næste generation Digital Post, sker håndtering af bl.a.:

- Samarbejdsmodel for sikkerhedsstyringen
- Beredskabet for håndtering af it-nedbrud og større forstyrrelser
- Årshjul som fastlægger, hvornår løbende processer gennemføres, fx risikovurdering, revision mm.
- Risikovurderingen udført på baggrund af Digitaliseringsstyrelsens model for risikovurderinger
- Revisionserklæringer udført af uafhængig revisor.

3.2.1 Eksterne sikkerhedsreviews

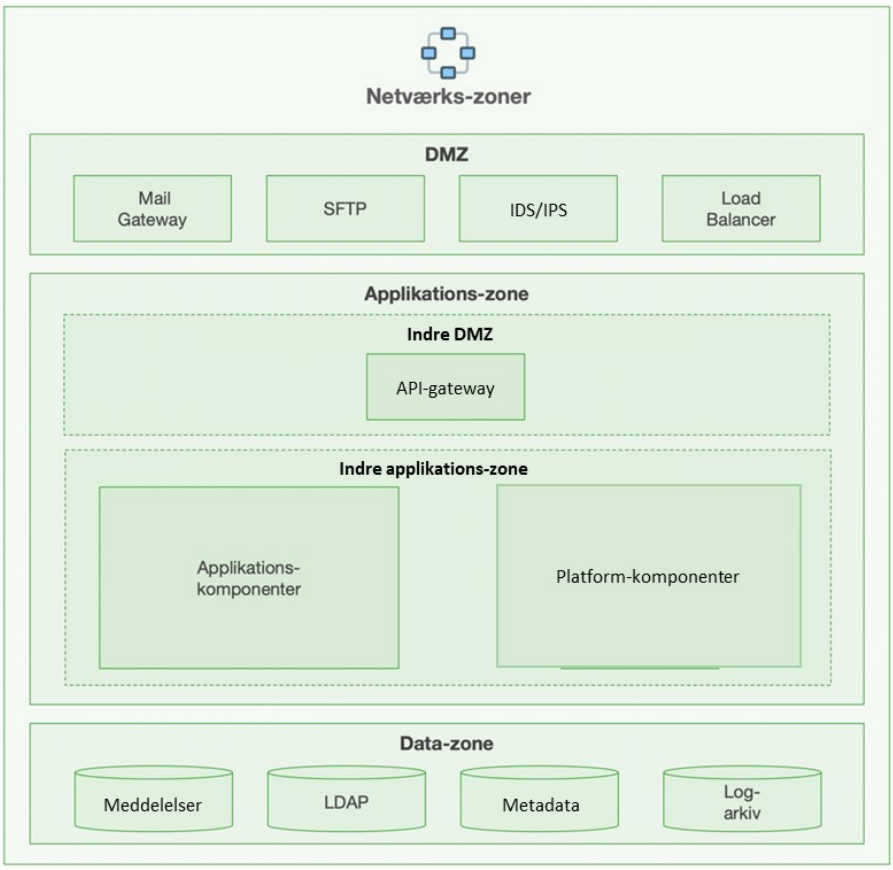
For at sikre at den udviklede Digital Post-løsning også i praksis reelt lever op til de høje sikkerhedskrav, udarbejdes og gennemføres løbende en lang række sikkerheds- og kvalitetstests, ligesom der gennemføres eksterne tilsyn af revisorer med udarbejdelse af revisorerklæringer til dokumentation af Digital Post-løsningens sikkerhed og overholdelse af de databeskyttelsesretlige krav hertil. Løsningens sikkerhed testes også via penetrationstests, udført af en uafhængig

tredjepart. Alt dette foretages i tæt samarbejde med leverandørerne, således at eventuelle fejl og mangler udbedres hurtigst muligt. Både tests og interne audits foretages løbende af leverandøren selv og Digitaliseringsstyrelsen.

3.3 Sikkerhed i driftsmiljøet

Digital Post-løsningen anvender et sikkert driftsmiljø, som benytter flere lag af sikkerhed. Disse lag opnås bl.a. ved hjælp af netværkssegmentering og firewalls på fysisk og logisk niveau. Løsningen beskyttes desuden mod DDoS-angreb på flere niveauer, både på datalinjerne til datacentrene (på internet service provider-niveau) og på firewall-niveau i selve datacentrene.
Der anvendes intrusion detection og prevention-mekanismer, der kan detektere og blokere ondsindet trafik mod løsningen når trafikken rammer ydersiden af løsningen – dvs. før trafikken behandles i selve Digital Post-løsningen. Segmentering af miljøerne i veldefinerede sikkerhedszoner, sikrer isolering af løsningens centrale komponenter. Derudover håndterer løsningen centrale dele af kommunikationssikkerheden gennem en centraliseret API-gateway. API-gatewayen sikrer, at kommunikation fra eksterne rettede snitflader er afkoblet og isoleret i forhold til den bagvedliggende infrastruktur.

Segmenteringen inkl. sikkerhedsmekanismer er afbilledet herunder.



Datacentrene, der anvendes til drift af Digital Post-løsningen, er bygget efter Tier 3+-standarder med høj grad af fysisk sikkerhed, herunder perimetersikring og biometrisk adgangskontrol.

3.4 Sikkerhed i udviklingsprocessen

Digital Post-løsningen er udviklet med stort fokus på sikkerhed, hvilket bl.a. betyder, at sikkerheden er tænkt ind i alle faser af udviklingsprojektet, herunder design, implementering og afprøvning. Den første risikovurdering blev udarbejdet af eksterne sikkerhedseksperter allerede inden udviklingen af løsningen blev igangsat og er løbende blevet vedligeholdt som del af arbejdet med sikkerheden af løsningen. Sikkerhedsaspekter indarbejdes som konkrete acceptkriterier, så der sikres fuldt fokus på sikkerheden under implementeringen og til verifikation i forbindelse med test og godkendelse af delprøver.
Processen for sikker udvikling er værktøjsunderstøttet, så sporbarhed og indblik i potentielle sårbarheder sikres kontinuerligt igennem hele udviklingsprocessen.

3.5 Løbende overvågning

Digital Post-løsningen vil fra lanceringen blive fulgt og overvåget meget nøje med henblik på at sikre, at løsningen er i overensstemmelse med gældende sikkerhedskrav og lever op til gængse sikkerhedsstandarder og best practices. Trafikken overvåges kontinuert og ved mistanke om forsøg på misbrug, er det muligt at iværksætte de rette og nødvendige foranstaltninger.

Digitaliseringsstyrelsen modtager desuden information om nye sårbarheder eller aktive angreb fra Center for Cybersikkerhed og leverandørerne modtager lignende information fra faglige netværk. Input fra disse kilder inddrages i det løbende arbejde med sikring af Digital Post-løsningen.

4. Dataansvar

I dette afsnit afdækkes dataansvaret for de forskellige aktører, der er benytter Digital Post-løsningen.

4.1 Dataansvarskonstruktionen

Digitaliseringsstyrelsen er dataansvarlig for Digital Post-løsningen. Digitaliseringsstyrelsen bliver dataansvarlig for Digital Post-løsningen, idet Digitaliseringsstyrelsen bestemmer formål og afgør med hvilke hjælpemidler, der må foretages behandling af personoplysninger i postløsningen. Det gælder både i forhold til udvikling, drift, vedligeholdelse og forvaltning af Digital Post-løsningen, herunder i forhold til fastlæggelsen af løsningens tekniske og organisatoriske sikkerhedsforanstaltninger. Digitaliseringsstyrelsen er dataansvarlig for behandlingen af personoplysninger i form af personnumre, CVR-numre, e-mail og telefonnumre eller lignende i forbindelse med drift, vedligeholdelse og forvaltning af postløsningen, jf. § 2 a, stk. 1 i lovbekendtgørelse nr. 686 af 15. april 2021 om Digital Post fra offentlige afsendere med senere ændringer (herefter Digital Post-loven).
For så vidt angår indholdet af de digitale postmeddelelser, fastslås det i Digital Post-lovens § 2 a, stk. 3, at de offentlige afsendere er dataansvarlige for indholdet af de meddelelser, de sender via postløsningen, og Digitaliseringsstyrelsen er databehandler for forsendelsen af meddelelser.

Digitaliseringsstyrelsens rolle som databehandler for offentlige afsenders forsendelse af meddelelserne indebærer, at styrelsen i den forbindelse alene behandler personoplysninger indeholdt i postmeddelelserne via instruks fra denne. Digitaliseringsstyrelsen har derfor hverken indflydelse på, hvornår meddelelser er afsendt eller på indholdet af meddelelserne.

I Digital Post-løsningen vil offentlige afsendere blive pålagt at have et modtagesystem. Modtagesystemer indebærer, at opbevaringen af meddelelser alene sker hos offentlige afsender. Digitaliseringsstyrelsen bliver derfor ikke databehandler for opbevaringen.

I § 2 a, stk. 4 fremgår det, at virksomheder er dataansvarlige for indholdet af de meddelelser, de sender via og opbevarer i Digital Post. Digitaliseringsstyrelsen er databehandler for virksomheders forsendelse og opbevaring af meddelelser i postløsningen. Opbevaringen vil ske i virksomhedens digitale postkasse, der udgør en del af Digital Post-løsningen.

Efter modtagelse af digitale postmeddelelser vil borgere og virksomheder være de eneste med råde- og ejendomsret over egen Digital Post. En borger er som udgangspunkt ikke omfattet af anvendelsesområdet for databeskyttelsesforordningen eller retshåndhævelsesloven, jf. hhv. artikel 2, stk. 2, litra c, i databeskyttelsesforordningen og § 1, stk. 1, i retshåndhævelsesloven. Borgeren er dermed ikke i databeskyttelsesretlig forstand dataansvarlig for den digitale post i dennes egen digitale postkasse, uanset om denne post eventuelt måtte indeholde personoplysninger om tredjeparter. Digitaliseringsstyrelsen bliver derfor ikke databehandler for opbevaring af posten i borgerens egen digitale postkasse.

Virksomheder, som modtager Digital Post indeholdende oplysninger om f.eks. virksomhedens kunder eller medarbejdere, er derimod dataansvarlige for de personoplysninger, der opbevares i virksomhedens digitale postkasse. Opbevaringen varetages af Digitaliseringsstyrelsen som databehandler.

Visningsklienter – såvel offentlige som kommercielle – er selvstændigt dataansvarlige for deres behandling af borgere og virksomheders personoplysninger, se nærmere herom nedefor i afsnit 5.2.

4.2 Lokationskravet og opbevaring af data

Det er vurderet, at der i Digital Post-løsningen vil ske behandling af personoplysninger, som på grund af deres karakter eller omfang indebærer en risiko for statens sikkerhed, og it-systemerne skal derfor opbevares i Danmark. Digital Post-løsningen er derfor omfattet af lokationskravet i databeskyttelseslovens § 3, stk. 9.

Lokationskravet medfører, at personoplysninger i Digital Post-løsningen skal opbevares på servere i Danmark, som en integreret del af it-systemet. Der opbevares således ikke personoplysninger uden for Danmark.

For så vidt angår visningsklienter til Digital Post-løsningen, er disse ikke omfattet af lokationskravet. Digitaliseringsstyrelsen har dog besluttet ikke at give mulighed for at hverken kommercielle eller offentlige visningsklientudbydere må opbevare en kopi af data, herunder MeMo og personoplysninger, i regi af deres visningsklienter.

Det er derudover et krav i tilslutningsaftalerne, at visningsklienterne ikke opbevarer personoplysninger, som en borger eller virksomhed fremfinder efter sessionen er afsluttet og borgeren eller virksomheden er logget af visningsklienten.

5. Visningsklienter

I dette afsnit beskrives den nye mulighed for at der etableres visningsklienter, som kan være offentlige eller private tjenester, der viser Digital Post til borgere og virksomheder.

5.1 Tilslutningsaftale

Digital Post-løsningen og § 10, § 10 a og 10 b i lov om Digital Post fra offentlige afsendere muliggør etableringen af visningsklienter, der integreres til Digital Post-løsningen, men som udvikles og driftes af andre end Digitaliseringsstyrelsen.
Digitaliseringsstyrelsen har på sin hjemmeside givet private virksomheder mulighed for at indgå en tilslutningsaftale som kommerciel visningsklient.
Tilslutningsaftalen indeholder en lang række krav, som en udbyder skal dokumentere opfyldt for at kunne opnå adgang til Digital Post-løsningens snitflader og derigennem udvikle og drifte en visningsklient. Kravene går både på forretningsforhold og organisatoriske forhold såvel som mere tekniske aspekter; herunder især konkrete krav til sikkerhed. Den overordnede hensigt med disse krav er først og fremmest at sikre borgere og virksomheder og deres data og personoplysninger bedst muligt, samt at selve visningsklienten sikres tilstrækkeligt og derigennem bidrager til at beskytte Digital Post-løsningen som helhed.
Digitaliseringsstyrelsen indgår ligeledes en tilslutningsaftale med offentlige myndigheder, der gerne vil udvikle en visningsklient.

5.2 Selvstændigt dataansvar

Når Digitaliseringsstyrelsen indgår en tilslutningsaftale med en privat virksomhed, en såkaldt kommerciel visningsklient, eller en offentlig myndighed, en såkaldt offentlig visningsklient, vil den pågældende visningsklientudbyder behandle en række personoplysninger, når borgere og virksomheder vælger at læse sine digitale postmeddelelser via deres visningsklient.
En visningsklientudbyder er selvstændigt dataansvarlig for den behandling af personoplysninger, som er nødvendig for at en borger eller virksomhed kan få vist sin post. Det er den pågældende visningsklientudbyder, der vurderer, hvilke personoplysninger, som udbyderen finder det nødvendig at behandle for driften, vedligeholdelsen og administrationen af deres visningsklienten (fx kontaktoplysninger i form af navn, e-mails og telefonnumre mv.). Visningsklientudbyderen er ikke dataansvarlig for personoplysninger indeholdt i meddelelserne fra offentlige afsendere, se nærmere herom i afsnit 4.1.

5.3 Godkendelsesproces

For at kunne blive godkendt som kommerciel visningsklient af Digital Post fra offentlige afsendere skal en udbyder af en kommerciel visningsklient igennem en godkendelsesproces bestående af to dele:

- Basisgodkendelse
- Løsningsgodkendelse.

I basisgodkendelsen får visningsklientudbyderen godkendt sin overordnede forretningsidé og de heri indeholdte supplerende ydelser, drift og support mv.

I løsningsgodkendelsen erklærer udbyders revisor, ved tro og love, at udbyders løsningsbeskrivelse, herunder teknik og sikkerhed, drift og support, ligger inden for rammerne af den godkendte forretningsidé (basisgodkendelsen). Digitaliseringsstyrelsens opgave i forbindelse med løsningsgodkendelsen er at sikre at alle formalia, herunder revisorerklæringer, dokumentation for løsningsgodkendelsen og idriftsættelseserklæringer er korrekt udfyldt. Når udbyder har fået sin løsningsgodkendelse er denne godkendt til at vise Digital Post fra offentlige via sin visningsklient.

5.4 Ændringssproces

Digitaliseringsstyrelsen skal til enhver tid sikre, at der er et opdateret grundlag for basisgodkendelsen og løsningsgodkendelsen for en given visningsklient. I tilslutningsaftalen er det udbyders ansvar at gøre Digitaliseringsstyrelsen opmærksom på, hvis der er forhold i udviklingen af udbyders visningsklient, som gør at vilkår og rammer for godkendelsen har ændret sig.

Digitaliseringsstyrelsen skal via dialog med udbyderen vurdere om en given ændring vil kunne håndteres som en mindre ændring, dvs. opdatering af afgrænsede afsnit i relevante bilag, eller om der vil være behov for en ny godkendelsesproces.

5.5 Ophør/afslutning af at være en udbyder af en visningsklient

Proces for ophør igangsættes idet Digitaliseringsstyrelsen konstaterer, at ét eller flere af følgende forhold er indtruffet for en udbyder:

1. Udbyder opfylder ikke kravene til bistand i forbindelse med tilsyn eller anden bistand
2. Udbyder opnår ikke fornyet godkendelse
3. Udbyder opfylder ikke længere tilslutningsaftalen og dennes krav til visningsklienter
4. Udbyder leverer ikke den årlige revisorerklæring, uden anmærkninger og/eller inden for den fastlagte frist
5. Der konstateres væsentlige mangler i revisorerklæringer
6. Udbyders drift af visningsklienten har en sådan karakter, at det indebærer en risiko for kompromittering af slutbrugerens meddelelser og/eller personoplysninger
7. Udbyders handlinger kan medføre, at den samlede tillid til Digital Post-løsningen lider skade.

Digitaliseringsstyrelsen kan vælge at suspendere adgang til Digital Post-løsningen. Denne mulighed vil Digitaliseringsstyrelsen kunne tage i anvendelse, såfremt der indtruffet et forhold, der indebærer en risiko for kompromittering af personoplysninger eller at udbyders handlinger kan medføre at den samlede tillid til Digital Post-løsningen lider skade.

Digitaliserings-
styrelsen