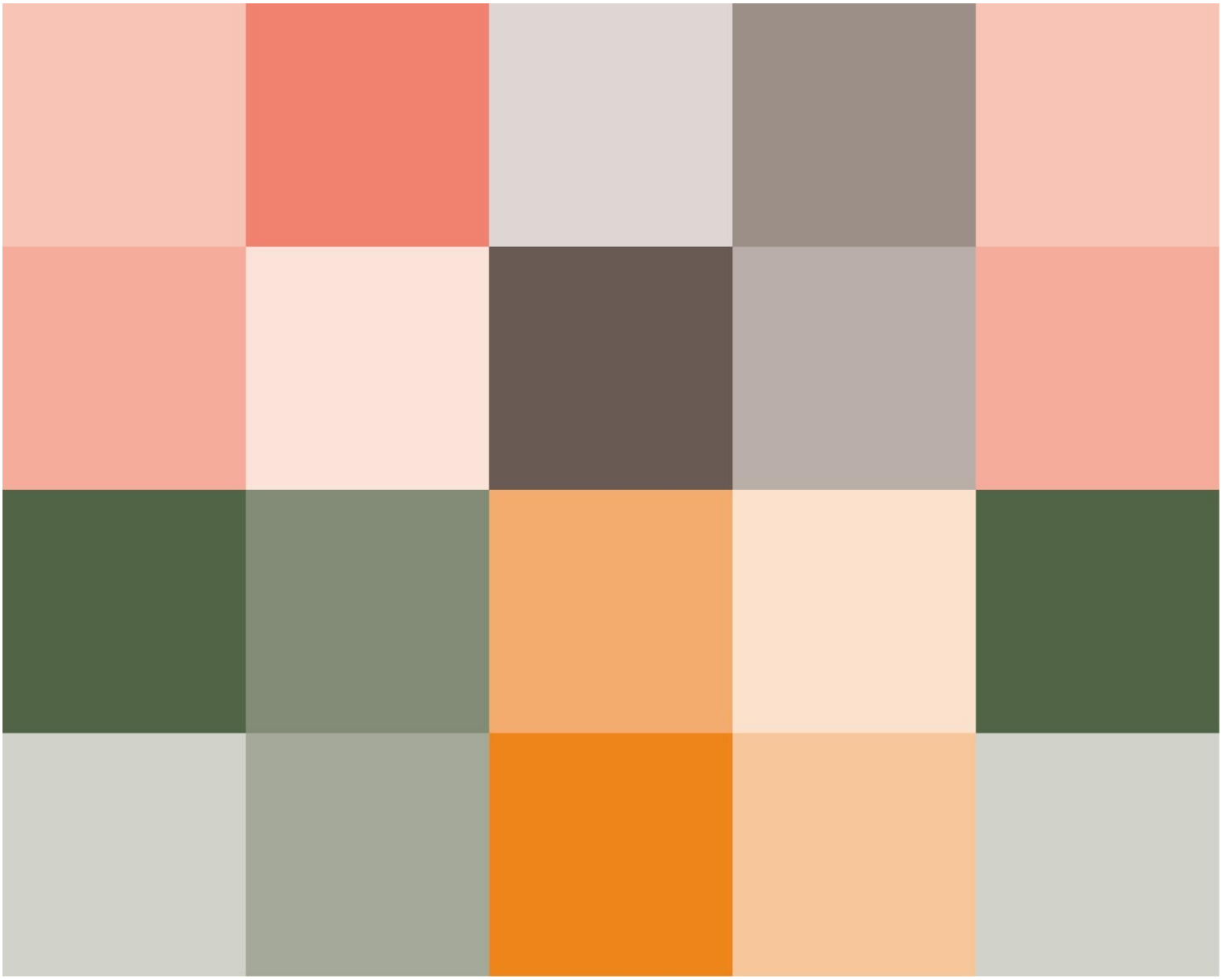


Översyn av infrastrukturen för säkra elektroniska försändelser

Rapportering av uppdrag

15 december 2022

Dnr I2022/01309

DIGG:s dnr 2021-2901

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Myndigheten för digital förvaltning (Digg) har fått i uppdrag att, mot bakgrund av det säkerhetspolitiska läget, genomföra en översyn och analys av infrastrukturen för säkra elektroniska försändelser, kallad Mina meddelanden, och den statliga digitala brevlådan Min myndighetspost. I uppdraget ingår att lämna förslag för att öka robustheten i systemet och säkerställa leverans av digital post i såväl fredstid som under krig och krigsfara.

Digg har i samarbete med Skatteverket genomfört en nulägesanalys av infrastrukturen med fokus på teknik, funktionella behov, risker och säkerhet, samt behov av regelutveckling. För att få ytterligare kunskap om infrastrukturen ska användas i händelse av höjd beredskap och krig behövs en totalförsvarsanalys genomföras av hela Diggs verksamhet. I händelse av att Diggs totalförsvarsanalys utmynnar i att hela eller delar av infrastrukturen är av betydelse vid höjd beredskap eller krig måste det genomföras en konsekvensanalys av vad det innebär för Mina meddelanden.

Den analys som Digg genomfört visar att det finns funktionella behov, risker och brister i dagens infrastruktur som behöver åtgärdas. Det gäller främst krav på ökad säkerhet och robusthet men även möjligheten att göra anpassningar för att möta behov från såväl avsändare som mottagare.

Digg anser att ytterligare författningsreglering skulle kunna göra infrastrukturen säkrare och mer robust. Som exempel nämns regler om sekretess och tystnadsplikt, tillsyn, sanktionsmöjligheter och särskilda regler vid krig och krigsfara samt för att tillgodose totalförsvarets behov. Digg anser också att personuppgiftsansvaret inom infrastrukturen bör regleras i författning. Vidare bör Digg ges i uppdrag att tillhandahålla den statliga digitala brevlådan Min myndighetspost.

Det finns flera tekniska och organisatoriska risker i dagens infrastruktur som medför potentiell risk för angrepp av olika slag i syfte att förändra, förstöra, otillgängliggöra och övervaka information i infrastrukturen. Digg anser att åtgärder i dagens infrastruktur inte är tillräckliga för att hantera identifierade brister och risker för att upprätthålla en robust och säker lösning över tid. Mot bakgrund av detta föreslår Digg att dagens infrastruktur genomgår en större transformation för att lösa flera utmaningar samtidigt och skapa en mer

ändamålsenlig och effektiv infrastruktur för framtiden. Digg ser gärna att regeringen ger förutsättningar för att skyndsamt påbörja denna transformation.

Framtidens infrastruktur för digital post i den offentliga förvaltningen ska säkerställa leverans av digital post vid var tid. Infrastrukturen ska utformas för att vara framtidssäker och vid var tid uppfylla gällande lagstiftning och säkerhetskrav, samt kunna möta potentiella krav som ställs på infrastrukturen i händelse av höjd beredskap och krig.

De centrala funktionerna som utgör kärnan i den föreslagna nya infrastrukturen för digital post är central meddelandehantering med central lagring och visningsklienter.

Med en central meddelandehantering finns samtliga meddelanden som skickas inom infrastrukturen lagrade på ett (1) ställe. Det är till den centrala meddelandehanteringen som mottagarens försändelser skickas. För att säkerställa skyddet av data och individens tillgång till försändelser över tid förespråkar Digg att den centrala meddelandehanteringen tillhandahålls i statlig regi. Till meddelandehanteringen ansluts sedan så kallade visningsklienter som är den tjänst som visar försändelser som finns lagrade i det centraliserade meddelandelagret för mottagaren. Digg anser att staten ska tillhandahålla en sådan visningsklient, men att det även bör finnas en marknad för privata aktörer att erbjuda visningsklienter.

Digg bedömer att den föreslagna lösningen åtgärdar de brister och risker som identifierats, genom att:

- Skapa en säkrare elektronisk kommunikation mellan avsändare och mottagare.
- Ge förutsättningar för att hantera behov av förändringar på ett effektivt sätt.
- I högre grad än i dag tillgodose juridiska och säkerhetsmässiga risker, dels utifrån ett nuläge där sekretess och dataskydd är i fokus, dels inför en situation att Sverige skulle ställas inför höjd beredskap och krig.

Utvecklingen av infrastrukturen enligt förslag förutsätter att Digg ges ytterligare finansiering samt att författningsändringar genomförs. Hela utvecklings- och investeringskostnaden är estimerad till ca 162 miljoner kronor.

Innehållsförteckning

1 Inledning

1.1 Digg tillhandahåller infrastrukturen Mina meddelanden

Myndigheten för digital förvaltning (Digg) har i uppdrag att tillhandahålla en myndighetsgemensam infrastruktur för säkra elektroniska försändelser från myndigheter till enskilda.[1] Digg har också i uppgift att främja användningen av infrastrukturen.[2]

Namnet på infrastrukturen som myndigheter och enskilda ansluter till är Mina meddelanden. Till infrastrukturen är också flera digitala brevlådor anslutna. Det är genom de digitala brevlådorna som enskilda kan ta del av de säkra elektroniska försändelserna som anslutna myndigheter skickar till enskilda.

Digg tillhandahåller den statliga digitala brevlådan Min myndighetspost.

1.2 Uppdrag att genomföra en översyn av Mina meddelanden och Min myndighetspost

I juni 2022 gav Regeringen Digg uppdrag att göra en översyn av infrastrukturen Mina meddelanden och den statliga brevlådan Min myndighetspost. Uppdraget ska slutredovisas till Regeringskansliet senast 15 december 2022.[3]

Av uppdraget framgår att Digg, mot bakgrund av det säkerhetspolitiska läget, ska genomföra en översyn och analys av Mina meddelanden och Min myndighetspost. Översynen ska omfatta en genomgång av den befintliga infrastrukturen i syfte att utröna om den är ändamålsenlig och kostnadseffektiv. Eventuella brister ska identifieras och i de fall de ryms inom uppdraget åtgärdas. Befintliga avtalsstrukturer och beroenden ska analyseras och utvärderas.

Digg ska beräkna kostnader och analysera behov av regelförändringar för utveckling av infrastrukturen och den statliga brevlådan samt lämna förslag på hur infrastrukturen kan utvecklas för att öka robustheten i systemet och säkerställa leverans av digital post i såväl fredstid som under krig och krigsfara.

---

[1] 1 § förordning (2018:357) om infrastruktur för säkra elektroniska försändelser.

[2] 4 § första punkten förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning.

[3] Regeringens beslut den 7 juni 2022 om ändring av regleringsbrevet för budgetåret 2022 avseende Myndigheten för digital förvaltning, I2022/01309.

I arbetet ska Digg beakta den utveckling som sker inom ramen för uppdraget att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte (I2022/00102).

Genom denna rapport slutredovisar Digg uppdraget till Regeringskansliet.

2 Beskrivning av infrastrukturen

2.1 Infrastrukturen Mina meddelanden

Digg tillhandahåller infrastrukturen Mina meddelanden för att myndigheter ska kunna skicka säkra elektroniska försändelser till enskilda. Under åren 2011 till 2019 hade Skatteverket uppdraget att tillhandahålla Mina meddelanden. Sedan hösten 2019 sker verksamhetsförvaltning och verksamhetsutveckling hos Digg medan IT-drift, IT-utveckling och IT-förvaltning utförs av Skatteverket på uppdrag av Digg.

Mina meddelanden är inte en enskild tjänst som utförs av en enskild aktör, utan består av ett antal samverkande tjänster som via Förmedlingsadressregistret (FaR), regelverk och specifikationer möjliggör för anslutna myndigheter att skicka säkra elektroniska försändelser till enskilda. Brevlådeoperatörerna tar emot de försändelser som skickas från anslutna myndigheter och tillgängliggör dem för enskilda i dennes digitala brevlåda.

Mina meddelanden har tre nivåer av skyddsåtgärder som i Allmänna villkor omnämns som skyddsklasser, där skyddsklass 3 är den högsta. Varje avsändare är skyldig att informationssäkerhetsklassificera den information som ska skickas via Mina meddelanden och samtliga brevlådeoperatörer som är anslutna till Mina meddelanden ska kunna hantera meddelanden av skyddsklass 1, 2 och 3. Kraven för de olika skyddsklasserna är av övergripande karaktär och ställs på Brevlådeoperatörens organisation, processer och rutiner, medan vissa är specifika för en viss skyddsklass.

Mina meddelanden består huvudsakligen av följande komponenter:

- Förmedlingsadressregistret (FaR). I FaR hanteras bland annat:
    - person- eller organisationsnummer för den enskilde brevlådeinnehavaren.
    - uppgift om vilken brevlådeoperatör den enskilde har valt.

- Regelverk i form av anslutningsavtal samt allmänna villkor för Mina meddelanden inklusive bilagorna:
    - Bilaga 1: Krav på säkerhet för Brevlådeoperatörer
    - Bilaga 2: Skyddsklasser
    - Bilaga 3: Definitioner
    - Bilaga 4: Servicenivåer (SLA)
- Tekniska specifikationer (API:er) som reglerar hur de olika aktörerna ska interagera med varandra.

2.2 Aktörer inom infrastrukturen

2.2.1 Infrastrukturansvarig

Som Infrastrukturansvarig för Mina meddelanden har Digg ett övergripande ansvar för infrastrukturen, vilket innefattar drift och förvaltning av Förmedlingsadressregistret (FaR), tekniska specifikationer och avtalsstrukturer. Vidare tillhandahåller Digg regelverket för infrastrukturen vilket huvudsakligen består av allmänna villkor med tillhörande bilagor. Ansvaret omfattar även att:

- vara avtalsombud mellan avsändare och brevlådeoperatörer,
- genomföra granskningar av nya brevlådeoperatörer för att säkerställa att de lever upp till de villkor Digg har ställt för att få ansluta,
- utveckla infrastrukturen, samt
- främja användningen av Mina meddelanden.

Digg har vidare i egenskap av Infrastrukturansvarig rätt att utföra kontroll av anslutna parter för att säkerställa att de uppfyller krav och åtaganden i Allmänna villkor över tid.

2.2.2 Brevlådeoperatörer

Det finns flera leverantörer av brevlådetjänster för digital post, så kallade brevlådeoperatörer, anslutna till infrastrukturen. Det är möjligt för den enskilde att själv välja i vilken av de anslutna digitala brevlådorna man vill ta emot sina meddelanden som skickas genom infrastrukturen. Samtliga brevlådeoperatörer

kräver att användaren identifierar sig med en e-legitimation med tillitsnivå 3, enligt Tillitsramverket för svensk e-legitimation.[4]

Brevlådorna hanterar:

- Mottagning och tillgängliggörande av meddelanden.
- Lagring av meddelandet i brevlådedatabasen.
- Mottagningskvittens till avsändaren.
- Avisering till mottagare om nytt meddelande.
- Möjligheten för enskilda att registrera och avregistrera sig hos Infrastrukturansvarig, samt att ändra uppgifter hos Infrastrukturansvarig.

2.2.2.1 Min myndighetspost

Min myndighetspost är statens digitala brevlåda som tillhandhålls av Digg. På uppdrag av Digg tillhandahåller Skatteverket förvaltning och IT-drift av tjänsten. Min myndighetspost hanterar enbart meddelanden från de myndigheter som är anslutna till infrastrukturen. Både privatpersoner och företag kan välja Min myndighetspost som sin digitala brevlåda.

Den statliga brevlådan är en garanti för att det alltid ska finnas en digital brevlåda ansluten till Mina meddelanden för att kunna ta emot och tillgängliggöra digital post från myndigheter till enskilda.

2.2.2.2 Privata brevlådeoperatörer

Det finns idag tre privata brevlådeoperatörer som är anslutna till Mina meddelanden. Kivra anslöt 2015, Billo och Fortnox anslöt i 2022. Digimail och e-Boks har varit anslutna men valt att lämna på egen begäran 2022.

Kivra erbjuder både privatpersoner och företag en digital brevlåda. Billo vänder sig endast till privatpersoner. Fortnox vänder sig enbart till företag.

Brevlådeoperatörer ansöker hos Digg om att ansluta till infrastrukturen. Den leverantör som godkänns ingår sedan anslutningsavtal med Digg och åtar sig därigenom att följa de allmänna villkoren för infrastrukturen.

---

[4] https://www.Digg.se/digitala-tjanster/e-legitimering/tillitsnivaer-for-e-legitimering/tillitsramverk-for-svensk-e-legitimation

Tabellen nedan visar marknadsandelen avseende mottagare per brevlådeoperatör.

Brevlådeoperatör	Marknadsandel mottagare
Kivra	94 %
Min Myndighetspost	6,0 %
Billo (ansluten 2022)	0 %
Fortnox (ansluten 2022)	0 %

Tabellen visar att 94 procent av brevlådeinnehavarna har valt Kivra, vilket betyder att Kivra hanterar den digitala myndighetsposten för över fem miljoner privatpersoner.

2.2.3 Avsändare - myndigheter

Myndigheter kan ansluta till infrastrukturen för att skicka digital post till enskilda. Med myndigheter avses alla statliga, kommunala samt regionala organ. I denna rapport används begreppet myndigheter vilket alltså omfattar även regioner och kommuner.

Myndigheter ansluter till infrastrukturen genom att teckna anslutningsavtal med Digg och förbinder sig därigenom att följa allmänna villkor för infrastrukturen.

Avsändande myndighet kan på egen hand hantera meddelandeförmedlingen, eller anskaffa en tjänst för förmedling av en extern tjänsteleverantör, för att skicka meddelanden till den brevlådeoperatör som finns registrerad för mottagaren hos Infrastrukturansvarig.

2.2.4 Mottagare - enskilda

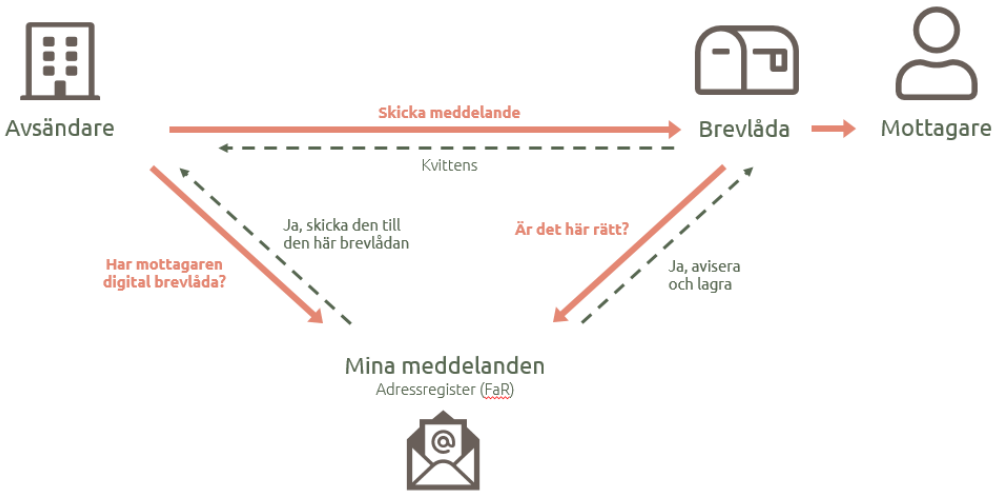
Mottagare av meddelanden är enskilda, vilket i dagsläget innebär en privatperson eller ett företag. Mottagaren ansluter sig till infrastrukturen genom att välja en ansluten brevlådeoperatör, registrerar sig hos denna och godkänner användarvillkoren för Mina meddelanden samt brevlådeoperatörens användarvillkor.

2.3 Hur fungerar Mina meddelanden?

När en ansluten myndighet har skapat ett meddelande (exempelvis ett beslut eller annan information) kan den välja att skicka meddelandet till den enskilde genom Mina meddelanden. Myndigheten ställer då en fråga till Förmedlingsadressregistret (FaR) för att få veta om den enskilde har en digital brevlåda, vilken brevlådeoperatör denne valt och om den enskilde vill ta emot digital post från just den myndigheten. Om den enskilde har en digital brevlåda och vill ta emot digital post från myndigheten skickar myndigheten meddelandet till den valda brevlådeoperatören. Brevlådeoperatören säkerställer då, genom en

kontroll mot Förmedlingsadressregistret (FaR), att den enskilde har valt denne som brevlådeoperatör och att denne vill ta emot digital post från myndigheten. Om så är fallet tillgängliggör brevlådeoperatören omedelbart meddelandet för mottagaren i dennes digitala brevlåda. Avsändande myndighet erhåller också en kvittens från brevlådeoperatören om att meddelandet levererats till mottagaren.

Nedan illustreras meddelandeflödet från avsändande myndighet till enskild.



2.4 Användning

Under år 2022 förväntas över 100 miljoner meddelanden skickas med hjälp av Mina meddelanden. Idag är 232 avsändare är anslutna till infrastrukturen samt ca 5,7 miljoner privatpersoner och ca 187 000 företag.

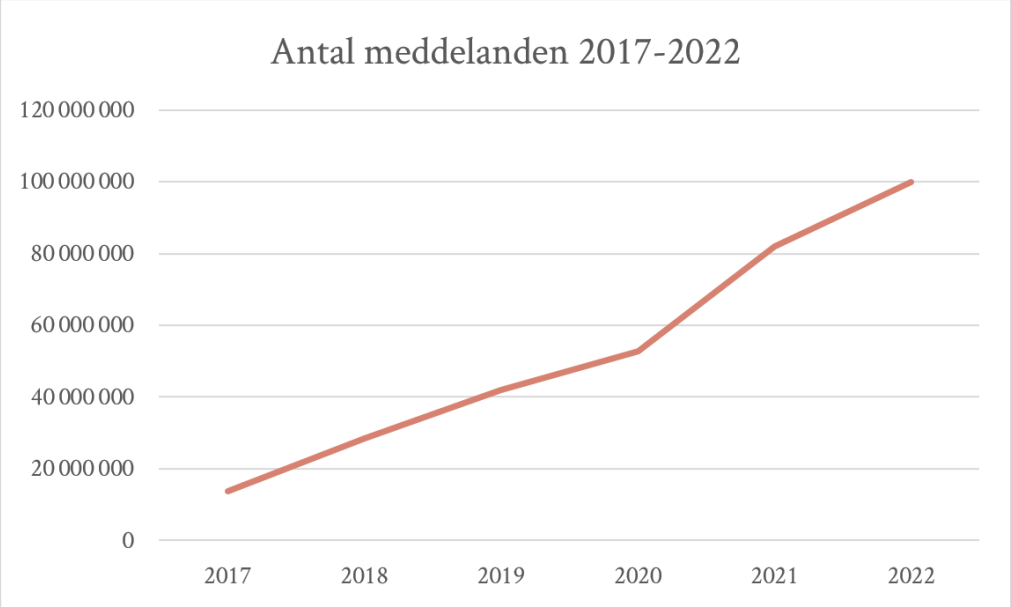
Tabellen nedan visar användningen av Mina meddelanden under år 2020 till 2022.

Användning	2022 -prognos	2021	2020
Meddelanden	100 000 000	81 934 098	52 770 330
Mottagare, privatpersoner	5 700 000	5 312 238	4 193 877
Mottagare, företag	187 000	160 661	133 986
Avsändare statliga myndigheter	62	57	56
Avsändare regioner	13	13	11
Avsändare kommuner	147	116	90
Avsändare kommunförbund	10	8	8

Anslutningarna till infrastrukturen ökar och bland avsändare är det framförallt kommuner som tillkommer.

Diagrammet nedan visar utvecklingen av antalet meddelanden som skickas via infrastrukturen 2017–2022. Antalet meddelanden har ökat i takt med att fler

aktörer anslutit sig, både avsändare och mottagare. Ökningen under 2021 hade primärt med lanseringen av covidbeviset att göra.



2.5 Nytta

Kostnaden för avsändarna för att skicka post digitalt är betydligt lägre än att skicka analog post. Idag är det inte förenat med någon avgift att ansluta till och skicka digital post via Mina meddelanden. De kostnader som uppstår hos anslutande myndigheter är kopplade till tekniska integrationer. Kostnadsbesparingarna är främst portokostnader men även kostnader för hantering av fysiska utskick. Ytterligare besparingar och nyttor är minskad miljöbelastning tack vare minskade transporter och minskat behov av papper, snabbare och säkrare utskick samt att mottagaren får sin post samlad på ett säkert sätt varhelst denne är i världen.

Digg räknar med en besparing på minst tre kronor per försändelse om post skickas digitalt i stället för att skickas med fysisk post. Det innebär en besparing under år 2022 på ca 300 000 000 kr för de anslutna myndigheterna. Denna besparing är beräknad utifrån dagens användning av digital post. Enligt *Uppföljning av statliga myndigheters digitalisering 2021*[5] är det fortfarande en betydande andel av de statliga myndigheterna som skulle kunna använda digital post för utskick till enskilda, men som inte är anslutna till infrastrukturen, och Digg bedömer därför att det

[5] Digg, Uppföljning av statliga myndigheters digitalisering 2021, En enkätundersökning, dnr: 2021-2731

finns stora möjligheter till ytterligare besparingar om flera statliga myndigheter, kommuner och regioner ansluter till Mina meddelanden.

Snabbare och säkrare post kan i sin tur bidra till nyttor i andra led, till exempel minskade antal missade sjukvårdsbesök till följd av utebliven eller försenad post.

För myndigheter är alternativet till att skicka digital post via Mina meddelanden antingen att bygga egna meddelandelösningar eller att anskaffa en digital post-tjänst på den privata marknaden.

3 Nulägesanalys

3.1 Digital post i dagens samhälle

3.1.1 Digitalisering förändrar kommunikationsvanor

I PTS-rapport *Svensk postmarknad 2022* beskrivs att samhällets digitalisering har lett till stora förändringar i användarnas kommunikationsvanor. Under de senaste årtiondena har det i en allt högre grad skett en förflyttning från skriftlig kommunikation till digital kommunikation och antalet brevförsändelser minskar för varje år. Allt fler företag och privatpersoner väljer att kommunicera via digitala kanaler, och ett ökande antal myndigheter, kommuner och regioner väljer att kommunicera med medborgare via digitala brevlådor.[6] Internetstiftelsens undersökning *Svenskarna och internet 2022* visar att nära 7 av 10 använder digitala brevlådor.[7]

Regeringen har på olika sätt verkat för att öka myndigheternas användning av digital post, och då i synnerhet infrastrukturen Mina meddelanden.[8] Ett tydligt exempel är det uppdrag som Digg har haft sedan myndigheten inrättades om att

[6] Se PTS:s rapport Svensk postmarknad 2022, rapportnummer PTS-ER-2022:16, diarienummer21-12344, s. 26. Svensk postmarknad 2022 (pts.se)

[7] Internetstiftelsens rapport Svenskarna och internet 2022, https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2022/anvandning-av-internet-och-e-tjanster/#digital-brevlada

[8] För en exemplifierande genomgång av initiativ fram till och med år 2017, se delbetänkandet av Utredningen om effektiv styrning av nationella digitala tjänster, digitalforvaltning.nu (SOU 2017:23), s. 155 f.

främja användningen av infrastrukturen för säkra elektroniska försändelser och därmed öka myndigheters användning av digital post.[9]

3.1.2 En stor mängd information hanteras och lagras i digitala brevlådor

En ökad användning av digital post innebär att mer information hanteras och lagras i de digitala brevlådorna. I sammanhanget bör det understrykas att det inte bara är myndigheter som skickar digital post, utan även privata aktörer (såsom privata vårdgivare, friskolor, dagligvaruhandel, apotek, kreditupplysningsföretag, försäkringsbolag och banker) skickar digital post till digitala brevlådor.[10]

De digitala brevlådorna används i många fall som lagringsyta åt brevlådeinnehavarna. Vad gäller Min myndighetspost kan konstateras att mängden data ökar utan att antalet användare av den digitala brevlådan ökar (snarare minskar något). Det talar för att många brevlådeinnehavare använder den digitala brevlådan som en lagringsyta för de meddelanden som skickats till den enskilde. För att sätta det i ett sammanhang kan sägas att Min myndighetspost är en av Skatteverkets största databaser.

Digg har ingen insyn i innehållet i den digitala posten som hanteras i de digitala brevlådorna.[11] Eftersom digitala brevlådor anses vara säkrare än e-post och då avsikten med Mina meddelanden är att ersätta myndigheters behov av att skicka brev med posten, kan det antas att en del av den digitala post som hanteras bör betraktas som skyddsvärd ur olika perspektiv. Digg utgår ifrån att det i de digitala brevlådorna lagras en stor mängd information, både om enskilda och om det offentliga.

3.1.3 Särskilt regelverk för digitala brevlådor saknas

För den myndighetspost som skickas inom infrastrukturen för säkra elektroniska försändelser finns ett regelverk. Regelverket består, utöver förordningen om myndighetsgemensam infrastruktur för säkra elektroniska försändelser, av en civilrättslig avtalskonstruktion. Genom avtal ställs bland annat krav på säkerheten

---

[9] 4 § förordning med instruktion för Myndigheten för digital förvaltning.

[10] Brevlådeoperatören Kivra har ett stort antal privata avsändare, se https://kivra.se/sv/privat/sa-funkar-det/alla-som-skickar.

[11] Digg har ingen insyn i den digitala post som förmedlas inom infrastrukturen eller som hanteras/lagras i Min myndighetspost. Det är de avsändande myndigheterna som avgör vilken information de skickar till den digitala brevlådan. Vad gäller den digitala post som förmedlas utanför infrastrukturen har Digg ingen roll.

för den digitala posten inom infrastrukturen. Digg har också rätt att kontrollera att anslutna parter lever upp till de ställda säkerhetskraven och genom avtal har Digg också rätt att stänga av eller säga upp avtalet med de parter som inte följer regelverket.

Vad gäller den digitala post som skickas till digitala brevlådor utanför infrastrukturen kan konstateras att det inte finns något särskilt regelverk. Det är i stället upp till tillhandahållaren av den digitala brevlådan att, genom avtal, reglera förutsättningarna för villkoren och tillhandahållandet av tjänsten. Någon särskild tillsyn eller kontroll utövas inte heller över dessa tjänster.

3.1.4 Styrning av användning av Mina meddelanden

Anslutningen till Mina meddelanden är idag frivillig för samtliga aktörer. Avsändande myndigheter som vill skicka digital post kan välja att ansluta sig till infrastrukturen och skicka digital post därigenom eller så kan de välja att anskaffa en digital post-tjänst på annat sätt.

Digg ser att det finns flera fördelar för myndigheter att välja att ansluta sig till Mina meddelanden framför att anskaffa en digital post-tjänst på annat sätt. Utöver fördelarna med ett centralt mottagarregister ställer Digg också omfattande krav på brevlådeoperatörerna och deras tjänster. Digg säkerställer att dessa krav efterlevs vilket gör att säkerheten upprätthålls.

Digg anser att det är en ineffektiv hantering av samhällets gemensamma resurser att varje myndighet ska anskaffa digital post-tjänster på egen hand. Det riskerar också att minska nyttan med den förvaltningsgemensamma infrastrukturen. I en situation där respektive myndighet anskaffar en egen digital post-tjänst är det inte heller möjligt för enskilda att i samma utsträckning som idag själv välja i vilken digitala brevlåda hen vill ta emot sin myndighetspost i, eftersom hen då måste använda sig av den digitala brevlåda som avsändande myndighet anskaffat för ändamålet.

3.2 Möter infrastrukturen för säkra elektroniska försändelser samhällets behov?

3.2.1 Ändamålsenlighet

Digitaliseringen av den offentliga förvaltningen ska bidra till en enklare vardag för medborgare, en öppnare förvaltning som stöder innovation och delaktighet samt högre kvalitet och effektivitet i den offentliga förvaltningen.

Den infrastruktur som finns idag skapades för att i fredstid tillgodose myndigheters behov av att, på ett säkert sätt, kunna skicka elektroniska försändelser till enskilda. Utifrån det perspektivet anser Digg att befintlig infrastruktur är ändamålsenlig.

Men ändamålsenlighet handlar också om förmågan att kunna möta nya behov och vidareutveckla infrastrukturen. Behov kan komma från avsändare, mottagare, brevlådeoperatörer eller andra offentliga aktörer men även från förändrad omvärldssituation eller en förändrad lagstiftning. Exempel på behov som ofta lyfts fram i Diggs dialoger med avsändare är möjlighet till dubbelriktad kommunikation, betalbara försändelser och större försändelser än den gräns som är beslutad i dagens infrastruktur. När det gäller förmågan att möta dessa och andra behov finns begränsningar i dagens infrastruktur vilket redogörs för nedan.

3.2.2 Det är svårt att vidareutveckla Mina Meddelanden

Utmaningarna och begränsningarna i att tillmötesgå behov och vidareutveckla dagens infrastruktur är dels kopplade till den tekniska infrastrukturen, och dels till samverkan med och beroendet till andra aktörer i infrastrukturen. Detta gör att infrastrukturen är trögrörlig och har svårt att möta nya behov. Det finns också utmaningar som hör samman med nuvarande lagstiftning och regelverk inom olika rättsområden, vilket redogörs för i kapitel 4.

3.2.2.1 Utveckling av funktionalitet i brevlådorna

I dagens lösning kan brevlådeoperatörer erbjuda olika funktionalitet och tilläggstjänster till sina användare. Det innebär att funktionalitet hanteras olika av brevlådeoperatörerna. Exempelvis kan en brevlåda erbjuda funktionalitet för att betala fakturor medan det inte är möjligt i en annan brevlåda. Avsändarna uttrycker önskemål och krav på funktionalitet till Digg då de vill ha konsekvent hantering i brevlådorna oberoende av brevlådeoperatör.

Det finns möjlighet för Digg att ställa nya krav på brevlådeoperatörer för att på så sätt reglera utveckling av ny funktionalitet genom att införa nya krav i allmänna villkor. Varje nytt krav medför dock en ny granskning av brevlådeoperatörerna för att säkerställa att de lever upp till kraven. I det fall en befintlig brevlådeoperatör inte lever upp till kraven har Digg rätt att stänga av eller säga upp anslutningsavtalet med brevlådeoperatören. Nya krav medför dock en risk att brevlådeoperatörer lämnar infrastrukturen om kraven blir för höga och kostnadsdrivande.

3.2.2.2 Utveckling av funktionalitet i Min myndighetspost

Digg agerar på en konkurrensutsatt marknad när Digg tillhandahåller Min myndighetspost. För att inte riskera att konkurrera på ett otillbörligt sätt har Digg aktivt valt att inte tillhandahålla en tjänst som ligger i framkant vad gäller utveckling av funktionalitet som efterfrågas och inte heller på annat sätt riskera att konkurrera med andra brevlådeoperatörer. Det har fått till konsekvens att Min Myndighetspost är en digital brevlåda med begränsad förmåga att uppfylla användarnas behov vilket kan bekräftas av att den också tappat användare de senaste åren.

3.2.2.3 Utveckling påverkar anslutna myndigheter

Eftersom Mina meddelanden används och är uppbyggd av flera aktörer i samverkan innebär utveckling i infrastrukturen ofta att aktörerna måste uppgradera, göra anpassningar eller ändringar i sina system för att fortsatt kunna nyttja infrastrukturen. Detta behöver ske inom en begränsad tidsperiod, särskilt om åtgärder är säkerhetsrelaterade.

Om en ny version av infrastrukturen kräver ändringar i aktörernas system måste den gamla och den nya versionen fungerar parallellt under en period. En sådan lösning gör att aktörerna kan genomföra sina anpassningar oberoende av varandra. Att ha parallella versioner ger dock ökade underhålls- och supportkostnader för Infrastrukturansvarig vilket gör att antalet versioner bör hållas nere samt att längden på övergångsperioden bör hållas så kort som möjligt.

Anslutna avsändare varierar i storlek, alltifrån stora myndigheter som Skatteverket och Försäkringskassan med egna stora IT-avdelningar, till små kommuner som inte har egen IT-avdelning och som dessutom har knappa resurser. Anpassningar till nya versioner av infrastrukturen prioriteras mot andra insatser, vilket kan innebära att anpassningen till nya versioner av infrastrukturen prioriteras ner eller till och med bort.

3.3 Tekniska brister och utmaningar

3.3.1 Tekniska brister i Mina Meddelanden

Dagens infrastruktur är byggd på gammal teknik. Konsekvensen av detta är att det finns en teknisk skuld som kräver åtgärd. Med anledning av detta pågår sedan 2021 ett tekniskt lyft av Mina meddelanden, med planerad driftsättning under första kvartalet år 2023. Det tekniska lyftet har fokus på att byta befintlig föråldrad

teknik till en mer modern teknik. Arbetet med tekniklyftet är nödvändigt och har begränsat möjligheterna till annan utveckling under lång tid.

3.3.1.1 Separering av miljöer för Mina meddelanden och Min myndighetspost

Dagens lösning för informationsseparering behöver uppdateras då omvärldsutveckling och teknik medfört ökade krav på denna förmåga. Detta har även påtalats av Riksrevisionen.

3.3.2 Tekniska brister i brevlådan Min myndighetspost

Min Myndighetspost har, tillsammans med övriga anslutna digitala brevlådor, utpekats som en betrodd tjänst av Post- och Telestyrelsen (PTS). Detta ställer höga krav på säkerhet och robusthet, vilket i sin tur ställer höga krav på drift- och förvaltningsorganisationen.

3.3.2.1 Begränsningar i dagens datalagring

Även om antalet mottagare som använder Min myndighetspost inte ökar så ökar mängden meddelanden för befintliga mottagare eftersom ingen gallring sker av äldre meddelanden. Dagens databasarkitektur kommer på sikt inte kunna hantera den ökade belastningen. Tjänsten skulle då inte leva upp till de krav på robusthet som finns. Att ha kvar dagens databasarkitektur kommer med dagens tillväxttakt även att innebära väsentligt ökade kostnader för lagring och förvaltning av databasen.

För att Min myndighetspost ska ha möjlighet att dels möta nuvarande tillväxt men också kunna ta emot större volymer i framtiden krävs en helt ny arkitektur för datalagring.

3.3.2.2 Kryptering av lagrade data

Det är ett krav i Allmänna villkor att innehållet i brevlådan ska lagras krypterat. Sedan dagens lösning implementerades i Min myndighetspost har tekniken gått framåt. Idag finns andra bättre lösningar för kryptering. En ny lösning för kryptering av lagrade data behöver därför tas fram och implementeras.

3.3.2.3 Teknisk skuld i Min myndighetspost

Försäkringskassan, Skatteverket och Digg genomförde under våren 2019 en gemensam genomlysning av Min myndighetspost. Analysen visade att Min myndighetspost bygger på föråldrad teknik samt att det finns en stor teknisk skuld som behöver omhändertas.

Dagens omfattande programkod i Min myndighetspost har av flera skäl blivit ostrukturerad vilket medfört svårigheter med livscykelhanteringen. Problemet har därför ökat över tid. Idag är det en stor utmaning för utvecklare att sätta sig in i koden, det är svårt att införa ny funktionalitet, och eftersom att det är svårt att få överblick uppstår oförutsedda och oönskade konsekvenser även vid små förändringar. Det är svårt att hitta kompetens som klarar av att hantera de äldre ramverk som används i Min myndighetspost. Den tekniska skuld som idag finns i Min myndighetspost skapar en dyrare förvaltning, en lägre kvalitet och en högre risk för dataintrång och andra säkerhetsrisker.

Digg och Skatteverket bedömer att Min Myndighetpost är i ett sådant läge att en nyutveckling är nödvändig för att säkerställa effektiv, säker drift och förvaltning. Om detta inte sker uppstår både risker och kostnader.

3.4 Privata brevlådeoperatörers roll i Mina meddelanden

3.4.1 Om en brevlådeoperatör lämnar infrastrukturen

Infrastrukturen bygger på att det finns väl fungerande marknad med flera anslutna brevlådeoperatörer för att möjliggöra valfrihet för enskilda. Nya brevlådeoperatörer kan tillkomma och befintliga kan lämna.

I det fall en brevlådeoperatör lämnar infrastrukturen kan det leda till stor påverkan på robustheten i infrastrukturen. En brevlådeoperatör kan lämna av olika anledningar. Som exempel kan nämnas att:

- En brevlådeoperatör väljer att på eget initiativ lämna infrastrukturen.
- Digg säger upp anslutningsavtal med brevlådeoperatör på grund av att denne inte lever upp till villkoren.
- En brevlådeoperatör går i konkurs.

Konsekvenserna för avsändande myndigheter och enskilda om en brevlådeoperatör med få användare lämnar är begränsade. Det medför dock att antalet brevlådeoperatörer att välja mellan blir färre.

Om en brevlådeoperatör med många användare lämnar infrastrukturen skulle det innebära stora konsekvenser för avsändande myndigheter och enskilda. För enskilda som vill fortsätta att få sin myndighetspost digitalt innebär det att de måste byta brevlådeoperatör. Om enskilda då inte väljer en ny brevlåda för sin myndighetspost kommer posten i stället att skickas analogt vilket innebär ökade portokostnader för avsändare, längre tid för posten att komma fram samt

miljökonsekvenser i form av ökat behov av papper och transporter. Det kan också finnas en risk att det saknas utskriftskapacitet hos utskriftsleverantörer och/eller utdelningskapacitet hos posten för de ökade mängderna.

Om en brevlådeoperatör lämnar infrastrukturen kan en enskild inte ta med sig sin tidigare mottagna post till en annan brevlådeoperatör. Lagringen av post sker hos brevlådeoperatörerna och det finns idag inga krav som reglerar möjligheten att flytta meddelandena till annan brevlåda eller att meddelanden ska vara tillgängliga hos en brevlåda som lämnar infrastrukturen. Däremot finns krav på att enskilda ska kunna föra ut meddelanden ur brevlådan när brevlådeoperatören upphör med sin verksamhet kopplad till infrastrukturen.

3.4.2 Ersättning till brevlådeoperatörer

Idag erhåller brevlådeoperatörerna inte någon ersättning för att de tillhandahåller sin tjänst åt anslutna parter i infrastrukturen trots att det torde vara förenat med kostnader för brevlådeoperatören att tillhandahålla en digital brevlåda. Det kan till exempel handla om kostnader till följd av kravet på identifiering med e-legitimation som följer av allmänna villkor.

Den största brevlådeoperatören, Kivra, har tidigare påtalat att de inte anser sig kunna fortsätta erbjuda tjänster inom infrastrukturen utan att få ersättning.

För att erbjuda en fungerande marknad och fortsatt möjliggöra för enskilda att själv kunna välja brevlåda är det av yttersta vikt att det finns flera digitala brevlådor anslutna till infrastrukturen som lever upp till de säkerhetskrav som är nödvändiga för att upprätthålla en robust och säker infrastruktur. Om Digg ställer krav som innebär att en brevlådeoperatör behöver vidareutveckla sin tjänst på ett sätt som är förenat med kostnader för brevlådeoperatören finns det risk för att brevlådeoperatören väljer att lämna infrastrukturen. Ett incitament för brevlådeoperatörer att stanna kvar i infrastrukturen och genomföra utveckling kan vara att införa ersättning till brevlådeoperatörerna. Införandet av ersättning kan också vara ett incitament för nya brevlådeoperatörer att ansluta till infrastrukturen.

Frågan om ersättning till brevlådeoperatörer har aktualiserats vid olika tillfällen över tid, senast i Regeringskansliets promemoria *Auktorisationssystem för*

elektronisk identifiering och digital post.[12] Avsikten var att införa auktorisationssystem till sommaren 2022, varigenom en möjlighet till ersättning för brevlådeoperatörer skulle ha kunnat införas, men lagförslaget har ännu inte genomförts.

Även om lagförslaget inte tagits vidare anser Digg att frågan om huruvida brevlådeoperatörerna ska erhålla ersättning för att erbjuda sina användare att ta emot myndighetspost genom infrastrukturen är en aktuell fråga som behöver hanteras. Frågan om huruvida ersättning ska utgå till brevlådeoperatörerna och hur en ersättning i sådana fall ska utformas kräver en noggrann analys.

Hur en eventuell ersättning ska finansieras behöver också utredas i anslutning till att en eventuell ersättning utreds. Digg anser att en eventuell ersättning inte behöver ha en direkt koppling till en avgift som en avsändande myndighet ska erlägga då en ersättning och en avgift fyller olika syften.

Detta bör tas i beaktande, liksom att en avgiftshantering på myndighetsnivå innebär en betydligt ökad administration både hos varje enskild myndighet och hos den myndighet som ska hantera detta vilket leder till ökade kostnader, i samband med att en eventuell finansieringen av ersättning genom avgift utreds.

4 Behov av regelutveckling

4.1 Digital post saknar idag nödvändig reglering

Det kan konstateras att digital post idag till stor del är ett oreglerat område. Detta till skillnad från den mer traditionella fysiska posthanteringen, som den digitala posten i viss utsträckning kommit att ersätta. Även elektroniska meddelanden som skickas i en elektronisk kommunikationstjänst är reglerade till viss del.

Huruvida det finns behov av att reglera digital post som företeelse i stort eller inte får lämnas osagt. Däremot ser Digg att det finns behov av att reglera den digitala post som skickas från myndigheter till enskilda genom infrastrukturen Mina meddelanden på annat sätt än vad som görs idag.

[12] Promemoria Auktorisationssystem för elektronisk identifiering och för digital post I2020/03269.

I det följande lämnas en översiktlig redogörelse av behov av regelutveckling som Digg identifierat som har ett direkt samband med infrastrukturen. Redogörelsen ska inte ses som uttömmande, och Digg vill understryka att konsekvenserna av att införa nedan angivna regler för att stärka infrastrukturen inte är utredda. Digg anser att det är nödvändigt att vidare utreda regleringsbehovet, särskilt om dagens infrastruktur ska utvecklas på det sätt som Digg föreslår.

I sammanhanget bör tydliggöras att Digg inte anser att det bemyndigande som återfinns i 5 § förordningen om myndighetsgemensam infrastruktur för säkra elektroniska försändelser ger Digg möjlighet att införa de regler som Digg anser krävs för att stärka skyddet för infrastrukturen.

4.2 Reglering som ger bättre förutsättningar för en säker infrastruktur

Digg har till uppgift att tillhandahålla en myndighetsgemensam infrastruktur för säkra elektroniska försändelser. I förordningen som reglerar infrastrukturen Mina meddelanden kan konstateras att det inte närmare redogörs för vad som avses med ”säkra elektroniska försändelser”. I avsaknad av definition får det antas att försändelser som skickas inom infrastrukturen Mina meddelanden i enlighet med de allmänna villkor som Digg uppställt och som tillgängliggörs i de till infrastrukturen anslutna digitala brevlådorna utgör säkra elektroniska försändelser i lagstiftarens mening.

I allmänna villkor med tillhörande bilagor uppställs krav på bland annat säkerhet som anslutna brevlådeoperatörer ska leva upp till. Det finns också en beskrivning av vilka olika skyddsnivåer som ett meddelande kan skickas med. Digg kan konstatera att de krav som uppställs i allmänna villkor medför en viss säkerhet kring försändelserna och enskildas integritet. Digg anser emellertid inte att den säkerhet som allmänna villkor medför är tillräcklig, utan att det behövs ytterligare reglering för att försändelserna ska vara ”säkra”.

4.2.1 Fysisk posthantering och elektronisk kommunikation har ett mer omfattande skydd

Skyddet för enskilda och skickade brev vid traditionell fysisk posthantering tillgodoses genom regler i bland annat postlagen (2010:1045). Där föreskrivs att postverksamhet ska bedrivas så att den tillgodoser rimliga krav på tillförlitlighet och så att skyddet för avsändarnas och mottagarnas personliga integritet upprätthålls (2 kap. 6 § postlagen). Genom lagen (2022:482) om elektronisk

kommunikation (härefter LEK) ska enskilda och myndigheter få tillgång till säkra och effektiva elektroniska kommunikationer (1 kap. 1 § LEK). De försändelser som skickas genom infrastrukturen omfattas inte av något av dessa regelverk. Inte heller i övrigt finns något regelverk motsvarande de nyss nämnda som på motsvarande sätt skyddar de försändelser som skickas genom infrastrukturen.

4.2.2 Regler om sekretess och tystnadsplikt saknas

För både den fysiska posthanteringen och för elektroniska kommunikationstjänster finns regler om sekretess och tystnadsplikt, med tillhörande sekretess- och tystnadspliktsbrytande bestämmelser.[13] Reglerna om sekretess och tystnadsplikt tar sikte på såväl den post som skickas i den fysiska posthanteringen som de elektroniska meddelanden som skickas genom elektroniska kommunikationstjänster.

Motsvarande regelverk finns inte idag för de försändelser som skickas genom infrastrukturen. Dock finns det idag regler om sekretess som gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden som kan tillämpas.[14] Den regleringen kan emellertid bara användas på uppgifter som förekommer i det allmännas verksamhet. I de fall försändelserna hanteras av privata brevlådeoperatörer saknas motsvarande skydd för försändelserna. Vidare kan det diskuteras om det är tillräckligt att enbart uppgifter om enskilds personliga eller ekonomiska förhållanden skyddas av sekretess när det är frågan om den här typen av verksamhet.

Det kan konstateras att det i den nuvarande infrastrukturen, till följd av avsaknaden av författningsreglering, är svårt att säkerställa korrekt tillämpning av tryckfrihetsförordningens bestämmelser om allmänna handlingar och offentlighets- och sekretesslagens (2009:400) bestämmelser om förbud mot röjande av sekretesskyddade uppgifter. En reglering i detta avseende kan tydliggöra ramverket för hur uppgifter som skyddas av sekretess (och tystnadsplikt) ska hanteras inom infrastrukturen samt vilka utvecklingsmöjligheter

[13] Se bland annat 2 kap. 14 § postlagen, 9 kap. 31 § LEK, 29 kap. 1 och 2 §§ OSL, samt 44 kap. 4 § OSL.
[14] Se 40 kap. 5 § OSL.

som medges till förmån för innovation. Därutöver kan noteras att vissa risker i kapitel 5 torde åtgärdas genom författningsreglering.

4.2.3 Regler om tillsyn och sanktionsmöjligheter behövs

Idag regleras det i allmänna villkor att Digg, i egenskap av Infrastrukturansvarig, har rätt att utföra kontroll av anslutna parter för att kontrollera om uppställda krav och åtaganden efterlevs.[15] Vid kontroller som Digg genomfört har Digg haft svårt att få de uppgifter som krävs och också få tillträde till utrymmen för att utföra nödvändig kontroll, trots att allmänna villkor stipulerar detta. För postverksamhet och elektroniska kommunikationstjänster finns regler som bland annat ger tillsynsmyndigheten rätt att få de uppgifter som behövs och också rätt till tillträde till lokaler, områden och andra utrymmen där verksamhet bedrivs. Med ett sådant regelverk skulle förutsättningarna för att utföra tillsyn av anslutna aktörer förbättras.

Om Digg vid en kontroll idag identifierar brister har Digg enligt allmänna villkor möjlighet att stänga av aktören eller säga upp anslutningsavtalet. Digg anser att dessa åtgärder är trubbiga och riskerar att få icke önskvärda konsekvenser när det är fråga om mindre brister eller avvikelser från gällande regelverk (exempelvis när det handlar om att en brevlådeoperatör skulle behöva vidta vissa förbättringsåtgärder – då säkerheten inte direkt äventyras på kort sikt). Digg har svårt att se att det är rimligt att i dagsläget införa andra sanktionsmöjligheter i allmänna villkor bland annat eftersom aktörerna idag tillhandahåller sina tjänster utan ersättning.

Vad gäller tillsyn av postverksamhet och elektroniska kommunikationstjänster kan tillsynsmyndigheten utfärda förelägganden och också förena sådana med vite, något som Digg ser skulle kunna vara ett användbart verktyg för en tillsynsmyndighet vid en granskning av kravuppfyllnad. Vidare kan konstateras att det också finns sekretessbrytande bestämmelser som gör det möjligt för myndigheter som granskas att lämna uppgifter vidare till den som utövar tillsyn, något som idag saknas vilket gör det nästintill omöjligt att utöva kontroll över myndigheter som har att följa offentlighets- och sekretesslagstiftningen, när uppgifter som skulle behöva lämnas ut skyddas av sekretess.

[15] Se avsnitt 13 i Allmänna villkor.

I sammanhanget bör även problematiken som finns kopplad till den kontroll som Digg idag i egenskap av Infrastrukturansvarig genomför av anslutna parter för att säkerställa att de uppfyller krav och åtaganden i allmänna villkor samtidigt som Digg tillhandahåller den digitala brevlådan Min myndighetspost nämnas.

Att utöva tillsyn över den egna verksamheten utan att exempelvis förtroendet för myndigheten som ansvarig för tillsynen rubbas eller att andra utövare kan uppfatta sig bli orättvist behandlade, är utmanande. En granskning torde alltid vinna på att den utförs av någon ”utomstående”. Digg förordar därför att uppgiften att bedriva tillsyn behöver utformas på ett sådant sätt som hanterar ovanstående utmaningar.

4.2.4 Särskilda regler kan behövas vid krig, krigsfara och för att tillgodose totalförsvarets behov

För den fysiska posthanteringen och för de elektroniska kommunikationstjänsterna finns det särskilda regler i händelse av krig och krigsfara. Det finns också regler om fredstida planering för totalförsvarets behov. Om infrastrukturen avses kunna användas i händelse av krig eller vid krigsfara anser Digg att det är nödvändigt att införa reglering som möjliggör att infrastrukturen kan upprätthållas i sådana situationer.

4.3 Reglering av personuppgiftsansvaret inom infrastrukturen

Idag anges i förordning om myndighetsgemensam infrastruktur för säkra elektroniska försändelser att Digg är personuppgiftsansvarig för Förmedlingsadressregistret (FaR). I övrigt regleras personuppgiftsansvaret inom infrastrukturen, liksom för alla annan verksamhet, ytterst av Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (härefter dataskyddsförordningen). I allmänna villkor beskrivs en fördelning av personuppgiftsansvaret inom infrastrukturen.

Idag finns en risk att ingående parter i infrastrukturen gör olika tolkningar av sitt personuppgiftsansvar utifrån dataskyddsförordningen jämfört med hur personuppgiftsansvaret beskrivs i allmänna villkor. Den reglering som finns i allmänna villkor av personuppgiftsansvaret kan därför komma att utgöra ett hinder för parter att ansluta till infrastrukturen. Då personuppgiftsansvarfrågan som regleras i allmänna villkor ännu inte är prövad rättsligt kan rättsläget vad gäller personuppgiftsansvaret inom infrastrukturen anses vara oklart.

Genom att personuppgiftsansvaret inom infrastrukturen regleras i författning undanröjs eventuella tvivel och skilda tolkningar kring personuppgiftsansvarsfrågan. En författningsreglering skulle även stärka tydligheten för enskilda om vilken part som är ansvarig för hanteringen av personuppgifterna. En sådan reglering skulle också underlätta för parterna inom infrastrukturen att ta sitt ansvar för hanteringen av personuppgifter. Genom en tydlig reglering som fördelar personuppgiftsansvaret till respektive part stärks säkerheten kring hanteringen av personuppgifterna. I samband med att en författningsreglering beträffande personuppgiftsansvaret införs kan nämnas att en konsekvensbedömning för infrastrukturen som sådan med fördel kan genomföras dels för att kartlägga integritetsrisker för individerna, dels för att underlätta bedömningarna för nya aktörer som avser ansluta till infrastrukturen. Beroende på omfattning kan vidare uppmärksammas att en författningsreglering av infrastrukturen kan medföra att den rättsliga grunden i dataskyddsförordningen tydliggörs och underlättar för samtliga parter i infrastrukturen.

Digg kan även här konstatera att *Utredningen om effektiv styrning av nationella digitala tjänster* i såväl delbetänkande (digitalforvaltning.nu, SOU 2017:23) som slutbetänkande (reboot – omstart för den digitala förvaltningen, SOU 2017:114) föreslagit att personuppgiftsansvaret inom infrastrukturen ska regleras i författning.

Ett författningsreglerat personuppgiftsansvar får även i detta avseende anses vara ett steg i utvecklingen av den nuvarande infrastrukturen med en decentraliserad meddelandehantering till en central meddelandehantering. Om en författningsreglering av personuppgiftsansvaret införs behöver den förändras i samband med att dagens infrastruktur utvecklas.

4.4 Digg bör ges i uppgift att tillhandahålla Min myndighetspost

En uttrycklig uppgift i Diggs instruktion om att tillhandahålla Min myndighetspost skulle stärka Diggs möjligheter och legala förutsättningar att erbjuda tjänsten Min myndighetspost åt enskilda. Digg skulle också kunna agera på ett annat sätt vad gäller utveckling av exempelvis funktionalitet i brevlådan.

Vidare undanröjs eventuella tvivel om att det inte skulle rymmas i Diggs uppdrag att tillhandahålla en digital brevlåda. Idag har Digg till uppgift att tillhandahålla en infrastruktur för säkra elektroniska försändelser som brevlådeoperatörer kan

ansluta till. I uppgiften uttalas inte att Digg ska agera brevlådeoperatör och tillhandahålla en digital brevlåda som ska ansluta till infrastrukturen.

Genom en uttrycklig reglering tar också staten ansvar för att säkerställa tillgången till en digital brevlåda inom infrastrukturen dit enskilda kan få sin myndighetspost. Infrastrukturens robusthet får därmed anses öka, då infrastrukturen är beroende av att det finns digitala brevlådor som är anslutna till infrastrukturen. Eftersom det i dagsläget inte kan anses proportionerligt att ålägga privata brevlådeoperatörer en skyldighet att ansluta sina tjänster till infrastrukturen är det inte möjligt att på annat sätt säkerställa att myndigheter kan skicka digital post till enskilda.

Att tillhandahålla Min myndighetspost utan uttryckligt stöd i författning påverkar även Diggs stöd för att behandla personuppgifter i tjänsten. Idag är den rättsliga grunden för behandling av personuppgifter avtal. Om Digg i stället skulle ha i uppdrag att tillhandahålla Min myndighetspost skulle den rättsliga grunden kunna vara allmänt intresse.

Lämpligen regleras Diggs uppdrag om att tillhandahålla Min myndighetspost i Diggs instruktion alternativt i förordning om myndighetsgemensam infrastruktur för säkra elektroniska försändelser. Digg kan även konstatera att *Utredningen om effektiv styrning av nationella digitala tjänster* i såväl delbetänkande (digitalforvaltning.nu, SOU 2017:23) som slutbetänkande (reboot – omstart för den digitala förvaltningen, SOU 2017:114) föreslagit att en myndighet ges i uppdrag, alternativt ges möjlighet, att tillhandahålla en digital brevlåda.

Att Digg erhåller ett sådant uppdrag kan också ses som ett första steg på vägen mot transformationen av den nuvarande infrastrukturen till en central meddelandehantering med tillhörande visningsklienter, som beskrivs i kapitel 6, där den tillhandahållande myndigheten behöver ha ett uttryckligt stöd för att tillhandahålla en central meddelandehantering, och eventuellt också en tillhörande visningsklient.

4.5 Om ersättning införs krävs reglering

I avsnitt 3.4.2 redogör Digg för att införandet av en eventuell ersättning till brevlådeoperatörerna behöver hanteras. Vidare anser Digg att finansieringen av en sådan ersättning behöver utredas. I avsnitt 6.3 anges även att Digg anser att förutsättningarna för en ersättning till kommande visningsklienter behöver ses över. Om ersättning ska införas krävs en reglering som möjliggör utbetalning av

ersättning till brevlådeoperatörer och visningsklienter. Beroende på hur ersättningen ska finansieras kan också eventuell reglering avseende finansieringen krävas.

4.6 Vilka ska kunna använda infrastrukturen?

4.6.1 Vem ska kunna agera avsändare?

Digg anser att det bör övervägas om det finns anledning att se över vilka som kan ansluta till infrastrukturen. Idag är det exempelvis enbart myndigheter som kan agera avsändare inom infrastrukturen, men det finns anledning att överväga om även andra aktörer skulle kunna agera avsändare.

En förändring av vem som kan agera avsändare inom infrastrukturen kan komma att få konsekvenser för vilka som kan vara mottagare av försändelser inom infrastrukturen. Ska vissa avsändare kunna vara både avsändare och mottagare (här avses framförallt aktörer av offentligfinansierad verksamhet, så kallade offentliga aktörer, som idag kan vara mottagare eftersom de faller in under begreppet ”enskild”)?

Förslag på att fler ska kunna agera avsändare inom infrastrukturen har tidigare lämnats.[16] Det bör dock uppmärksammas att Försvarsmakten uttryckt att en vidgad krets av avsändare kan innebära nya hot som infrastrukturen behöver hantera.[17]

4.6.2 Vilka enskilda ska kunna ansluta som mottagare?

Idag finns krav inom infrastrukturen på att den som skaffar en digital brevlåda behöver ha en e-legitimation. Någon lägsta åldersgräns för att skaffa en digital brevlåda finns inte. För att tydliggöra vilka möjligheter minderåriga har att ansluta till infrastrukturen för att ta kunna emot digital post från det offentliga anser Digg att det bör övervägas om det ska införas regler om vid vilken ålder enskilda tidigast ska kunna ansluta till infrastrukturen.

[16] Se bland annat digitalforvaltning.nu, SOU 2017:23, reboot – omstart för den digitala förvaltningen, SOU 2017:114 och Regeringskansliets promemoria *Auktorisationssystem för elektronisk identifiering och för digital post,* publicerad 21 december 2020.

[17] Se Försvarsmaktens yttrande över slutbetänkande Reboot – en omstart för den digitala förvaltningen (SOU 2017:114), Försvarsmaktens beteckning FM2018-7168:2.

4.6.3 Ombudshantering bör regleras

Idag kan brevlådeinnehavare dela ut behörighet åt fysiska personer att ta del av innehållet i brevlådan. Dessa fysiska personer agerar då ombud åt brevlådeinnehavaren. Digg bedömer att det är ett behov som sannolikt kommer att kvarstå, och om en central meddelandehantering införs kommer frågan bli allt mer aktuell. För att säkerställa att det är möjligt att även framgent dela ut behörighet åt annan för att denne ska kunna ta del av innehållet i brevlådan bör det övervägas om sådan reglering behöver införas.

Det kan finnas situationer då en brevlådeinnehavare inte har förmåga att dela ut behörighet åt annan, exempelvis i händelse av plötslig allvarlig sjukdom eller vid dödsfall. Det kan då finnas försändelser i brevlådan som är nödvändiga för andra att ta del av. Det bör övervägas om det ska regleras vilka möjligheter det finns att tilldela andra behörigheter i sådana situationer. Vid en sådan utredning bör även regler om sekretess och möjlighet att efterge sekretess beaktas.

4.7 Reglering av när en försändelse ska anses ha kommit mottagaren tillhanda

För att undvika otydligheter kring när en försändelse ska anses ha kommit en mottagare tillhanda bör det övervägas om det är möjligt att införa reglering om när en försändelse ska anses ha kommit en mottagare till handa.

5 Risk- och säkerhetsanalys

5.1 Övergripande om risk- och säkerhetsanalys

I detta kapitel beskrivs riskerna som har identifierats i infrastrukturen Mina meddelanden under ett normalläge och vid höjd beredskap och krig. Identifierande risker baseras till stor del på tidigare genomförda riskanalyser.[18] Identifierade risker utifrån höjd beredskap och krig är i denna rapport inte uttömmande. För en mer komplett riskanalys behöver Digg under kommande år genomföra en mer omfattande utredning av myndighetens betydelse inom totalförsvaret och således få svar på infrastrukturens bäring utifrån perspektivet höjd beredskap och krig.

[18] Digg genomför årligt riskhanteringsarbete. Digg har under 2021-2022 genomfört revisioner och säkerhetsgranskrningar av brevlådeoperatörer, vilket har visat på brister.

I händelse av att infrastrukturen skulle anses utgöra en del av totalförsvaret ska infrastrukturen kunna hantera en störning under minst tre månader vid en säkerhetspolitisk kris i Europa och Sveriges närområden. Under dessa månader är utgångspunkten att logistiskflödena med omvärlden har begränsningar men inte är helt avbrutna.[19] Digg kan beroende på totalförsvarsanalysens utfall erhålla ett bredare ansvar än att endast se över sina egna komponenter. Det som är av betydelse är att skyddsvärd infrastruktur ska fungera utifrån det faktum att de mest kvalificerade hotaktörerna alltid kommer att agera mot de svagaste länkarna i våra sammankopplade system och därför behöver hela hotskalan inom IT-säkerhetsområdena tas i beaktande.[20]

I syfte att skydda informationen effektivt och ändamålsenligt kan säkerhetsskyddslagen (2018:585) samt lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster anses tillämplig för vissa delar. Om infrastrukturen bedöms omfattas av dessa regelverk aktualiseras krav gällande bland annat kontroll av information, säkerhetsklassificerade upphandlingar och robust incidenthantering, som går utöver de krav som idag ställs på infrastrukturen. Innan Digg genomfört totalförsvarsanalysen och därigenom konstaterat ifall och vilka delar av infrastrukturen som kan komma att omfattas av totalförsvaret, går det inte fastställa i vilka delar säkerhetsskyddslagen är tillämplig.[21]

Digg genomför årligen risk- och sårbarhetsanalyser i syfte att säkra för myndigheten relevanta delar. Därutöver har en säkerhetsskyddsanalys tidigare tagits fram som uppdateras med anledning av infrastrukturens utveckling. Säkerhetsskyddsanalysen tar sikte på att identifiera säkerhetskänslig verksamhet, säkerhetsskyddsklassificerade uppgifter och om verksamheten omfattas av för Sverige förbindande säkerhetsskyddsavtal.

Informationen i denna redogörelse är kopplad till vad risken är, vilken konsekvens risken har, var risken återfinns samt vem som drabbas om risken skulle realiseras. Riskerna är inte kopplade till kommersiella intressen eller andra intressen som inte berör informationen som sådan.

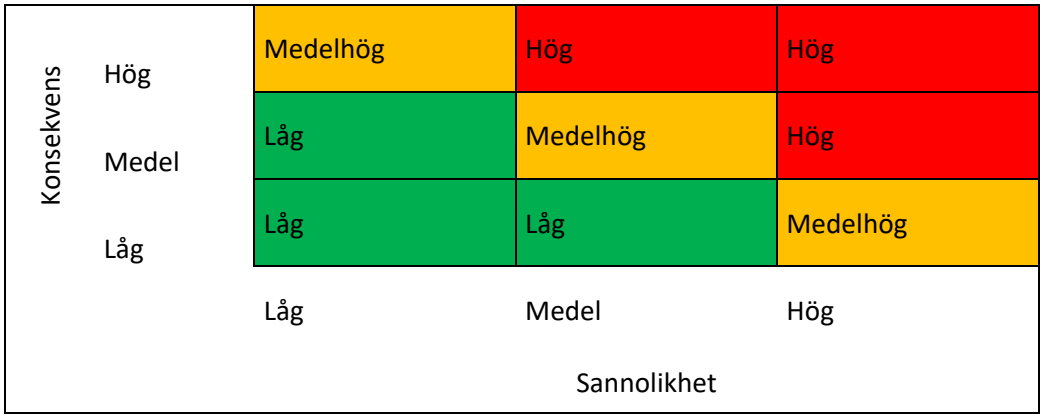
---

[19] Prop. 2020/21:30 Totalförsvaret 2021-2025, s. 84 f.

[20] Prop. 2020/21:30 Totalförsvaret 2021-2025, s. 63

[21] Som exempel kan det sannolikt konstateras att samtliga informationsflöden inte har betydelse vid höjd beredskap och krig. Däremot är det svårare att dels bedöma infrastrukturens betydelse i samhället i stort, dels bedöma särskilda informationsmängder från särskilda verksamheter såsom vissa statliga myndigheter eller hälso- och sjukvårdssektorn.

Konsekvensen av en risk är bedömd efter sannolikhet att risken inträffar och vilka konsekvenser det skulle få, i tre nivåer, låg, medelhög och hög, enligt tabellen nedan:



5.2 Normalläge

Vid normalläge är det främst hotaktörer som vill komma åt information eller göra den otillgänglig, främst från vad som kan beskrivas som hackare och kriminella organisationer i syfte att tjäna pengar. Det är begränsat med hot från nationalstatsaktörer, som troligen är mer inriktade på dold informationsinhämtning och förberedelser för höjd beredskap och krig, genom att exempelvis obemärkt ta sig in i systemen och exempelvis försöka exfiltrera eller förändra och/eller förstöra information. Exempel på angrepp i normalläge är att försöka ta sig in i enskild brevlåda eller göra tjänsten otillgänglig för slutanvändaren där hotaktören kräver pengar för att göra den tillgänglig igen.

I ett normalläge aktualiseras främst frågor om individens integritet utifrån dataskyddsförordningen och myndigheternas hantering av sekretesskyddade uppgifter utifrån offentlighets- och sekretesslagen. Utöver potentiella hot och risker mot individernas integritet och myndigheternas generella sekretesshantering kan det även föreligga risker kopplade till den allmänna förvaltningsrätten, såsom myndigheters skyldighet att bevara handlingar enligt tryckfrihetsförordningen och arkivlagen (1990:782) samt myndigheters skyldigheter att lämna ut allmänna handlingar enligt offentlighetsprincipen.

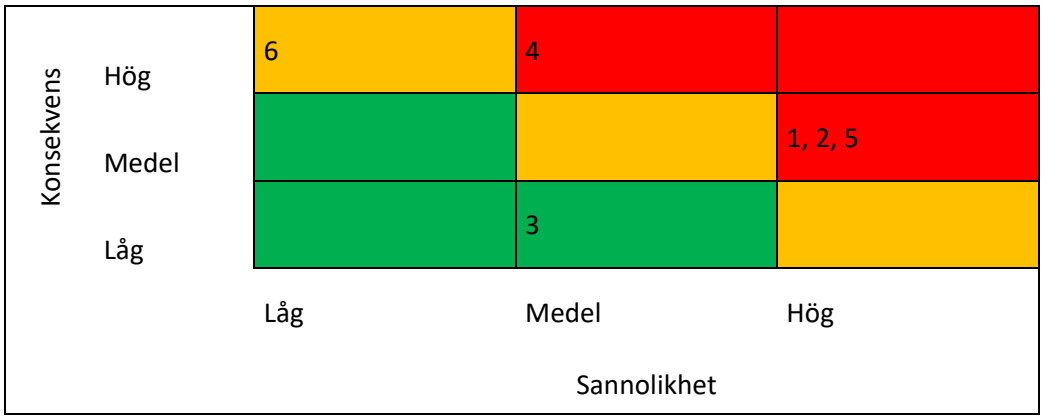
Riskanalysen har identifierat en övergripande risk och sex mer detaljerade risker i anslutning till infrastrukturen, vilka redogörs för i bilaga 1.

- Risk och säkerhetsanalys (RSA) 0
- RSA 1
- RSA 2

- RSA 3
- RSA 4
- RSA 5
- RSA 6

RSA 0 är en övergripande risk som har en bred påverkan på samtliga aktörer i infrastrukturen, där allvarlighetsgrad varierar mellan aktörer. Risken är därför svår att bedöma generellt. Av de sex detaljerade riskerna, bedöms fyra ha allvarlighetsgrad hög, en risk bedöms som medel och en bedöms som låg.

Matrisen nedan visar bedömda risker vid normalläge.



5.3 Höjd beredskap och krig

Vid höjd beredskap är risken att nationalstatsaktörer som är fientligt inställda mot Sverige kan komma att destabilisera Sverige och dess institutioner. Angrepp mot tillgänglighet och riktighet är troliga och även enklare att genomföra än att slå direkt mot konfidentialiteten. Exempel på angrepp kan vara att utge sig för att vara en avsändare i systemet eller att göra tjänsten otillgänglig för slutanvändaren.

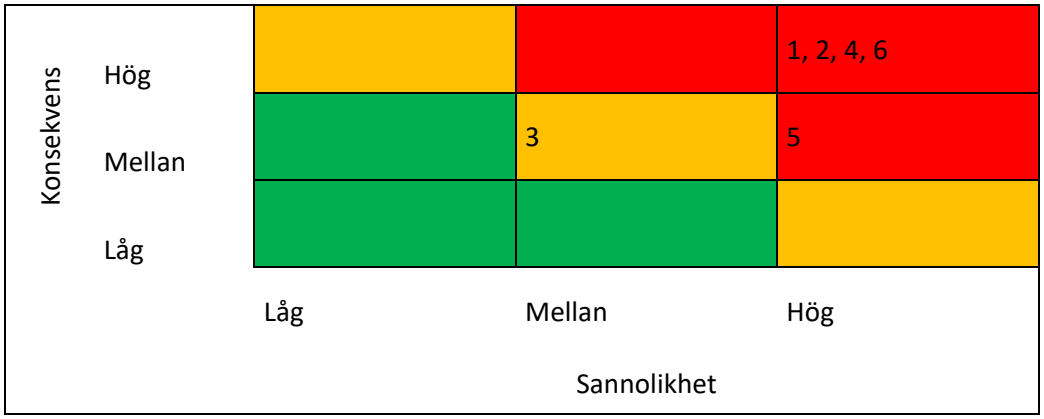
Vid krig är hotaktören främst nationalstatsaktörer som genomför direkta eller indirekta angrepp mot infrastrukturens alla delar. Angrepp begränsas inte av lagstiftning utan allt är tillåtet.[22] Om aktören inte kan manipulera eller komma åt informationen i läsbart skick är det troligt att försök görs att förstöra eller otillgängliggöra informationen.

[22] En angripare har ofta någon sorts ”interna” regler och lagar i angriparstaten för vad som är tillåtet ur ett eget riskperspektiv, exempelvis att de vill kunna förneka att de har gjort ett angrepp. Vid höjd beredskap och krig så behöver de inte låtsas och är mer fria och troligen även mer ”våldsamma” i sina angrepp, då de till exempel inte behöver kunna förneka ett angrepp.

Vid höjd beredskap eller krig ökar sannolikheten för att vissa risker inträffar vilket kan få konsekvenser för Sveriges säkerhet, samtidigt som andra risker i det läget inte är lika aktuella.

Riskerna RSA 1-6, som vid normalläge som redogjorts ovan i avsnitt 5.2 och bilaga 1, får en annan bedömning gällande sannolikhet och konsekvenser vid höjd beredskap eller krig. Då bedöms fem risker med allvarlighetsgrad hög och en risk som medelhög.

Matrisen nedan visar bedömda risker vid höjd beredskap och krig.



5.4 Slutsats

Det finns flera tekniska och organisatoriska risker som medför potentiell risk för angrepp av olika slag i syfte att förändra, förstöra, otillgängliggöra och övervaka information i infrastrukturen. I syfte att minimera identifierade säkerhetsbrister måste Digg se över och åtgärda helhetslösningen bland annat beträffande kontroll över meddelandehanteringen och regleringen av infrastrukturen. I händelse av att Diggs totalförsvarsanalys utmynnar i att hela eller delar av infrastrukturen är av betydelse vid höjd beredskap eller krig måste det genomföras en konsekvensanalys av vad det innebär för Mina meddelanden.

5.4.1 Normalläge

I normalläget är hoten och riskerna främst kopplad till integritet, sekretess och funktionalitet. Tidigare analyser som genomförts har visat på vissa säkerhetsrisker, dessa är främst utifrån ett normalläge. I normalläget är konsekvenserna av bristerna som identifierats inom Mina meddelanden och anslutna aktörer närmast sammankopplade med säkerhetsrisker som kan komma att påverka funktionaliteten hos en samhällsviktig infrastruktur, eller konsekvenser för den rättsliga tillämpningen som ytterst påverkar individens sekretesskyddade information eller personuppgifter.

5.4.1.1 Åtgärder för att mildra generella brister främst i normalläge

Förbättrade rutiner och processer för nuvarande lösning:

- Upprätta en användarvänlig handbok med syfte att förtydliga säkerhetskraven i infrastrukturen och förenkla implementeringen av säkerhetsarbetet.
- Säkerställa löpande uppföljning av överenskommen åtgärd över funna säkerhetsbrister över tid.
- Implementera en riskbaserad granskning, dvs. en aktör som inte sköter sig får fler granskningar.

Åtgärder som kräver ändringar i regelverk och teknik:

- Göra säkerhetskraven mätbara baserat på säkerhet, dataskydd och i förhållande till antal användare och nya användare, så att granskande myndighet kan mäta aktörerna.
- Upprätta och implementera en eskaleringsprocess med påföljder för aktörer som inte uppfyller kraven eller åtgärdar brister efter påpekande.
- Förstärka kraven på incidentrapportering. Idag ställs krav på rapportering vid större incidenter, men det finns inga krav om att rapportera driftsavbrott, bristande svarstider, eller bristande kvalitet i leveransen etc.
- Författningsreglera hela eller delar av infrastrukturen i syfte att stärka det idag civilrättsliga regelverket och förtydliga ansvarsområden hos aktörerna i inom infrastrukturen samt mandat hos kravställande myndigheter.
- Upprätta en process för att hantera om en brevlådeoperatör lämnar infrastrukturen, som bland annat omfattar ett sätt att meddela dess användare om förändringarna.

5.4.2 Höjd beredskap och krig

I höjd beredskap och krig ökar konsekvenserna för både individ och Sverige. Det är svårt att förutse alla tänkbara scenarios, men troligt är angrepp i syfte att förändra ”Sverigebilden”, motståndskraft i samhället, tilltro till myndigheter etc. Det kan konstateras att tidigare analyser av Mina meddelanden inte tagit höjd för att infrastrukturen ska fungera tillfredsställande vid höjd beredskap och krig. Utifrån nuvarande identifierade säkerhetsbrister som finns vid höjd beredskap och krig är en rekommendation att det säkerställs tekniska, organisatoriska och juridiska förutsättningar för att kunna garantera infrastrukturens säkerhet genom exempelvis nedsläckning av hela eller delar av infrastrukturen.

Inom ramen för totalförsvaret behöver en bredare analys göras för att utröna om alla delar i Mina Meddelanden är av vikt för totalförsvaret eller om det bara är samhällsviktigt upp till en viss nivå.

6 Framtidens infrastruktur för digital post

6.1 Infrastrukturen behöver transformeras

Digg har i kapitel 3. Nulägesanalys och kapitel 5. Risk- och säkerhetsanalys beskrivit och analyserat risker och brister samt behov av förändringar av dagens infrastruktur.

Analyserna visar på brister som det i dagens infrastruktur finns begränsade möjligheter att åtgärda. Det gäller främst kraven på ökad säkerhet och robusthet men även möjligheten att göra anpassningar för att möta behov från såväl avsändare som mottagare. Ändamålsenligheten i dagens lösning är i många avseenden begränsad till de behov som identifierades för mer än tio år sedan då infrastrukturen skapades och till det kommer brister i förmågan att följa den tekniska utvecklingen. Digg anser att åtgärder i dagens infrastruktur inte är tillräckligt för att säkerställa en säker och robust hantering av elektroniska försändelser i höjd beredskap och krig. Mot bakgrund av detta föreslår Digg att dagens infrastruktur genomgår en större transformation och att detta sker skyndsamt.

För att en infrastruktur för digital post ska bli kostnadseffektiv ska den nya lösningen nyttja existerande funktionalitet inom olika byggblock som tillhandahålls inom Ena – Sveriges digitala infrastruktur, där så är lämpligt.

6.2 Mål med ny infrastruktur

Framtidens infrastruktur för digital post i den offentliga förvaltningen ska säkerställa leverans av digital post vid var tid utan påverkan av yttre omständigheter. Lösningen ska vara robust, säker, kostnadseffektiv och säkerställa att enskilda alltid har åtkomst till sina elektroniska försändelser.

Den nya infrastrukturen ska utformas för att vara framtidssäker och vid var tid uppfylla gällande lagstiftning och säkerhetskrav, samt kunna möta potentiella krav som ställs på infrastrukturen i händelse av höjd beredskap och krig.

Digg bedömer att den föreslagna lösningen åtgärdar de brister som identifierats i nulägesanalysen samt hanterar och reducerar de risker som beskrivs i bilaga 1, genom att:

- Skapa en säkrare elektronisk kommunikation mellan avsändare och mottagare.
- Ge förutsättningar för att hantera behov av förändringar på ett effektivt sätt.
- I högre grad än i dag tillgodose juridiska och säkerhetsmässiga risker som identifierats, dels utifrån ett nuläge där sekretess och dataskydd är i fokus, dels inför en situation att Sverige skulle ställas inför höjd beredskap och krig.

6.3 Ny infrastruktur för digital post

De centrala funktionerna som utgör kärnan i den föreslagna nya infrastrukturen för digital post är central meddelandehantering med central lagring och visningsklienter.

Utöver dessa centrala funktioner finns behov av funktioner för ombudshantering, organisationsidentifiering, auktorisation, tillgänglighet och spårbarhet inom infrastrukturen. Dessa funktioner återfinns i befintliga byggblock inom Ena eller är under utveckling och kan återanvändas i den nya infrastrukturen för digital post. Dock ska poängteras att för de byggblock som nämns ovan finns också behov av ytterligare finansiering och rättsliga förutsättningar för att de ska kunna stödja utvecklingen, i enlighet med vad Digg bland annat anfört i budgetunderlaget inför 2023.

Det finns också behov av att möjliggöra för personer som inte har svenskt personnummer att ta emot digital post från myndigheter.

6.3.1 Central meddelandehantering med central lagring i statlig regi

Med en central meddelandehantering finns samtliga meddelanden som skickas inom infrastrukturen lagrade på ett (1) ställe. Det är till den centrala meddelandehanteringen som mottagarens försändelser skickas. För att säkerställa skyddet av data och individens tillgång till försändelsen över tid förespråkar Digg att den centrala meddelandehanteringen tillhandahålls i statlig regi. Till meddelandehanteringen ansluts sedan så kallade visningsklienter som är den tjänst

som visar försändelser som finns lagrade i det centraliserade meddelandelagret för mottagaren.

Ett utökat statligt ansvar för meddelandehanteringen från myndigheter till enskilda säkerställer enskildas tillgång till meddelanden vid höjd beredskap och krig, och medför en mer robust och säker meddelandehantering jämfört med dagens lösning. Det ger också möjlighet för användaren att byta leverantör av visningsklient och fortsatt ha tillgång till sina tidigare försändelser från myndigheter.

Den centrala meddelandelagringen bör implementeras på ett sådant sätt att den speglas över ett flertal datacenter. Genom en sådan åtgärd kan meddelanden göras tillgängliga, även om ett datacenter skulle ha problem med att tillhandahålla meddelandena vid ett givet tillfälle, vilket ökar robustheten i lösningen. För ökad säkerhet bör försändelser lagras krypterade på mottagarnivå med hjälp av asymmetrisk kryptering.

Den centrala meddelandehanteringen innebär att viss funktionalitet som idag finns ute hos respektive brevlådeoperatör blir centraliserad. Bland annat blir funktionaliteten för att avisera en mottagare om att det finns nya meddelanden en central funktion. Detsamma gäller funktionalitet för enskild att ge behörighet till annan att få tillgång till inkomna meddelanden. Funktionaliteten kring behörighetstilldelning bör också möjliggöra att behörighet kan delas ut på en mer detaljerad nivå än vad som är möjligt idag.

6.3.1.1 Ny skyddsklass

För att ytterligare säkra distributionen av meddelanden från avsändare till central meddelandelagring föreslår Digg att det införs ytterligare en skyddsklass för försändelser. Den nya skyddsklassen avser en krypterad försändelse från avsändare till mottagare. Denna typ av försändelse höjer säkerheten vid överföringen och varje meddelande till en mottagare krypteras individuellt.

6.3.1.2 Central meddelandehantering ökar kapaciteten

Jämfört med dagens lösning, där förmedling innebär en kontroll mot Förmedlingsregistret (FaR) för att få information om användaren önskar digital post och vilken brevlåda en försändelse ska skickas till, blir förmedlingen i den nya lösningen förenklad. Försändelser kommer att skickas till den centrala

meddelandelagringen i stället för att distribueras till olika brevlådeoperatörer vilket förenklar förmedlingens anslutningar.

6.3.2 Visningsklient i stället för brevlådor

En visningsklient visar upp de meddelanden som finns i den centrala meddelandelagringen. Utifrån en identifierad användares behörighet, vars regelverk upprättas och kontrolleras centralt, möjliggör den centrala meddelandelagringen för en visningsklient att visa upp de meddelanden som ingår i behörigheten för den identifierade användare, som kan vara en privatperson, en representant för ett företag eller ett ombud för en person eller ett företag.

Digg anser att det ska finnas en statlig visningsklient för att säkerställa att enskilda alltid kan hantera sin post från offentlig verksamhet. En statlig visningsklient ska vara tillgänglig för så många som möjligt utan att göra avkall på säkerheten.

En statlig visningsklient ska också möjliggöra användning av (samtliga) e-legitimationer enligt minst nivå 3 i Tillitsramverket för svensk e-legitimation inkluderat en eventuell kommande statlig e-legitimation, som Digg har i uppdrag att föreslå utformning av.[23]

6.3.2.1 Privata leverantörer som erbjuder visningsklienter

Digg anser att det är viktigt att även fortsättningsvis möjliggöra för dagens brevlådeoperatörer och andra privata aktörer att vara anslutna till infrastrukturen. Brevlådeoperatörernas roll förändras dock jämfört med dagens infrastruktur då de i stället för att lagra meddelanden från myndigheter kan ansluta som visningsklienter. Försändelser som lagras centralt ska kunna nås från den visningsklient som den enskilde själv väljer att teckna avtal med och alltid från den statliga visningsklienten.

Genom att möjliggöra för privata leverantörer att ansluta som visningsklienter uppnås flera fördelar för mottagaren, såsom möjligheten att komma åt alla sina försändelser, från både privata avsändare och myndigheter, samlat på ett ställe.

Att möjliggöra för privata leverantörer att ansluta som visningsklienter i stället för att de, som idag, även lagrar post från offentlig verksamhet kan i vissa avseenden sänka tröskeln för att ansluta till infrastrukturen och bidra till att fler leverantörer

[23] Uppdrag att föreslå hur en statlig e-legitimation kan utformas, I2022/01335

ansluter. Därmed ökar valmöjligheten för enskilda. Konkurrens kan ge bättre förutsättningar för innovation och kundnytta genom att det utvecklas nya tjänster vilket kan leda till att fler mottagare ansluter sig till infrastrukturen. Lösningen eliminerar även vissa av de säkerhetsrisker som identifierats med att decentralisera lagring av stor mängd information mellan flera olika privata leverantörer utanför statlig insyn och kontroll.

Om en brevlådeoperatör lämnar den nuvarande infrastrukturen innebär det att meddelanden som skulle ha skickats digitalt i stället skickas analogt. I den nya infrastrukturen kommer meddelanden att fortsätta gå ut digitalt även om en visningsklient lämnar infrastrukturen. Detta eftersom meddelanden lagras centralt och valet om att ta emot meddelanden från myndigheter digitalt finns i den centrala meddelandehanteringen och inte hos brevlådeoperatörerna som idag. I den nya lösningen aviseras mottagare från den centrala meddelandehanteringen och meddelanden går alltid, enligt förslaget, att läsa i den statliga visningsklienten.

6.3.2.2 Reglering av visningsklienter

Visningsklienternas roll i den föreslagna lösningen skiljer sig från den roll som brevlådeoperatörer har i infrastrukturen idag. Vilka krav som ska ställas på de visningsklienter som vill ansluta till infrastrukturen behöver utredas. Digg har identifierat ett antal utgångspunkter att beakta i ett sådant arbete.

- En mottagare/enskild har rätt att bestämma över sina mottagna meddelanden.
- Om en visningsklient erbjuder tilläggsfunktionalitet ska detta regleras mellan enskild och tillhandahållare av visningsklient, inte genom Infrastrukturansvarig.
- Eventuella begränsningar i vad som ska få erbjudas kopplat till myndighetspost måste utredas vidare, samt om viss funktionalitet ska möjliggöras genom till exempel metadata om meddelanden.
- Det måste kunna säkerställas att visningsklienten agerar på uppdrag av en enskild, de får inte använda uppgifter utan samtycke.
- Det är viktigt att reglera vilken funktionalitet Infrastrukturansvarig ska tillhandahålla gentemot leverantörer av visningsklienter. Ett exempel på en sådan tjänst är information om firmatecknare som idag tillhandahålls inom infrastrukturen via Bolagsverket.

- Funktionalitet ska inte regleras i avtal mellan avsändare och tillhandahållare av visningsklient. En avsändare som vill säkerställa att alla mottagare av försändelser får samma möjlighet att använda exempelvis betalfunktionalitet för en fakturaförsändelse, oavsett vilken visningsklient som mottagaren använder, bör själv tillhandahålla denna funktionalitet.
- Ett av målen med den nya infrastrukturen är att kunna hantera behov av förändringar på ett effektivt sätt. Vilka krav som ställs på respektive aktör bör utformas för att möta detta mål.

Privata leverantörer som tillhandahållare av visningsklienter kräver även fortsättningsvis att Digg eller annan myndighet genomför granskning av dessa aktörer för att säkerställa att de lever upp till uppsatta krav. Den föreslagna lösningen bör dock medföra att detta arbete blir mindre omfattande än i dagens infrastruktur, men det påverkas av vilka krav som ska ställas på de visningsklienter som vill ansluta till infrastrukturen.

Det finns risk för fortsatta utmaningar kopplade till utveckling av infrastruktur och funktionalitet med privata leverantörer kopplade till infrastrukturen. Det är därför viktigt att det regleras hur vidareutveckling ska hanteras och hur nya krav kan ställas.

6.4 Ersättning till visningsklienter

I samband med utvecklingen av infrastrukturen anser Digg att behovet av ersättning till eventuella visningsklienter behöver ses över. I den nya lösningen som föreslås i denna rapport får dagens brevlådeoperatörer en annan roll vilket bör genomsyra en eventuell ersättning till visningsklienter. Ersättningsfrågan för den kommande lösningen behöver därför särskiljas från frågan om ersättning i den nuvarande lösningen.

En eventuell ersättning till visningsklienterna bör utformas på ett sätt som gör att den bidrar till samhällets fortsatta digitalisering och att prioriterad funktionalitet utifrån ett förvaltningsgemensamt perspektiv säkerställs. Även i detta avseende behöver finansieringen av en eventuell ersättning utredas vidare.

6.5 Digital post i andra länder

I arbetet med att ta fram förslag på åtgärder har Digg fört dialog med Danmark, Finland och Nederländerna om deras lösningar för digital post. Dessa tre länder

använder samtliga centraliserad lagring av meddelanden. Den lösning som Digg föreslår liknar till stor del den danska lösningen som bygger på att meddelanden lagras centralt och att visningsklienter, både statliga och privata, visar upp meddelanden för enskilda. Genom denna omvärldsanalys har vi stämt av att den föreslagna lösningen fungerar praktiskt och vi kan också ta del av de andra ländernas utmaningar och lärdomar.

Det finns också dialoger med de andra länderna kring möjligheten att skapa gränsöverskridande federationer för digital post. En sådan federation skulle kunna innebära att svenska personer som får digital post från utländska myndigheter kan ta del av dessa i den svenska lösningen och att motsvarande skulle fungera för utländska personer som är ansluten till digital post i annan medlemsstat.

7 Planering framåt

7.1 Åtgärdsplan

Den analys som Digg genomfört visar att det säkerhetspolitiska läget ställer krav på såväl säkerhet som robusthet som dagens infrastruktur inte kan tillmötesgå. För att skapa en säker, robust och ändamålsenlig infrastruktur behöver därför dagens infrastruktur och den statliga digitala brevlådan utvecklas. De olika åtgärderna som Digg föreslår nedan innebär en stegvis utveckling av den befintliga infrastrukturen mot en ny infrastruktur för digital post som är säker och robust. Åtgärderna beskrivs övergripande och listas i prioritetsordning.

Punkt 1–5 presenterar de åtgärder som Digg anser krävs för att höja säkerheten i dagens infrastruktur, utifrån de brister och risker som identifierats i utredningen. Digg rekommenderar starkt att även punkt 6–8 genomförs för att nå en så säker och robust lösning som möjligt. I det fall totalförsvaranalysen som ska genomföras av Digg visar på att infrastrukturen är en del av totalförsvaret anser Digg att punkt 6–8 är tvingande utifrån det säkerhetspolitiska läget.

1. Uppdatera säkerhetskyddsanalys. Denna behöver förnyas för att utreda om Mina meddelanden och Min myndighetspost faller in under säkerhetskyddslagstiftningen, utifrån huruvida infrastrukturen är att anse som samhällsviktig i normalläge. Beroende på resultatet kan kravbilden för befintlig och ny lösning påverkas. Genomföra totalförsvarsanalys för att utröna vilka delar av infrastrukturen som eventuellt har betydelse för Sverige vid höjd beredskap och krig.

2. Utreda eventuella ytterligare behov, utöver de som redovisas i denna rapport och som framkommer i den kommande säkerhetsskyddsanalysen, av förändringar i nuvarande lösning för att höja säkerheten och robustheten i infrastrukturen och Min myndighetspost. Arbetet ska bedrivas i samverkan med parter som är anslutna till infrastrukturen (främst utvalda avsändande myndigheter och brevlådeoperatörer) men även samverkan med expertmyndigheter såsom MSB, PTS och IMY kan bli aktuell. Även Skatteverket, i egenskap av it-driftleverantör åt Digg, behöver involveras i arbetet.

3. Utifrån identifierade behov analysera behov av regeländringar i nuvarande lösning.
    - Regeländringar som ryms inom Diggs mandat genomförs. Exempel på regeländringar som ryms inom Diggs mandat är eventuella ändringar av allmänna villkor med tillhörande bilagor för Mina meddelanden, användarvillkor för Mina meddelanden och användarvillkor för Min myndighetspost. Vidare kan det även vara aktuellt att införa föreskrifter[24].
    - Regeländringar som ligger utanför Diggs mandat påtalas för behörig instans, exempelvis Regeringskansliet.

4. Genomföra säkerhetshöjande åtgärder i dagens produktionsmiljö för Mina meddelanden och Min myndighetspost. Nedan listas prioriterade åtgärder, de kan dock komma att påverkas av resultatet av en genomförd säkerhetsskyddsanalys och ytterligare behovsinsamling.
    - Informationsseparering, som innebär att Mina meddelanden och Min myndighetspost får en egen IT-miljö hos Skatteverket. Detta är en pågående aktivitet, utifrån krav från Riksrevisionen. Efter denna åtgärd är informationen tillräckligt separerad från Skatteverket. Detta medför ökad säkerhet och ökad effektivitet då Skatteverkets och Mina meddelandens IT-miljöer påverkar varandra i minsta möjliga mån.
    - Utökad kryptering.

[24] Digg får med stöd av 5 § förordningen om myndighetsgemensam infrastruktur för säkra elektroniska försändelser meddela de föreskrifter som behövs för inrättande och drift av infrastrukturen. Digg har hittills inte nyttjat detta bemyndigande.

- Möjlighet för Digg att kontakta brevlådeinnehavare inom Mina meddelanden, oavsett brevlådeoperatör, med syftet att kunna informera om alternativa brevlådor för att ta emot sin post från myndigheter, i det fall en brevlådeoperatör lämnar infrastrukturen.

5. Konstruera en ny meddelandelagring med visningsklient, som ersätter dagens Min myndighetspost och hanterar de risker och brister som identifierats för brevlådan. Lösningen ska:
    - Byggas på ny modern teknik.
    - Stödja utökade behov av datalagring.
    - Använda ny säkrare datalagring/kryptering.
    - Möjliggöra för personer som inte har svenskt personnummer att ta emot digital post från myndigheter.
    - Möta mottagare och avsändares behov av funktionalitet.

6. Genomföra förberedande aktiviteter för att gå över till en ny lösning för Mina meddelanden med ett centralt meddelandelager dit all post skickas och som bygger på den lösning som tagits fram för Min myndighetspost, i steg 6. Förberedelserna innefattar bland annat att:
    - Utreda behov av och föreslå regleringsförändringar.
    - Utreda behov av obligatorium.
    - Utreda vilka krav som ska ställas på visningsklienter.
    - Utreda frågan om ersättning till visningsklienter. Digg anser att annan part bör ansvara för detta.
    - Utreda långsiktig IT-drift.
    - Förbereda utökade krav på driftmiljöer och lagring.
    - Samverka med avsändare kring säkerhetsbehov.
    - Ta fram ett anslutningsförfarande inklusive process för granskning av visningsklienter.
    - Ta fram en plan för hur övergången ska genomföras.

7. Genomföra en övergång till ny lösning för Mina meddelanden med ett centralt meddelandelager. Hur och när övergången ska genomföras är beroende av det som framkommer och beslutas under förberedelserna i steg 7. Övergången innefattar bland annat att:
    - Möjliggöra migrering av försändelser till centralt meddelandelager
    - Hantera utökade behov av datalagring.
    - Hantera förändringar i förmedlingsadressregistret.

- Hantera ansökan, granskning och anslutning av visningsklienter.
- Uppdatera förmedlingen av försändelser hos avsändare.
- Information och kommunikation om förändring till enskilda och samtliga aktörer i infrastrukturen.

8. Införande av ny skyddsklass.

7.1.1 Tabell mappning risker och föreslagna åtgärder

Tabellen nedan visar vilka utav de föreslagna åtgärderna som hanterar de identifierade bristerna och riskerna. Riskerna beskrivs i Bilaga 1.

Mappning av vilka åtgärder som hanterar identifierade brister och risker, eller minskar konsekvenserna av riskerna	Brister från kap 3.2 och kap 4. Risker från kap 5, specificerade i bilaga 1													
Åtgärder	3.2.2 Svårt att vidareutveckla Mina Meddelanden	3.3.1.1 Separering av IT-miljöer	3.3.2.1 Begränsningar i dagens datalagring	3.3.2.2 Kryptering av lagrade data	3.3.2.3 Teknisk skuld i Minmyndighetspost	4. Behov av regelutveckling	RSA 0	RSA 1	RSA 2	RSA 3	RSA 4	RSA 5	RSA 6	Kommentar
Förbättrade rutiner och processer i nuvarande lösning						M				M	M			Arbete pågår.
Regeländringar i nuvarande lösning	M				M	M				M	X			
Säkerhetshöjande åtgärder i dagens produktionsmiljö		X		M										
Ny meddelandelagring med visningsklient			X	X	X									
Övergång till centralt meddelandelager	M					X	M	X	M	X	M	M	M	
Införande av ny skyddsklass				M									M	Förstärker kryptering för särskilt känslig information

X= löser/minimerar risken

M = Minskar konsekvenser av risken

7.2 Estimerade kostnader för utveckling och investering

Digg har tillsammans med Skatteverket genomfört en övergripande estimering av de föreslagna åtgärderna samt vilka ytterligare investeringar som behövs i infrastruktur, samt behovet av information och kommunikationskampanjer i samband med övergången till ny infrastruktur. De beräknade kostnaderna behöver dock fortsätta analyseras i takt med att mer kunskap gällande åtgärderna erhålls. Kostnaderna kommer också att bero på beslut om de regleringsförändringar som sannolikt behöver genomföras för att uppnå målet. Digg har inte tagit med kostnader hos avsändare och brevlådeklienter i analysen. Påverkan på avsändare

planeras att bli minimal. De brevlådeoperatörer som idag är anslutna till infrastrukturen och vill fortsätta vara anslutna som visningsklienter kommer få en kostnad i samband med övergången. Här bör en utredning göras för att besluta om en eventuell ersättning för detta arbete. Digg bedömer att det i samband med övergången till ny lösningen bör genomföras kommunikationskampanjer för att informera om lösningen till samtliga aktörer i infrastrukturen, samt för att ytterligare öka anslutningen på både avsändar- och mottagarsidan.

Utvecklingen av digital post enligt beskriven åtgärdsplan förutsätter att Digg ges ytterligare finansiering och att författningsändringar genomförs. Dock kan den del av lösningen, som är kopplad till att möjliggöra för personer med andra identitetsbegrepp än svenskt personnummer att ta emot digital post, genomföras med den finansiering myndigheten har fått för att uppfylla SDG – förordningen[25].

7.2.1 Tabell åtgärder, tidsplan och estimerad kostnad

Åtgärd	Tidplan	estimat timmar	Övriga kostnader
Utreda förslag om regeländringar i nuvarande lösning	Q1-Q4 2023	2 000	
Uppdatera säkerhetskyddsanalys	Q1 2023	300	
Säkerhetshöjande åtgärder i dagens produktionsmiljö	2023	500	
Ny meddelandelagring med visningsklient	2023-2024	30 000	
Förberedelser för centralt meddelandelager	2023-2024	8 000	
Övergång till centralt meddelandelager	2024-2026	10 000	75 000 000
Införande av ny skyddsklass	2025-2026	10 000	
Information till enskilda och aktörer i infrastrukturen			20 000 000
	kostnad utveckling kr:	66 755 700	
	kostnad infrastruktur kr:		75 000 000
	kostnad information kr:		20 000 000
	Totalt investeringsbehov kr:	161 755 700	

Investeringen i infrastruktur är beräknad på redundans över fyra lokationer.

[25] Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012

7.3 En kostnadsanalys för förvaltning

Under 2022 är kostnaden för drift, förvaltning och vidareutveckling av infrastrukturen för digital post och brevlådan min myndighetspost uppskattad till ca 40 000 0000 kr (inkluderat upparbetade avskrivningar).

Vid införandet av ny lösning kommer det vara behov för parallella drifts- och utvecklingsmiljöer under en längre period till dess att det är möjligt att avveckla existerande miljöer. Då tillkommer en kostnad för avveckling av dagens miljöer och infrastruktur.

Kostnad för drift och förvaltning av ny lösning, vilket innebär att man inför samtliga åtgärder i tabell 7.2, är estimat med mycket stor osäkerhet, beräknad utifrån följande förutsättningar och antaganden:

- Tillgänglighet 24/7.
- Beräknat utifrån exempel meddelandevolym på 200 000 000 meddelanden.
- Hälften av meddelandena aviseras via sms.
- Kostnad för sms-avisering är i dagsläget 30 öre per sms.
- Kostnader för sms-avisering hanteras centralt i lösningen, inte hos respektive visningsklient.
- Kostnad för inloggning med e-legitimation är 17 öre per inloggning enligt valfrihetssystemet.
- Inloggning med e-legitimation görs hos visningsklient, här beräknat att ¼ del av mottagarna använder den statliga brevlådan.
- Inte beräknat ersättning till visningsklienter.
- Drift över fyra lokationer är estimerad till 30 procent av investeringskostnaden.

Förvaltning och drift för ny lösning, med utgångspunkt i 200 miljoner skickade meddelanden per år:

- Organisation för drift och förvaltning = 20 miljoner kr.
- Sms-avisering 100 miljoner meddelanden x 0,3 kr = 30 miljoner kr.
- Inloggning e-leg = 50 miljoner meddelanden x 0,17 kr = 8,5 miljoner kr.
- Drift (med redundans 4 lokationer) = 22,5 miljoner kr.

Årlig drift och förvaltning: 81 miljoner kr.

Enligt räkneexemplet ovan med en meddelandevolym på 200 miljoner meddelande per år beräknas nyttan i form av kostnadsbesparingar (enligt principer som beskrivs i avsnitt 2.5) till 600 miljoner kr per år.

Årlig kostnadsbesparing: 600 miljoner kr.