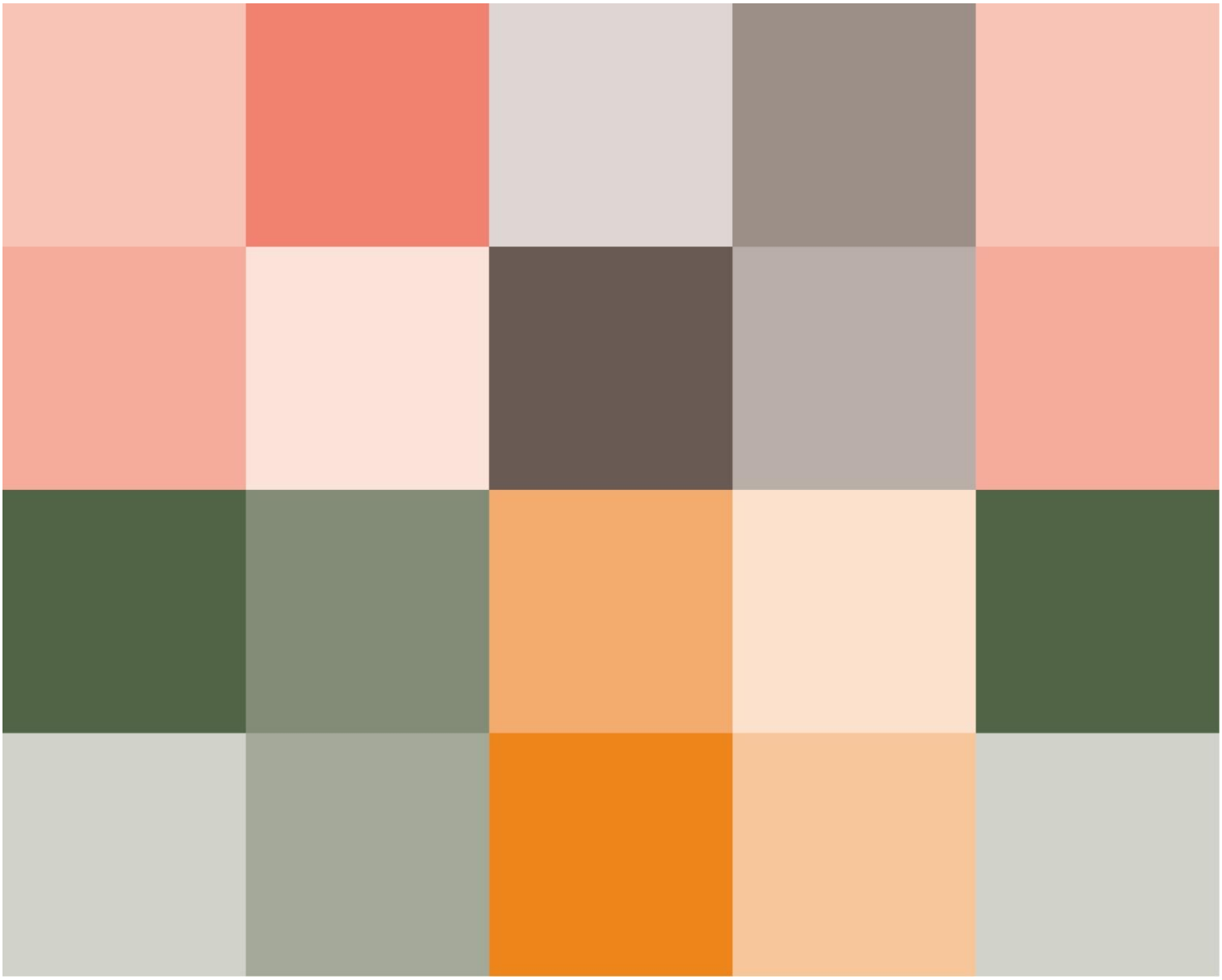

Delrapportering av uppdrag att tillhandhålla infrastruktur för säker digital kommunikation i offentlig sektor.

30 september 2022
Dnr I2021/03317
DIGG:s dnr 2021-2909

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

DIGG delredovisar regeringsuppdrag att utveckla och tillhandahålla infrastruktur för säker digital kommunikation inom offentlig sektor (I2021/03317) genom att presentera relevanta delar av pågående arbete och analyser i denna rapport.

Syftet med säker digital kommunikation (SDK) är att möjliggöra säkert och effektivt digitalt utbyte av bland annat känsliga personuppgifter och sekretessbelagd information inom offentlig sektor inklusive privata utförare av helt eller delvis offentligt finansierad verksamhet. Målet är att ersätta informationsutbyte som idag sker via fax, brev, telefon och andra analoga eller digitala kanaler som uppfattas som ineffektiva samt kan innebära säkerhetsrisker. Verksamhetsområden som identifierats där det finns särskilt stort behov för en säker digital lösning är bland andra socialtjänst och skola, kommunal vård och omsorg, samt hälsa och sjukvård.

Med utgångspunkt i SDK:s användningsområde och målsättningen om en bred anslutning inom hela den offentliga sektorn, inkluderat privata aktörer, har DIGG genomfört analyser av juridiska problemställningar samt risk och säkerhetsanalyser för att säkerställa att infrastrukturen har potential att uppfylla sitt syfte. Analyser har genomförts avseende de tekniska komponenterna, ramverk och regelverk, vad som krävs för att hantera förvaltning, anslutningsprocess och stöd till deltagare. Det har även genomförts analyser för att utreda frågor kopplade till upphandling, konkurrens, sekretess och dataskydd samt avtal. DIGG har också utrett och lämnar förslag på hur drift och förvaltning av infrastrukturen långsiktigt ska finansieras.

Analyserna ligger till grund för det fortsatta arbetet hos DIGG med att ta över ansvaret för SDK. DIGG har fattat ett inriktningsbeslut att tillhandahålla SDK i egen regi och har etablerat ett uppdragsteam för arbetet. Kunskapsöverföring från Inera är centralt i det vidare arbetet. DIGG har också etablerat samarbete med SKR, Inera och utpekade myndigheter för att främja anslutning. DIGG har utifrån hittills insamlade erfarenheter identifierat att kostnaderna för genomförandet överstiger medel som DIGG initialt fick för genomförandet av uppdraget, vilket också hanteras av Regeringen för 2022. DIGG behöver dock förstärkning fortsatt under 2023 och framåt för att de främjande och vidareutvecklande åtgärderna som

föreslås i rapporten ska kunna genomföras. Även de medel som DIGG äskat för åtgärder inom civilt försvar via MSB bedöms behövas för säkerhetsåtgärder.

Rättslig bedömning

Sammanfattningsvis föreligger inga rättsliga hinder utifrån det tilltänka upplägget i SDK. DIGG har identifierat vissa juridiska risker som kan uppstå i händelse av att en deltagare bryter mot regelverket i SDK. DIGG ser behov av riskreducerande åtgärder samt vidare arbete för att motverka identifierade juridiska risker och otydligheter. Dessa behöver genomföras hos DIGG, Inera, deltagare och accesspunktsoperatörer.

DIGG anser att myndighetens instruktion behöver revideras med en reglering där det framgår att DIGG ska ansvara för infrastrukturen. I det fortsatta arbetet med rättsliga förutsättningar behöver det genomföras analyser av möjligheten till kontroller av deltagare och leverantörer gällande regelefterlevnad, om behov föreligger att författningsreglera hela eller delar av anslutningen till SDK, samt av privata aktörers avtalsförhållanden beträffande deras anslutning till SDK. DIGG planerar tillsammans med Inera fortsatt behovsanalys av privata aktörers anslutning till SDK med tillhörande utredning gällande konkurrensaspekterna för detta.

DIGG anser att den hantering som sker hos externa leverantörer är att betrakta som teknisk bearbetning och lagring. Det innebär att det föreligger en straffsanktionerad tystnadsplikt hos samtliga leverantörer i SDK:s informationskedja. Enligt DIGGs uppfattning går det ifrågasätta om uppgifterna ska anses som röjda. Eftersom bedömningar beträffande när uppgifter anses röjda ankommer varje enskild deltagare föreslår DIGG en sekretessbrytande bestämmelse. Detta i syfte att frångå den potentiella röjandeproblematiken som kan uppstå för deltagarna i samband med utkontraktering inför och i anslutning till SDK.

Risker och åtgärder

SDK bygger på rätt säkerhet och systemisk tillit vilket ställer krav på bedömningar och systematiskt informationssäkerhetsarbete hos alla aktörer som ingår i infrastrukturen. I analysen har bland annat följande risker och åtgärder uppmärksammats.

Vid anslutning till SDK är det viktigt att deltagarna genomför ett grundligt rättsligt utredningsarbete för att inte risker kopplade till sekretessbestämmelser och bestämmelserna i dataskyddsförordningen ska uppkomma. Analyserna har visat att det finns risk för att främst kommuners tillgång till juridisk kompetens inom IT-rättsområdet är begränsad. DIGG kan bidra med vägledning för att underlätta för deltagarna, det förutsätter dock att finansiering för stöd till anslutning ges.

DIGG har identifierat en möjlig risk utifrån sekretess och dataskydd om en deltagare felaktigt anger funktionsadresser i adressboken vilket skulle kunna leda till att informationen når en otillåtet bred krets av mottagare. Åtgärder för detta finns idag och behöver vidareutvecklas för att anpassas till att omfatta alla anslutna deltagare.

Att anslutningen till SDK sker på kommun, region och myndighetsnivå, innebär att alla verksamheter inom en kommun eller region är anslutna till SDK som en deltagare. En korrekt behörighetshantering hos den funktion som har åtkomst till krypteringsnycklarna innebär sannolikt inte några juridiska problem, men en bristfällig informationssäkerhet där krypteringsnycklarna hanteras felaktigt kan medföra att sekretessuppgifter riskeras röjas. En åtgärd för att minimera risken att krypteringsnyckeln hanteras felaktigt är om anslutning sker på verksamhetsnivå i stället för organisationsnivå, vilket frångår tillämpningen om att varje deltagare fritt förfogar över att upprätta egna interna mottagare i SDK. Detta är dock en omfattande förändring som behöver föregås av en helhetsanalys då åtgärden bland annat påverkar arkitekturen, ansvarsförhållanden och kostnaderna i SDK.

DIGG har identifierat ett behov av att förtydliga krav på accesspunktoperatörer i form av regler och rutiner i samband med anslutning, samt behov av tydligare krav på certifikatshantering inom meddelandetjänsten. Arbete med att åtgärda dessa risker pågår.

Det finns identifierade risker som är kopplade till DIGGs nuvarande organisation för utveckling och tjänsteförvaltning, vilket belyser viktiga områden som DIGG behöver förstärka och förbättra inför övertagandet av ansvar för hela SDK-infrastrukturen. Dessa risker är förbättringsområden på DIGG och kommer åtgärdas inom ramen för det pågående arbetet med övertagandet av ansvaret samt i förvaltningen av plattformen.

DIGG planerar genomföra en säkerhetsskyddsanalys för att utreda om plattformen träffas av säkerhetsskyddslagstiftning (SFS 2018:585). Detta kommer genomföras i ljuset av det säkerhetspolitiska läget och ny beredskapslagstiftning.

Finansieringsmodell

DIGG föreslår att drift och förvaltning av SDK ska finansieras genom ett förstärkt förvaltningsanslag till DIGG. Dagens finansiering sker via ett årligt regeringsbeslut från anslagspost 2:7 ap.3, vilket DIGG föreslår istället ska ligga permanent på DIGGs förvaltningsanslag (2:6 ap.1).

DIGG bedömer att anslagsfinansiering skapar bättre förutsättningar för möjligheter för att förvaltningsgemensamma tjänster ska användas på ett sådant sätt som avses, medan en avgiftsfinansiering i många fall motverkar anslutning och användning.

Avgiftsfinansiering skulle troligen leda till en bedömning att anslutningen till SDK är upphandlingspliktig för kommuner och regioner. En upphandlingsplikt bedöms motverka ett brett införande och en hög anslutningsgrad till SDK.

Innehållsförteckning

1 Inledning

1.1 Om uppdraget

Myndigheten för digital förvaltning (DIGG) fick den 16 december 2021 ett regeringsuppdrag att utveckla och tillhandahålla infrastruktur för säker digital kommunikation inom offentlig sektor (I2021/03317). DIGG ska utifrån de erfarenheter och den pilotverksamhet för Säker digital kommunikation (SDK), som bedrivits i samarbete mellan Sveriges Kommuner och Regioner (SKR) och DIGG under 2022, förbereda för att senast den 29 september 2023 ansvara för tillhandahållandet av infrastruktur för säker digital kommunikation.

Målsättningen är att infrastrukturen för säker digital kommunikation på sikt ska kunna användas av, och vara till nytta för, hela den offentliga sektorn samt kunna användas för kommunikation med privata utförare av helt eller delvis offentligt finansierad verksamhet och andra organisationer som offentlig sektor har behov av att kommunicera med.

Denna delredovisning av uppdraget redogör för resultatet av de analyser som har genomförts och som ligger till grund för det fortsatta arbetet med infrastruktur för säker digital kommunikation. Detta i enlighet med uppdraget att redovisa resultatet av en riskbedömning och en beskrivning av vilka åtgärder som vidtagits för att reducera dessa risker, analys av säkerhetskrav och en beskrivning av på vilket sätt infrastrukturen möter dessa krav, resultatet av en rättslig analys, en beskrivning av den nya infrastrukturens förhållande till andra infrastrukturer för säker kommunikation samt förslag på hur drift och förvaltning av infrastrukturen långsiktigt ska finansieras.

1.2 Bakgrund

Faxen används fortfarande i stora delar av offentlig sektor, särskilt inom hälso- och sjukvården, skolan och socialtjänsten. Utbyte av känsliga och sekretessbelagda uppgifter sker inte bara via fax, utan också via brev och andra kanaler. Statliga myndigheter har delvis kunnat ersätta faxen genom strukturerade elektroniska informationsutbyten, men använder faxen för att kommunicera med välfärdens verksamheter. För att alla verksamheter inom välfärden ska kunna kommunicera på ett säkert och effektivt sätt så behövs en gemensam infrastruktur som uppfyller kraven på en god informationssäkerhet.

Under flera år har SKR drivit utvecklingsarbetet kring SDK. SKR initierade i 2015 arbete med en långsiktig lösning för utbyte av känslig information mellan olika organisationer i offentlig sektor. 2016 publicerade SKR en rapport, *2016-03-31, version 1.1, om Säker digital meddelandehantering mellan myndigheter, Nuläges- behovs- och marknadsanalys.* Rapporten låg till grund för uppstarten av SDK-projektet. Rapporten beskriver behov och viktiga aspekter som en då framtida lösning behöver hantera. Det handlar om att enkelt och snabbt kunna skicka och ta emot meddelanden i den normala arbetssituationen, och att man därmed ska kunna minska administration och ledtider i arbetsprocesserna. Kravet på säkerhet är primärt, vilket gör att det är särskilt viktigt att tekniska lösningar verkligen säkerställer att integritetskänsliga personuppgifter inte hamnar i fel händer. Utöver tekniska lösningar förutsätts en organiserad samverkan över myndighetsgränser för att långsiktigt möta behovsbilden. De grundläggande behov som lyfts fram i rapporten som avgörande för en gemensam lösning är följande:

- *Tillförlitlighet*, vilket rör frågor som ”hur hindrar jag att integritetskänslig information kommer i orätta händer?”, ”hur hittar jag rätt mottagare?” och ”hur kan jag vara säker på att bara avsedd mottagare kan läsa meddelandet?”. För mottagaren är det förstås också viktigt att kunna lita på att ”avsändaren verkligen är den som den utger sig för att vara”.
- *Skydd mot obehörig åtkomst*, vilket innebär att säkerställa att integritetskänslig information inte kommer i orätta händer. Skydd mot obehörig åtkomst till elektroniskt lagrad och förmedlad information löses i allmänhet genom kryptering.
- *Adressering*, vilket innebär att ett meddelande bör vara ställt till en ”funktion” eller ”roll” i den mottagande organisationen, inte riktat till enskilda medarbetare.
- *Autentisering*, vilket handlar om tillförlitlighet vid säkerställande av avsändares och mottagares identiteter. Exempelvis genom behovet av elektroniska certifikat som båda sidor kan lita på genom att båda organisationerna i avtal är bundna till att hantera den egna organisationens certifikat enligt givna överenskomna regler och rutiner (identitets-federationer).

2016 startades utvecklingsprojektet SDK i regi av SKR. Utvecklingsarbetet har finansierats av och bedrivits i samarbete med ett stort antal kommuner och

regioner samt flera statliga myndigheter. Inera[1] har på uppdrag av SKR drivit utvecklingsprojektet SDK och DIGG har sedan 2018 bidragit med kompetens och finansiering. Det genomfördes flera pilotstudier under 2019 och 2021 där kommuner, regioner och myndigheter deltog, vilket bidragit till lösningens utveckling samt att sprida kunskap och intresse för SDK. Hösten 2020 tog DIGG en mer aktiv roll i genomförandet som ansvarig för utveckling av delar av den tekniska lösningen. 1 mars 2022 produktionsattes SDK och lanserades som tjänst hos Inera, vilket innebär att det sedan dess är möjligt att ansluta till och använda SDK. Ansvaret för SDK är i dagsläget delat mellan SKR/Inera och DIGG där Inera är federationsägare och tillhandahåller SDK-federationen (se avsnitt 3.2.2) och DIGG tillhandahåller den underliggande plattformen för transportinfrastruktur (se avsnitt 3.2.1)

I december 2021 ingicks en överenskommelse mellan staten och SKR, *En överenskommelse mellan staten och Sveriges Kommuner och Regioner om etablering och införande av infrastruktur för säker digital kommunikation i offentlig sektor,* med syfte att åstadkomma en gemensam syn på mål, takt, finansiering och ansvar när det gäller utveckling och förvaltning av, samt anslutning till, infrastruktur för säker digital kommunikation. Överenskommelsen är en del av regeringens och SKRs gemensamma och långsiktiga arbete med att utveckla välfärdens digitala infrastruktur. Staten åtar sig i överenskommelsen att senast den 29 september 2023 ta ansvar för att tillhandahålla en infrastruktur för säker digital kommunikation. SKR åtar sig att under en övergångsperiod från den 1 januari 2022 och fram tills dess att DIGG tillhandahåller en infrastruktur, i samverkan med DIGG, etablera och tillhandhålla en infrastruktur för säker digital kommunikation. SKR åtar sig även att aktivt arbeta för att kommuner och regioner ansluter till infrastrukturen under 2022. DIGG ska också inom ramen för sitt uppdrag stödja införandet och anslutning till den infrastruktur som etableras under 2022.

1.3 Metod och utgångspunkt för DIGGs genomförande

DIGG har under våren 2022 analyserat infrastrukturen för SDK utifrån olika perspektiv för att få en förståelse för vad uppdraget att tillhanda infrastrukturen kommer innebära för myndigheten. Analyser har genomförts

[1] [1] Inera är ett aktiebolag som ägs av regioner, kommuner och SKR Företag.

avseende de tekniska komponenterna, ramverk och regelverk, samt vad som krävs för att hantera förvaltning, anslutningsprocess och stöd till deltagare. Det har även genomförts rättsliga analyser för att utreda frågor kopplade till upphandling, konkurrens, sekretess och dataskydd samt avtal. DIGG har därutöver genomfört risk- och säkerhetsanalyser. Vidare har DIGG bedömt vilka åtgärder som behöver vidtas för att leva upp till relevanta krav och reducera risker. Analyserna är genomförda med stöd av Inera. DIGG har även samrått med Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet gällande infrastrukturens utformning. DIGG har etablerat samverkan med de myndigheter[2] som i respektive regleringsbrev för 2022 fått i uppdrag att förbereda anslutning till SDK, samt löpande informerat de myndigheter som ingår i uppdraget att etablera den förvaltningsgemensamma digitala infrastrukturen.[3]

DIGG har analyserat olika alternativa modeller för att tillhandhålla infrastrukturen från och med 29 september 2023. DIGG fattade i juni 2022 ett inriktningsbeslut om att SDK-federationen ska flyttas från Inera till DIGG, så att DIGG kan ta ett helhetsansvar för hela SDK-infrastrukturen. Inriktningsbeslutet förutsätter ett mycket nära samarbete med SKR och Inera i genomförandet. Det innebär också att DIGGs samarbete med Försäkringskassan gällande drift av infrastruktur behöver fördjupas (avsnitt 8.3).

För att bibehålla kontinuiteten i arbetet med SDK har DIGG som utgångspunkt att existerande infrastruktur, arkitektur, principer, ramverk och processer ska återanvändas i så stor grad som är ändamålsenligt, beaktat resultat av de analyser som genomförs inom ramen för uppdraget. Ytterligare en utgångspunkt har varit att infrastrukturen ska utgå från och komplettera det arbete som bedrivs med att etablera den förvaltningsgemensamma digitala infrastrukturen Ena (avsnitt 6.1).

---

[2] Myndigheter som fått uppdrag gällande SDK är Arbetsförmedlingen, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Polismyndigheten, Kriminalvården, Skolverket, Socialstyrelsen, Statens institutionsstyrelse

[3] (I2019/03306, I2020/03366 och I2020/02753)

2 SDK målgrupp och nytta

2.1 Målgrupp för SDK

Målbilden som togs fram i 2017 i samband med utvecklingsprojektet SDK var att skapa en lösning som möjliggör utbyte av information digitalt på ett enhetligt, effektivt, säkert och överenskommet sätt, oavsett om deltagaren är en offentlig aktör eller privat aktör inom offentligt finansierad verksamhet.

I regeringsuppdraget framgår att tilltänkta deltagare i SDK är offentlig sektor och dess behov att kommunicera med varandra, företag och andra organisationer. Som exempel nämns privata utförare av offentligt finansierad verksamhet samt andra organisationer som offentlig verksamhet har ett behov av att kommunicera säkert med.

Med offentlig sektor avses i denna delrapportering alla statliga myndigheter, kommuner, regioner, kommunala- och regionala bolag samt förbund. I arbetet med SDK har det förutsatts att privata aktörer inom offentligt finansierad verksamhet har ett behov av och ska ingå i SDK. I behovsanalyser av exempelvis skola, vård och omsorg har ingen distinktion gjort mellan privata utförare och offentlig aktör. Istället har det förutsatts att behoven av SDK inom verksamheterna är de samma, obeaktat av om verksamheten bedrivs i offentlig eller privat regi.

Antalet privata utförare inom kommunal, respektive regionverksamhet 2020, uppgick till dryga 43 500 privata utförare av kommunal verksamhet och 5 100 privata utförare av regional verksamhet. Samma utförare kan förekomma i olika verksamhetsområden inom en kommun/region eller hos flera kommuner/regioner, men antalet unika privata utförare var 2020 närmare 11 500 stycken.[4]

[4] Källa: SCB's allmänna företagsregister: Företag (FDB) efter näringsgren SNI 2007, ägarkategori och storleksklass

2.2 Fallstudie av SDK

För att få en ökad förståelse för kommuners och regioners olika förutsättningar att tillvarata digitaliseringens möjligheter genomförde DIGG under 2021 en fallstudie genom att studera utvecklingsprojektet SDK. Fallstudiens uttalade syfte var att öka kunskapen om kommuners, regioners och statliga myndigheters olika förutsättningar att ansluta till och använda SDK.

Det framkommer i studien att överlag finns en stor medvetenhet om att befintliga metoder och tillvägagångssätt för överföring av exempelvis känsliga personuppgifter och sekretessbelagd information är ineffektiva och innebär säkerhetsrisker. Mot bakgrund av de brister som dagens metoder innebär ser intervjupersoner positiva aspekter och stora vinster med att använda SDK. I fallstudien framgår att kommuner, regioner och myndigheter har liknande behov men olika förutsättningar att ansluta till SDK. De olika förutsättningarna beror bland annat på resurser och kompetens inom digital- och juridisk kompetens, men även IT-kompetens.

Information som kommunerna avser att utbyta via SDK är främst sekretessbelagda uppgifter samt känsliga personuppgifter. I stort sett alla kommuner i fallstudien planerar att använda SDK för överföring av information som rör socialtjänsten. Ytterligare aktuella verksamhetsområden för informationsutbyte är arbetsmarknadsenheterna, hälso- och sjukvård samt vård och omsorg. Även skolan ses som ett område där SDK kan bidra till säkert informationsutbyte av känslig information om elever. Några kommuner ser även att de kan använda SDK för att överföra eller utbyta mindre känsliga uppgifter, till exempel ansökningar om bygglov.

I fallstudien framgår att regionerna avser att använda SDK för överföring av främst individinformation. Regionerna har behov av att utbyta information inom den egna regionen, med andra regioner samt med kommuner och myndigheter. Uppgifter som planeras att utbytas är till exempel patientuppgifter inom hälso- och sjukvården, elevuppgifter inom elevhälsa och psykiatri samt sekretessbelagda uppgifter inom socialtjänsten och polisen.

Myndigheterna i fallstudien avser att använda SDK för stora delar av myndigheternas kärnverksamheter, exempelvis kundservice, ärendehantering och folkbokföring.[5]

2.3 Samhällsekonomisk kostnadsanalys för SDK

Utöver fallstudien genomförde DIGG under 2021 även en samhällsekonomisk kostnadsanalys för SDK där sju användningsfall analyserades avseende kostnadsbesparingar som SDK kan skapa för samhället i stort. Inom ramen för kostnadsanalysen framhävs utöver kostnadsbesparingar olika nyttor som SDK medför.

De sju användningsfallen valdes ut för att belysa processer som antingen är komplexa med många inblandande deltagare i kommunikationen och/eller omfattande i antalet informationsutbyten. Utbytet av information sker i dagsläget med hjälp av olika digitala och analoga lösningar, som istället skulle kunna ske genom SDK. Användningsfallen är följande:

1. Extratjänst för arbetssökande – utbyte mellan Arbetsförmedlingen och kommuner.
2. Beslut om ersättning – utbyte mellan Arbetsförmedlingen och Försäkringskassan.
3. Inkomna samtal till Arbetsförmedlingens kundtjänst.
4. Orosanmälningar enligt SoL-14 – anmälan till socialtjänsten.
5. Omhändertagande av unga (LVU) – utbyte mellan polis och andra aktörer.
6. BUP:s kontakt med elevhälsan.
7. Informationsutbyte mellan vård- och omsorgsenheten på kommunen och vården på regionen.

I analysen framgår att de kostnadsbesparingar som SDK kan skapa är såväl kvantifierbara som icke-kvantifierbara.

De kvantifierbara nyttor eller kostnadsbesparingar som identifierats i rapporten är primärt i form av eliminering av ineffektiv arbetstid. För de sju användningsfallen skulle kostnadsbesparingarna eller nyttan kunna bli omkring 1 620 mnkr per år eller cirka 3 500 årsarbetskrafter. Av dessa utgör användningsfall 7,

[5] [5] Uppdrag att genomföra en analys om förutsättningar för kommuners och regioners deltagande i den förvaltningsgemensamma digitala infrastrukturen, I2020/02241, I2021/00941, Löpande rapportering, Dnr 2020–1439

(informationsutbyte mellan vård- och omsorgsenheten på kommunen och vården på regionen) den absolut största delen på mellan 1,259 och 1,578 mnkr per år. Utöver dessa finns många andra processer som skulle kunna nyttja SDK, både inom eller mellan offentliga sektor och offentligt finansierad privat verksamhet.

De icke-kvantifierbara (kvalitativa) nyttorna som nämns i rapporten är bland annat ökad säkerhet i informationsutbytet och minskade ledtider som både gynnar medarbetare och kunder/klienter. SDK skulle även kunna bidra till att skapa denna form av nyttor, vilka inte borde vara försumbara för den totala nyttan även om de är svåra att estimera värdet av dessa.[6]

3 Nulägesbeskrivning av SDK

I det följande framgår en översiktlig beskrivning av den infrastruktur för säker digital kommunikation som är etablerad inom ramen för utvecklingsprojektet SDK i samverkan mellan SKR, Inera och DIGG. Beskrivningen avser nuläget när ansvaret för infrastrukturen är delat mellan SKR och DIGG.

3.1 Vad är SDK

SDK är en infrastruktur där olika aktörer samverkar och ansvarar för olika delar. Infrastrukturen är byggd för att möjliggöra att skicka information mellan olika system, mellan olika typer av verksamheter, och ska kunna hantera en stor mängd anslutna deltagare. Till denna infrastruktur kan deltagare (det vill säga kommuner, regioner och statliga myndigheter) ansluta sina egna system. På det sättet kan organisationerna utbyta information fast de har olika lokala system för meddelandehantering. SDK möjliggör säker överföring av meddelanden inklusive eventuella bilagor (PDF).

3.2 Infrastrukturens olika delar

3.2.1 Plattform

Infrastrukturen bygger i grunden på en plattform för transport av information, vilken möjliggör för olika aktörer att utbyta information inom ramen för SDK-federationen (avsnitt 3.2.2). Plattformen är en nationell anpassning av EU-

[6] Samhällsekonomisk kostnadsnyttoanalys Säker Digital Kommunikation (SDK) Dnr 2020-1439

byggblocket eDelivery[7]. Plattformen definierar gemensamma regler för samverkan och förvaltas av DIGG som är plattformsansvarig. Plattformen består av följande:

- ramverk med regelverk och specifikationer
- plattformstjänster
    - SMP: Metadatatjänst, eDelivery Service Metadata Publisher
    - SML: Lokaliseringstjänst, eDelivery Service Metadata Locator
    - PKI-tjänst: eDelivery PKI-tjänst för accesspunkter
    - CertifikatsPubliceringstjänst: Certifikatspubliceringstjänst som används för att publicera publika nycklar för organisation-till-organisation kryptering och signering av meddelanden mellan deltagare.

3.2.2 SDK-federationen

Till plattformen är SDK-federationen ansluten. En federation är ”en organiserad sammanslutning av självständiga och kända aktörer som samverkar och på säkra och tillitsfulla sätt utbyter data och meddelanden enligt ett visst syfte med hjälp av federationens transportinfrastruktur och dess miljöer inom ramen för plattformen och dess ramverk”.[8]

För SDK-federation ansvarar Inera som federationsägare. SDK-federationen består av följande:

- Ramverk med regelverk och specifikationer.
- Federationsdeklaration som specificerar hur SDK-federationen följer och anpassar de regler och specifikationer som ingår i plattformen.
- SDK auktorisationskomponent: Intern stödkomponent som används för behörighetskontroll till SDK adressbok och SDK testklient.
- SDK adressbok: Gemensamt adress- och kodverksregister med information om SDK-anslutna användarorganisationer och funktioner inom dessa.

[7] eDelivery är ett europeiskt byggblock inom CEF som tillhandahåller tekniska specifikationer och standarder, installerbar programvara och kringtjänster för att olika projekt ska kunna skapa nätverk av noder för säkert digitalt informationsutbyte. eDelivery måste implementeras med egna specifikation för att det ska fungera praktiskt, detta har gjorts för SDK inom DIGGs eDelivery-projekt.

[8] Enligt definitionen i dokumentet Plattform – Ordlista, DIGG, 2022-03-01.

- SDK kodverksapplikation: intern stödkomponent som används för hantering av de kodverk som ska vara tillgängliga i SDK adressbok.
- SDK testbädd: extern testmiljö med bland annat testverktyg för att verifiera förutsättningar att bli godkänd användarorganisation i SDK-federationen.
- SDK Öppen testmiljö, en miljö där leverantörer kan testa och få sina SDK-lösningar för Meddelandetjänst och Meddelandeklient godkända.

3.2.3 Accesspunkter

Deltagarens system ansluts till så kallade accesspunkter. Accesspunkterna följer samma tekniska specifikationer och kan därför kommunicera med varandra. Den som ansvarar för accesspunkten kallas för accesspunktsoperatör och måste genomföra tester och godkännas av DIGG för att kunna delta och agera i plattformen. Både offentliga aktörer och privata tjänsteleverantörer kan bli godkända som accesspunktsoperatörer och tillhandahålla accesspunktslösningar för deltagare, det vill säga lösningar för anslutning till SDK. En deltagare kan även etablera sin egen accesspunkt.

3.2.4 Deltagares tekniska lösning

Deltagare väljer vilken klientlösning/slutanvändarsystem som ska användas inom organisationen, det vill säga det system som handläggare eller andra använder när de ska skriva och skicka meddelanden via SDK. Det är möjligt att integrera SDK i ett existerande handläggningssystem, utveckla eller köpa en egen SDK-klient. Det är deltagaren som ansvarar för meddelandekrypteringen i enlighet med regelverk och specifikationer för SDK.

3.2.5 Adressering i SDK

Adressboken innehåller adressuppgifter för att hitta rätt mottagare på funktionsnivå bland andra anslutna deltagare inom SDK. I adressboken finns uppgifter om deltagaren och funktionsadress. I adressboken ska det inte förekomma personuppgifter eller sekretessklassad information. I adressbokens loggar finns dock information om administratörer av adressboken. Varje deltagare som är ansluten till SDK ansvarar för att lägga in sina funktionsadresser i SDK adressbok. Det pågår arbete med att standardisera hur funktionsadresser ska struktureras med hjälp av kodverk baserat på bland annat verksamhetens geografiska hemvist och verksamhetsområde.

3.3 Anslutning av deltagare

Det anslutningsförfarande som tillämpas beskrivs i SDK-federationsdeklaration vilken ingår som en bilaga i avtalet mellan DIGG och Inera. Vid anslutning av deltagare till SDK-federationen ingår en deltagare ett anslutningsavtal med Inera. Anslutningsavtalet innehåller bland annat villkor för tillträde till och användning av infrastrukturen och innefattar bland annat en självdeklaration som måste fyllas i för att bli godkänd för anslutning.

I dagsläget är en deltagare i SDK-federationen en kommun, region eller en statlig myndighet. Det innebär att alla verksamheter inom en kommun eller en region är anslutna till SDK som en deltagare, exempelvis deltagaren Munkedals kommun eller deltagaren Region Stockholm. Arbete pågår för att även möjliggöra anslutningar av privata aktörer som verkar inom offentligt finansierad verksamhet.

En deltagare väljer lösning för accesspunkt (egenutvecklad eller genom leverantör) och interna informationssystem såsom meddelandetjänst (egenutvecklad eller genom leverantör), samt hur man ska tillgängliggöra SDK till användarna i den egna organisationen (till exempel egen lösning eller integrerat i existerande system). Deltagaren publicerar det certifikat som ska användas för signering och kryptering av meddelanden i meddelandeutbytet med andra deltagare deltagare. Anslutningsmodellen innebär att alla meddelanden som skickas till en funktionsadress använder deltagarens gemensamma certifikat.

Deltagaren ansvarar för att synliggöra och lägga upp de verksamhetsfunktioner som ska använda SDK-federationen som funktionsadresser i adressboken. Det är upp till respektive deltagare att avgöra på vilken nivå funktionsadresser ska användas med stöd av adressbokens kodverk. En funktionsadress kan till exempel vara kopplad till en organisatorisk enhet (ex. socialtjänsten eller ett äldreboende) eller ett specifikt informationsflöde (handläggning sjukpenning). Det går däremot inte att skicka meddelanden till enskilda personer, (avsnitt 3.2.5).

4 Rättslig analys

Sammanfattningsvis föreligger inga rättsliga hinder utifrån det tilltänka upplägget i SDK. DIGG har identifierat vissa juridiska risker som kan uppstå i händelse av att en deltagare bryter mot regelverket i SDK. DIGG ser behov av riskreducerande åtgärder samt vidare arbete för att motverka identifierade juridiska risker och otydligheter. Dessa behöver ske hos DIGG, Inera, deltagare och accesspunktsoperatörer.

DIGG föreslår att en sekretessbrytande bestämmelse gällande teknisk bearbetning och teknisk lagring införs. En sådan bestämmelse skulle underlätta bedömningar inom offentlig sektor beträffande röjande av sekretessuppgifter vid anslutning till SDK.

DIGG anser att myndighetens instruktion behöver ändras så att det framgår att DIGG ansvarar för SDK. I det fortsatta arbetet avser DIGG genomföra en fortsatt analys för att utröna om infrastrukturen lämpligast bör författningsregleras. Analysen kommer bland annat ta sikte på om behov föreligger att utöva kontroller av deltagare och leverantörer gällande regelefterlevnad samt om behov föreligger att författningsreglera hela eller delar av anslutningen till SDK

DIGG avser därutöver att genomföra en analys beträffande anslutningsförfarandet till SDK för att dra slutsatser om i vilken omfattning finansieringsmodellen påverkar konkurrens- och upphandlingssituationen.

4.1 Inledning

SDK aktualiserar en rad juridiska frågeställningar som är nödvändiga att belysa. I denna delrapport sammanfattas DIGGs avvägningar och slutsatser som framgår av den rättsliga analysen, för mer information om juridiska avvägningar och bedömningar beträffande SDK, se bilaga 1.

4.2 Sekretess och dataskydd i förhållande till strukturen i SDK

DIGG har analyserat de rättsliga förutsättningarna för SDK beträffande hanteringen av externa leverantörers behandling av krypterad information. Den juridiska utredningen behandlar kryptering som säkerhetsåtgärd utifrån ett sekretesshänseende och dataskydd för behandlingar inom Sverige. DIGG understryker att den juridiska utredningen som genomförts avseende krypteringar i SDK inte tar sikte på krypteringar som tillräcklig säkerhetsåtgärd, utifrån EDPB:s rekommendationer för tredje landsöverföringar.

Enligt regelverket för SDK-federationen har externa leverantörer av accesspunkter, meddelandetjänster eller meddelandeklienter ingen åtkomst till information annat än i krypterad form. Det är uteslutande deltagarna i SDK-federationen som bestämmer ändamålen för informationshanteringen.

DIGG anser att den hantering som sker hos externa leverantörer är att betrakta som teknisk bearbetning och lagring. Det innebär att det föreligger en straffsanktionerad tystnadsplikt hos samtliga leverantörer i SDK:s informationsflöde. Om deltagaren avser utkontraktera ytterligare tjänster inför anslutning, såsom krypteringshantering, utöver vad som regleras i SDK måste varje enskild deltagare genomföra sin egen rättsliga bedömning.

Enligt DIGGs uppfattning är inte uppgifterna som hanteras av accesspunktsoperatörerna i SDK att betrakta som röjda. Emellertid då bedömningar beträffande när uppgifter anses röjda ankommer varje enskild deltagare föreslår DIGG en sekretessbrytande bestämmelse. Detta i syfte att frångå den potentiella röjandeproblematiken som kan uppstå för deltagarna i samband med utkontraktering inför och i anslutning till SDK. Den sekretessbrytande bestämmelsen som föreslås är densamma som presenterades i IT-driftsutredningen[9].

DIGG behandlar personuppgifter idag som plattformsansvarig inom SDK. Även framgent avser DIGG behandla personuppgifter inom ramen för det övergripande ansvaret för SDK-infrastrukturen. I en övergripande beskrivning behandlar DIGG enbart personuppgifter som är nödvändiga för att administrera och tillgängliggöra infrastrukturen för deltagarna och för dessa behandlingar är DIGG personuppgiftsansvarig. Deltagarna ansvarar själva för den information som transporteras i SDK och bestämmer självständigt ändamålen med personuppgiftsbehandlingen. Det är med andra ord deltagarna som är personuppgiftsansvariga för den information som skickas och tas emot inom SDK.

Personuppgiftsansvaret övergår i samband med att informationen når respektive deltagares accesspunkt. Beroende på om en deltagare utkontrakterar accesspunktstjänster eller inte kan ett personuppgiftsbiträdesförhållande uppstå mellan deltagaren och accesspunktsoperatören. Detsamma gäller vid

[9] Delbetänkandet SOU 2021:1 och slutbetänkandet 2021:97.

utkontraktering av meddelandetjänst och meddelandeklient. Deltagare behöver vid utkontraktering genomföra en egen bedömning huruvida ett personuppgiftsbiträdesförhållande mellan deltagaren och dennes leverantör uppstår eller inte.

4.3 Funktionsadresser i adressboken

Målsättningen med SDK är att ansluta statliga myndigheter, kommuner och regioner samt privata aktörer som offentlig sektor har ett behov att kommunicera med. Deltagarna ansluter på organisationsnivå. Det yttersta ansvaret att upprätta en intern struktur av mottagare inom SDK, som säkerställer sekretess och dataskyddsbestämmelserna, tillfaller den anslutande deltagaren.

Idag finns flera kodverk implementerade i SDK Adressbok samt fler är under pågående utveckling. Kodverken syftar till att underlätta för andra organisationer att hitta rätt mottagare i en organisation, genom att stödja strukturerad sökning av funktionsadresser. . En funktionsadress kan tilldelas en eller flera koder i ett kodverk för att möjliggöra exakta sökningar. Genom att tilldela en funktionsadress koder från ett av adressbokens kodverk möjliggörs för andra deltagare att söka fram funktionsadressen genom filtrering utifrån koder i kodverket. Den som söker behöver således inte känna till det exakta namnet på funktionsadressen som sökes, utan kan söka fram funktionen utifrån exempelvis ett verksamhetsområde via en kod i ett kodverk.

I händelse av att en deltagare felaktigt implementerar funktionsadresser i adressboken i SDK och därigenom frångår kodverket kan konsekvensen bli att informationsflödet når en, utifrån sekretess och dataskydd, otillåtet bred krets mottagare. Det kan jämföras med ungefär samma slags risk som föreligger idag beträffande felaktig hantering av fax, brev och epost.

För att säkerställa de allmänna principerna i dataskyddsförordningen är det viktigt att samtliga deltagare säkerställer en korrekt implementering av funktionsadresserna i adressboken för att på så vis kontrollera vem som har rätt att se vilken information. Vid en felaktig implementering av funktionsadresser i adressboken uppstår utöver en sekretessproblematik även risker i förhållande till dataskyddsförordningen. En allt för bred krets av mottagare hos en myndighet torde medföra problem utifrån de allmänna principerna i dataskyddsförordningen. Risken för en felaktig sekretesshantering kan bli större hos kommuner eftersom de omfattar mer än en myndighet, som till sin natur omfattas av olika

sekretessregleringar, och anslutningen till SDK sker på organisationsnivå, det vill säga den juridiska personen och inte myndigheten.

4.4 Anslutningsförfarande

Oaktat om en felaktig implementering av funktionsadresserna i adressboken föreligger eller inte finns det en viss risk med att krypteringsnyckeln administreras på organisationsnivå om informationen omfattas av sekretessbestämmelser på verksamhetsnivå. En korrekt behörighetshantering hos den administrativa funktionen som har åtkomst till krypteringsnycklarna torde inte medföra några omfattande juridiska problem. Nuvarande upplägg förutsätter en tillfredställande informationssäkerhet hos deltagarna inom SDK. Omvänt kan en bristfällig informationssäkerhet där krypteringsnycklarna hanteras felaktigt medföra att sekretessuppgifter riskeras röjas. För en sådan situation aktualiseras även frågan om en tillräcklig teknisk- och organisatorisk säkerhetsnivå i förhållande till kraven i dataskyddsförordningen.

En möjlig vidareutveckling för att minimera risken att krypteringsnyckeln hanteras klandervärt är att förändra så att anslutning kan ske på verksamhetsnivå i stället för organisationsnivå, vilket frångår tillämpningen om att varje deltagare fritt förfogar över att upprätta egna interna mottagare i SDK. En sådan omfattande förändring behöver föregås av en helhetsanalys då åtgärden påverkar arkitekturen, ansvarsförhållanden och kostnaderna i SDK.

För en deltagare som inte själv avser drifta nödvändiga funktioner för anslutning till SDK uppstår frågan om utkontraktering av accesspunkter, meddelandetjänster och meddelandeklienter. Idag kontrolleras accesspunktsoperatörerna genom ett summariskt förfarande. För hantering av sekretessbelagd information och känsliga personuppgifter uppställer SDK krav på kryptering av all information och gentemot samtliga funktioner i infrastrukturen. Krypteringarna appliceras dels gentemot utomstående, dels i förhållande till accesspunkterna. Samma krav gäller för samtliga funktioner inom SDK.

Ytterst tillfaller ansvaret för informationshanteringen i meddelandetjänsten varje enskild deltagare. Detsamma gäller för hantering av krypteringsnycklar i meddelandetjänsten. En bristfällig utkontraktering av funktionerna i SDK riskerar medföra att sekretessuppgifter röjs på ett otillåtet sätt och att kraven om tillräcklig teknisk och organisatorisk säkerhet i dataskyddsförordningen inte efterlevs. En åtgärd för att minimera risker som kan uppstå i samband med att en deltagare

utkontrakterar delar av SDK skulle kunna vara en utökad kontrollfunktion beträffande anslutande deltagares accesspunkter, meddelandetjänster och meddelandeklienter. Det behöver dock utredas om en sådan kontrollfunktion kan fungera rent praktiskt. Resurser och kostnader för en sådan utredning har inte tagits höjd för i DIGGs arbete med SDK idag.

4.5 Avtalsmodell

Nuvarande avtalsmodell inom plattformen och SDK-federationen utgår från ett anslutningsförfarande där deltagrana ingår avtal med federationsägare. Via avtalet förbinds deltagarna till bland annat regelverk och tekniska specifikationer. DIGG föreslår att genomföra en översyn om skyldigheten att tillhandahålla SDK ska framgå av författning och att DIGG i sådant fall erhåller föreskriftsrätt på området. DIGG gör bedömningen att en stor del av det nu civilrättsliga förfarandet kan ersättas med föreskrifter. Om en författning med föreskriftsrätt meddelas krävs en förnyad analys för att utröna vad i nuvarande avtalsmodell som kan ersättas med föreskrifter. Vissa avtal såsom personuppgiftsbiträdesavtal och eventuellt säkerhetsskyddsavtal bedöms fortfarande behöva ingås i tillämpliga fall. I det fortsatta arbetet med att ta över ansvaret för SDK kommer DIGG behöva se över avtalsmodellen, avseende de kunskaper som uppkommer under vägen, rörande bland annat rättsliga åtgärder och säkerhetsåtgärder.

En mer fördjupad analys behöver genomföras gällande privata aktörer för att utreda om det är juridiskt nödvändigt med ett avtalsförfarande beträffande deras anslutning till SDK om det finns en förordning.

4.6 Konkurrens

SDK är avsedd att nyttjas inom all offentlig sektor samt mellan offentlig sektor och privat sektor där det finns behov. När offentlig sektor tillhandahåller varor och tjänster så behöver bestämmelserna om konkurrensbegränsande offentlig säljverksamhet beaktas (KOS-reglerna).

DIGG har gjort bedömningen att SDK i konkurrensrättslig mening bör ses som en offentlig säljverksamhet som i sig kan omfattas av KOS-reglerna. Denna bedömning är densamma oavsett vilken finansieringsmodell som SDK tillämpar, eftersom verksamheter som är anslagsfinansierade eller som erbjuder tjänsten utan kostnad kan omfattas av KOS-reglerna. Vidare gör DIGG bedömningen att SDK sannolikt kommer att betraktas som försvarbar utifrån allmän synpunkt i ett konkurrenshänseende och därmed inte träffas av förbud enligt KOS-reglerna om

det framgår tydligt via författning att DIGG ska tillhandahålla SDK. DIGG planerar en fortsatt utredning gällande konkurrensaspekterna för SDK efter att en behovsanalys har genomförts beträffande vilka privata aktörer som avser ansluta och i vilken omfattning privata aktörer de facto kommer att ansluta till SDK.

Utöver konkurrensaspekter beträffande SDK uppstår sannolikt liknande frågor i den situationen en offentlig aktör avser tillhandahålla accesspunkter för andra deltagare. Vid en sådan situation inom kommunal sektor kan även frågor om den kommunala kompetensen aktualiseras.

4.7 Upphandling

Den upphandlingsrättsliga analysen har fokuserat på att belysa de relationer som kan komma att uppstå mellan olika aktörer ur ett upphandlingsrättsligt perspektiv med tyngdpunkten vid deltagarnas anslutning till SDK, anskaffning av eventuella tredjepartstjänster och eventuella underleverantörer.

Sammanfattningsvis har de upphandlingsrättsliga bedömningar utmynnat i att en kommun eller en regions anslutning till SDK kan vara upphandlingspliktig, beroende på finansieringsmodell. Statliga myndigheters anslutning är sannolikt inte upphandlingspliktig, oberoende av finansieringsmodell. Detsamma gäller för en offentlig accesspunktsoperatör eller tredjepartsleverantör vid anslutning till SDK. Däremot är själva köpet av accesspunkt eller andra tredjepartstjänster från en privat leverantör sannolikt upphandlingspliktigt (för mer information om bedömningen se Bilaga 1. Rättslig analys).

4.8 Tillgången till juridisk kompetens

Ett av syftena med SDK:s regelverk är att säkerställa en korrekt implementering av funktionsadresserna i adressboken. Precis som vid all utkontraktering ankommer det på deltagaren att beakta och säkerställa sekretessbestämmelserna och bestämmelserna i dataskyddsförordningen, dels vid upprättande av adressbok, dels vid utkontraktering inför anslutning till SDK. Deltagaren måste därutöver genomföra bedömningar om huruvida upphandling är nödvändig och om personuppgiftsbiträdesförhållande föreligger. Det är särskilt viktigt att deltagarna genomför juridiska bedömningar vid införskaffande av meddelandetjänster och meddelandeklienter, då handlingsutrymmet för enskilda deltagare att införskaffa bristfälliga lösningar får anses som mer omfattande än i jämförelse med införskaffande av accesspunkter. I fallstudien, som beskrivs i avsnitt 2.2, framgår det bland annat att mindre kommuner är medvetna om att lagar och förordningar

ska följas men att majoriteten av dem ännu inte diskuterat rättsliga aspekter som rör SDK. Det framgår vidare att den allmänna tillgången till juridiskt stöd varierar mellan kommunerna och där juridiskt stöd finns att tillgå saknas i förekommande fall jurister med kompetens inom IT-rättsområdet. Inom statliga myndigheter och regioner finns juridisk kompetens att tillgå i större omfattning. Samma lägesbild bekräftades genom intervjuer vid införandet av myndighetens rättsliga stöd till förvaltningsgemensamma digitala infrastrukturen.[10]

En metod att riskminimera är att minska handlingsutrymmet för anslutande deltagare genom utökade regleringar i SDK. DIGG kan ge vägledning i juridiska frågor för att underlätta för deltagarna och det kan möjliggöras om finansiering för stöd till anslutning ges.

5 Risk- och säkerhetsanalys

DIGG avser genomföra en säkerhetsskyddsanalys för att utreda om plattformen träffas av säkerhetsskyddslagstiftning (SFS 2018:585). Detta kommer genomföras i ljus av det säkerhetspolitiska läget och ny beredskapslagstiftning.

DIGG kommer vidareutveckla plattformen och SDK-federationen och härda transportinfrastrukturen kring säkerhet och tillit enligt uppdrag. Handlingsplaner håller på att tas fram för att åtgärda identifierade utmaningar och risker ur ett långsiktigt perspektiv. Vidareutveckling kommer ske i samverkan med SKR, Inera och MSB.

DIGG anser att fortsatt arbete behöver genomföras beträffande anslutningsförfarandet till SDK-federationen för deltagare.

5.1 Inledning

SDK ska användas för att kunna kommunicera säkert vilket innebär att löpande arbete med riskhantering och informationssäkerhet är centralt för samtliga aktörer som ingår i infrastrukturen.

[10] 2021-01-21, I2021/00288, Dnr 2021-164

Under utvecklingsarbetet med SDK har det bedrivits löpande arbete gällande säkerhet och informationssäkerhet. Säkerhetsarbetet har bedrivits i samverkan med myndigheter, regioner och kommuner som deltagit i pilotprojekten. Det har genomförts säkerhetsanalyser, informationssäkerhetsklassningar, tekniska säkerhetstester samt säkerhetsbedömningar som omhändertagits i infrastrukturen och nuvarande regelverk och specifikationerna för SDK-federationen och plattformen.

SDK är baserad på egenskaper och funktioner med fokus på *rätt säkerhet* och *systemisk tillit* för att skapa trygghet och förtroende hos alla inblandade aktörer.

Rätt säkerhet innebär att aktörers rättsliga förutsättningar, verksamhetsbehov och krav på digital samverkan kan hanteras inom SDK-federationens och plattformens juridiska, organisatoriska, finansiella och tekniska säkerhetsåtgärder.

Systemisk tillit bygger på att infrastrukturens samtliga anslutna aktörer, deltagare och accesspunktsoperatörer, tillsammans med plattformsansvarig och federationsägare har bevisade förmågor att tillsammans via systematiskt informationssäkerhetsarbete ge förutsättningar för säker, trygg och effektiv digital samverkan för alla inblandade.

5.2 Regelverk och specifikationer för SDK

Regelverk och specifikationer syftar till att etablera gemensamma säkerhetskrav för hantering av uppgifter klassade upp till (och innefattande) konsekvensnivån allvarlig enligt MSB:s modell för klassificering av information.

5.2.1 Regelverk och specifikationer för plattformen

Regelverket och specifikationer (ramverket) för plattformen är uppbyggda för att i framtiden kunna hantera flera federationer och innehåller åtgärder för att möta deltagarnas behov av rätt säkerhet och tillit. Detta innebär att:

- Krav ställs på deltagande aktörer att dokumentera digital samverkan med behov av krav på säkerhetsåtgärder, informationssäkerhetsklassificera meddelanden för att kunna utvärdera om kraven tillfredsställs av en federations utbud av tillit, säkerhet och funktion.
- Krav ställs på samtliga aktörer i plattformen och SDK-federationen att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete motsvarande ISO27000-serien.

- Plattformen för SDK-federationen inkluderar såväl TLS kommunikationskryptering mellan accesspunktsoperatörer som meddelandekryptering av information mellan deltagare.
- Tekniska lösningar för kryptering och signering av meddelanden och information sker genom certifikatlösningar, baserat på digitala privata och publika nycklar – PKI.
- Granskning inför godkännande av accesspunktsoperatörer sker genom angivna kriterier, verifieringar, samt tester enligt definierad anslutningsprocess och avtal.
- Programvaror och tekniska miljöer är separerade inom plattformen och SDK-federationen.
- Tekniska miljöer har genomgått externa säkerhetstester/ penetrationstester innan produktionssättning hos Försäkringskassan och Inera.

Plattformen vidareutvecklas löpande och det pågår aktiviteter inom följande områden:

- Vidareutveckling av ramverket med tillhörande regler och rutiner för informationssäkerhet pågår för att öka tydlighet kring systemisk tillit och säkerhet för plattformen.
- Programvaror vidareutvecklas av DIGG för plattformstjänsterna SMP och Certpub för publicering av certifikat för deltagare samt administration av anslutna accesspunktsoperatörer.
- Etablera rutiner för felhantering, support och incidenthantering med kontaktvägar för samtliga inblandade aktörer.

5.2.2 Regelverk och specifikationer för SDK-federationen

Regelverket för SDK-federationen har utvecklats av Inera och förvaltas i enlighet med Ineras interna regelverk, anvisningar och rutiner för IT-verksamhet. Regelverket omfattar bland annat:

- SDK-federationsdeklaration där det redogörs för hur SDK-federationen uppfyller gällande krav och förutsättningar för att skapa rätt säkerhet och systemisk tillit för deltagare.
- Krav på certifikatutfärdare och identifieringsnivåer för deltagare.

- Användning av mTLS samt SITHS-certifikat för att öka skalskyddet och minska risken för hot och sårbarhet kopplat till cybersäkerhet som utgör anpassningar av plattformens ramverk.
- Rutiner för felhantering, support, incidenthantering och kontaktvägar för deltagare samt driftspartner

SDK-federationen vidareutvecklas löpande av Inera och det pågår aktiviteter inom många områden i samverkan med DIGG och andra aktörer, exempelvis:

- Vidareutveckling av regelverket för informationssäkerhet för att stärka systemisk tillit och rätt säkerhet inom SDK-federationen.

5.3 Extern risk och säkerhetsanalys

DIGG har under sommaren 2022 gett i uppdrag till en externa IT-revisorer att genomföra en övergripande riskanalys och säkerhetsbedömning av informationssäkerhetsrisker samt IT-säkerhetsrisker. Analysen har utgått från gällande lagar och förordningar.

IT-revisorerna har analyserat DIGGs kommande uppdrag som ansvarig för hela SDK infrastrukturen (plattformen och SDK-federationen) och förutsättningarna för detta ansvar utifrån den kunskap som finns nu. Arbetet har skett genom informationssamling relaterad till IT-miljön, parter och ansvar, policy, rutiner, applikationer, avtal, funktionella och icke funktionella krav. Information har insamlats via intervjuer av berörda parter och nyckelpersoner hos DIGG och Inera. Metodiken har baserats på RISK-IT och ISO27005 kompletterade med accepterad IT och informationssäkerhetsstandarder såsom COBIT, ITIL, NIST, CIS, ISO27000-serien.

Resultatet från analysen är identifierade risker med ett antal åtgärder som behöver hanteras inom pågående arbete hos DIGG och Inera, samt i arbetet med ansvarsförflyttningen av SDK-federationen från Inera till DIGG.[11]

5.1 Samråd med MSB

DIGG har i enlighet med uppdraget initierat ett samråd med Myndigheten för samhällsskydd och beredskap (MSB) gällande infrastrukturens utformning. Det finns fortfarande när rapporten lämnas in ett behov av att fördjupa samrådet. MSB

[11] IT- och informationssäkerhets riskanalys, Dnr 2021-2909

önskar tillgång till ytterligare dokumentation för att kunna bedöma de samrådsfrågor som DIGG behöver svar på, bland annat en helhetsbild av hur den tekniska infrastrukturen är uppbyggd, säkerhetsåtgärder, samt hur tillgängligheten för tjänsten upprätthålls. DIGG avser föra en fortsatt dialog kring detta i syfte att säkerställa att SDK-infrastrukturen uppfyller de krav som MSB ser som avgörande.

5.2 Risker, hantering och åtgärder

Genom samrådet med MSB och resultatet av den externa risk- och säkerhetsanalysen har DIGG fått fördjupade insikter och underlag för hantering av utmaningar och risker. Ytterligare arbete behöver ske för att fördjupa förståelsen av vilka åtgärder som vi ska genomföra samt i vilken prioritetsordning.

Grundläggande är ett systematiskt riskhanterings- och informationssäkerhetsarbete för SDK kommer behöva ske framgent i nära samarbete med de aktörer som medverkar i infrastrukturen. Det är viktigt att varje aktör tar sitt eget ansvar för det men även att hitta former för gemensamma stöd och funktioner.

SDK måste dimensioneras för att möta framtidens anslutningstakt och krav på säkerhet och tillit, samt kunna hantera omfattande störningar i samhället och behov av redundans.

DIGG behöver löpande analysera SDK utifrån uppdraget som beredskapsmyndighet gällande cybersäkerhet och totalförsvar. DIGG ser behov av att genomföra en säkerhetsskyddsanalys för att utreda om plattformen träffas av säkerhetsskyddslagstiftning (SFS 2018:585).

DIGGs bedömning av risk- och säkerhetsanalysen är att prioritera åtgärder rörande de risker som kan påverka den nuvarande driften av plattformen som är under DIGGs ansvar. En åtgärdsplan är framtagen och beslutad. Detta handlar om att förtydliga krav på accesspunktoperatörer i form av regler och rutiner i samband med godkännandeprocessen vid anslutning, även uppföljning och efterlevnad förtydligas inför förvaltning.

Vidare har DIGG informerat Inera om de risker som identifierats som påverkar SDK-federationens delar som Inera ansvarar för. DIGG och Inera planerar att synkronisera åtgärder när så är nödvändigt. Den risk som analyseras först är nya och utökade krav och behov av tydligare krav på certifikatshantering. Inera vidtar

åtgärder genom att bland annat förtydliga krav på certifikatshantering i SDKs regelverk.

Vidare är dagens anslutningsmodell, där deltagare ansluts på kommun- och regionnivå är identifierad som en möjlig risk då det innebär att alla underliggande anslutna organisation använder deltagarens gemensamma certifikat för kryptering. Detta kan innebära bland annat en risk för röjande av sekretessuppgifter. Detta är en risk som behöver analyseras av DIGG, Inera och deltagande aktörer.

Det finns identifierade risker som är kopplade till DIGGs nuvarande organisation för utveckling och tjänsteförvaltning som ger råd kring viktiga områden som DIGG behöver förstärka och förbättra inför övertagandet av ansvar för hela SDK-infrastrukturen. Dessa risker är sedan tidigare kända och identifierade som förbättringsområden på DIGG och planeras åtgärdas inom ramen för det pågående arbetet med övertagandet av ansvaret samt i förvaltningen av plattformen.

Identifierade risker och behov av förändringar från dagens hantering kan innebära ökade kostnader för drift och förvaltning av infrastrukturen samt ökade krav på deltagare och accesspunktsoperatörer.

6 SDK i relation till annan infrastruktur och uppdrag

6.1 Ena – Sveriges digitala infrastruktur

SDK-infrastrukturen ska utgå från och komplettera det arbete som bedrivs med att etablera den förvaltningsgemensamma digitala infrastrukturen, vilken har fått namnet Ena-Sveriges digitala infrastruktur.[12] Tanken bakom Ena är att istället för att varje offentlig aktör ska utveckla sina egna lösningar, på sitt eget sätt, vinner alla på att det finns en sammanhållen infrastruktur som kan användas och återanvändas för att lösa förvaltningsgemensamma grundläggande behov. Syftet med att se på hur SDK kan utgöra en del av Ena är att både möjliggöra för effektivt utnyttjande av de kompetensområden, ramverk och processer med mera som är uppbyggd inom Ena, samt möjliggöra

[12] (I2019/03306, I2020/03366 och I2020/02753)

för att den utveckling som är gjort inom SDK på sikt kan återanvändas helt eller delvis för nya användningsområden.

Följande beskrivning är en första nulägesanalys av och exempel på hur SDK kan integreras i Ena, men utgör inte ett konkret förslag för framtiden. DIGG avser tillsammans med relevanta aktörer arbeta vidare ytterligare under 2022 och 2023 innan förslag och beslut om till exempel nya byggblock kan fattas.

6.1.1 Nulägesanalys av SDK som en del av Ena

Genom analyser av SDK-infrastrukturen är bedömningen att vissa delar lämpar sig väl för att passa in i den byggblocksbaserade struktur som Ena består av. Idag tillhör federationer en tillämpning som använder Ena och är inte någon av de kategorier som Ena tillgängliggör.

DIGG bedömer utifrån analysen att det kan skapas idékandidater för ett nytt byggblock samt ske vidareutveckling av befintliga inom Ena genom SDK:s utveckling. En idé om byggblock kan vara att hantera den transportinfrastruktur för eDelivery såsom Transportprofil, Kuverteringsprofil, Transportmodell och tillhörande testbädd kan placeras. DIGG ser idag inte att Ena ska hantera meddelandemodeller då detta är specifika delar som respektive användare av transportinfrastrukturen bör ansvara för inom respektive federation. På detta sätt blir transportinfrastrukturen förvaltningsgemensam medan tillämpningarna hanterar federationsspecifika specifikationer. Den adresseringstjänst (SMP) som hanterar adressering av accesspunkter kan eventuellt placeras inom byggblock Adressregister, och att PKI-hantering och Certifikatspubliceringen som är starkt kopplade till identifiering av aktörer kan eventuellt placeras inom byggblocket Identitet. Adressboken inom SDK-federationen kan placeras inom byggblocket Adressregister som är tänkt att hantera denna typ av information. Till adressboken så ingår också en testbädd som möjliggör tester gentemot denna för anslutna aktörer.

6.2 SDK i förhållande till andra infrastrukturer för säker kommunikation

Samverkan med andra infrastrukturer styrs av vilka krav på tillit och säkerhet som ställs på den digitala samverkan mellan berörda verksamheter. Konstruktionen och konfigurationen av nu gällande regelverk för plattformen har utgått från SDK-federationens säkerhetsbehov och grundläggande användningsfall men regelverk och ramverk i plattformen och SDK-federationen erbjuder möjligheter

för framtida samverkan med andra infrastrukturer inom Sverige för säker kommunikation. Plattformen bygger på EU-byggblocket eDelivery vilket ger grundförutsättningar för att samverka med andra infrastrukturer inom Sverige och EU som också bygger på eDelivery.

SGSI (Swedish Government Secure Intranet) är ett intranät, skiljt från internet, för säker och krypterad kommunikation mellan myndigheter i Sverige och i Europa. Samverkan med MSB pågår för att analysera hur SDK-infrastrukturen relaterar till SGSI.

Rakel är ett digitalt radiokommunikationssystem för trygg och säker kommunikation mellan medarbetare inom samhällsviktig verksamhet. Samverkan med MSB pågår för att analysera hur SDK-infrastrukturen relaterar till Rakel.

7 Finansieringsförslag

DIGG föreslår att drift och förvaltning av SDK ska finansieras genom ett förstärkt förvaltningsanslag till DIGG. Dagens finansiering sker via ett årligt regeringsbeslut från anslagspost 2:7 ap.3, vilket DIGG föreslår istället ska ligga permanent på DIGGs förvaltningsanslag (2:6 ap.1).

7.1 Tidigare förslag kring finansiering av förvaltningsgemensam digital infrastruktur

Inom ramen för regeringsuppdragen, *Uppdrag att etablera en förvaltningsgemensam digital infrastruktur* och *Uppdrag att etablera ett nationellt ramverk för grunddata inom den offentliga förvaltningen* har förslag lämnats kring finansiering. I rapporten gör de ingående myndigheterna i uppdraget ställningstagandet att Ena bör finansieras genom anslag. Bedömning från regeringsuppdraget, vilken DIGG delar, är att anslagsfinansiering skapar bättre förutsättningar för att hantera förvaltningsgemensamma digitala tjänster på ett långsiktigt och stabilt sätt, vilket i sin tur ökar även möjligheterna och incitamenten för att dessa tjänster ska användas på ett sådant sätt som är avsett. Samtidigt görs bedömningen att avgifter i många fall motverkar anslutning till och användning av den förvaltningsgemensamma infrastrukturen. En avgiftsmodell bör införas först när en tjänst är mogen. Med mogen menas att tjänsten är etablerad och används, den

har uppnått sin potential i form av funktionalitet för att skapa nytta och att en stor mängd användare har anslutits sig.[13]

I rapporten *Styrning och finansiering av förvaltningsgemensam digital infrastruktur* skriver Ekonomistyrningsverket (ESV) att anslag är huvudregeln för att finansiera statlig verksamhet och bör därför alltid övervägas som ett förstahandsalternativ. Anslagsfinansiering kan ge bättre möjligheter för att hantera förvaltningsgemensamma digitala tjänster på ett långsiktigt, stabilt och förutsägbart sätt. Det skulle innebära ökade möjligheter och incitament för att förvaltningsgemensamma tjänster ska används så som är avsett. ESV skriver vidare i samma rapport att riksdagens och regeringens möjligheter till styrning ökas med anslagsfinansiering, då de kan bestämma ambitionsnivån för olika investeringar och verksamheter. Enligt ESV finns det situationer där anslagsfinansiering är mest lämplig. Ett exempel är att när det kan vara svårt att identifiera den målgrupp som ska betala för tjänsten eller när det är tydligt att ett avgiftsuttag skulle få icke önskvärd eller en hämmande effekt på anslutning och användning. DIGGs bedömning är att en avgift ger en hämmande effekt på anslutning till SDK. [14]

7.2 Finansieringsmodeller för SDK

Finansiering av SDK har beröringspunkter med finansieringen av Ena. Analysen har utgått från de ställningstaganden som gjorts inom de regeringsuppdrag som föregått Ena. SDK är en tjänst som är under etablering. Det är därför svårt att förutspå hur många aktörer som kommer att ansluta sig som deltagare och i vilken takt anslutningen kommer att ske. I detta tidiga stadium finns, genom Ineras arbete, tillräcklig kännedom om kommuner, regioner och statliga myndigheter, storlek, behov och förutsättningar. DIGG ska enligt uppdrag även ansluta privata utförare. Det fortsatta arbetet behöver skapa kunskap om dessa deltagares behov och förutsättningar. Det behövs även en anslutningsmodell som är anpassad för både offentliga och privata deltagare. En sådan anslutningsmodell finns inte på

[13] Bolagsverket, DIGG, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, MSB, Riksarkivet, Skatteverket, Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte samt Uppdrag att etablera ett nationellt ramverk för grunddata inom den offentliga förvaltningen – slutrapport 2021-12-01, Sundsvall, 2021,

[14] Ekonomistyrningsverket, Rapport Styrning och finansiering av förvaltningsgemensam digital infrastruktur, ESV 2020:23, Stockholm, 2020

plats idag. Det finns inte heller någon prognos för hur många deltagare som kommer att ansluta sig eller i vilken takt anslutningen kommer att ske. Bedömningen är att en avgiftsmodell där kostnaderna fördelas på få anslutna deltagare, i detta tidiga skede, leder till höga avgifter per deltagare, vilket är hämmande för anslutningen. För att nå en hög anslutningsgrad och etablera SDK som en självklar tjänst att använda, är det endast anslag som kan ge en stabil och förutsägbar finansiering.

Den juridiska bedömningen av KOS-regler (avsnitt 4.6) och upphandling (avsnitt 4.7) är att anslagsfinansiering kan verka främjande för anslutning till SDK. Avgiftsfinansiering skulle troligen leda till en bedömning att anslutningen till SDK är upphandlingspliktig, för kommuner och regioner. En upphandlingsplikt bedöms motverka ett brett införande och en hög anslutningsgrad till SDK.

Anslagsfinansiering kan omvärderas när tjänsten uppfattas som mogen vad gäller funktionalitet, nytta och tillräckligt antal användare.

Denna senare analys kan utgå från den metod som använts i rapporten *Modeller för fördelning av nyttor och kostnader för digital infrastruktur – exemplet verksamt.se*. Statskontoret bedömer att modellen passar bättre vid framtagandet av nya tjänster än för befintliga tjänster. DIGG bedömer dock att denna modell kan vara vägledande vid en omvärdering av finansieringsmodell för drift och förvaltning av SDK. [15]

7.2.1 Finansiering av SDK drift och förvaltning via anslag

SDK behöver säkras en långsiktig finansiering för drift och förvaltning. DIGGs förslag är att detta bäst sker genom en finansiering via anslag. Idag finansieras arbetet från sakanslaget för välfärdens digitala infrastruktur, 2:7 ap.3. Utifrån att detta blir en permanent uppgift för DIGG föreslår DIGG istället ett förstärkt förvaltningsanslag till DIGG.

Statliga myndigheter kommer på detta sätt att investera i övriga sektorers digitalisering. Man kan argumentera för att även kommuner och regioner ska vara en del av omfördelningen inom ram. DIGGs uppdrag inkluderar privata utförares

[15] Statskontoret, Modeller för fördelning av nyttor och kostnader för digital infrastruktur – exemplet verksamt.se – slutrapport, 2018-05-08, Stockholm, 2018 (Fi2018/00585/DF)

anslutning. Vid en omfördelning inom statsbudgeten inom ram innebär detta att statliga myndigheter kommer att investera i övriga sektorers digitalisering.

7.2.2 Finansiering av SDK drift och förvaltning med avgifter

Att den aktör som använder en förvaltningsgemensam tjänst också betalar kan vara rimligt. Avgifter för användning kan beräknas på olika sätt. Avgiftsmodeller är administrativt betungande att ta fram och att underhålla över tid för att säkerställa full kostnadstäckning. Avgiftsmodeller medför även administrativa kostnader som måste adderas till avgiften. Avgiftsfinansiering innebär att anslutna deltagare betalar avgifter som motsvarar DIGGs kostnader för drift och förvaltning och DIGGs administrativa kostnader för att hantera avgifter.

DIGG har i huvudsak analyserat avgifter som baseras på användningen (transaktionsbaserad) och avgifter för viss tidsperiod (abonnemang).

Transaktionsbaserade avgifter är lämpliga när kostnaderna för tjänsten ökar med en ökad användning, vilket därmed medför en hög flexibilitet i finansieringen. Det innebär också att den som använder tjänsten har en valfrihet i hur stor användningen ska vara utifrån sina ekonomiska förutsättningar. En sådan avgift riskerar att hämma användningen, vilket har en motsatt effekt mot syftet att uppnå ett högt nyttjande. DIGG bedömer att detta finansieringsalternativ kommer att innebära en avsevärd ökade administrativa kostnader inklusive att utveckla IT-stöd/försystem för att möjliggöra fakturering av avgifter.

En avgift i form av abonnemang, exempelvis årsavgift är inte kopplad till användningen. En avgift i form av abonnemang är lämplig när kostnaderna för tjänsten inte ökar med en ökad användning. För den anslutna deltagaren så är avgiften förutsägbar. Bedömningen i dagsläget är att årsavgifter innebär mindre administrativa kostnader jämfört med avgift per styck. Antagandet bygger på att det är enklare administration och ger lägre kostnader för IT-stöd.

En alternativ avgiftsmodell som skulle vara tänkbar och rättvis, vore att basera avgiftens storlek på regioners respektive kommuners folkmängd. Denna modell används av ofta av tredjepartsleverantörer av IT. DIGGs bedömning är dock att en eventuell framtida abonnemangsmodell behöver utgå från andra beräkningsgrunder då folkmängd är inte är applicerbart på statliga myndigheter och privata utförare.

Ett sätt att fördela ett abonnemang är att alla deltagare, som ansluter sig, betalar en lika stor avgift. Det kan tyckas orättvist att stora och små kommuner ska betala lika. Dock kan avgiften vara liten i det fall anslutningsgraden blir hög.

DIGGs bedömning är att en avgiftsfinansiering av SDK inte är lämplig, då tjänsten inte är mogen och att avgifter bedöms som hämmande för anslutning och användning

7.3 Kostnader kopplade till anslutning till SDK

För en deltagare så finns det flera typer av kostnader förknippade med anslutning. DIGG vill kort belysa dessa då de kan ha påverkan på anslutningsviljan till SDK.

I den samhällsekonomiska kostnadsnyttoanalys, kring kommuner och statliga myndigheters anslutning som redogörs för i avsnitt 2.3, fokuseras på tre typer av kostnader kring anslutning till SDK:

- Engångsavgift för anslutning till SDK, för de kostnader som tillhandahållaren har.
- Engångskostnad för implementation/installation av meddelandetjänst, meddelandeklient och accesspunkt, vilken betalas till tredjepartsleverantör. De aktörer som utvecklar en egen funktionalitet har inte denna kostnad, men egna utvecklingskostnader med mera.
- Årlig licenskostnad för meddelandetjänst, meddelandeklient och accesspunkt som betalas till tredjepartsleverantör. De aktörer som utvecklar en egen funktionalitet har inte denna kostnad, men egna utvecklingskostnader med mera.

De uppskattade kostnaderna i kostnadsnyttoanalysen har beräknats utifrån information som erhållits genom intervjuer och skriftlig kommunikation med kommuner, regioner och statliga myndigheter, samt andra aktörer involverade i utvecklingen av SDK samt tredjepartsleverantörer. Tabellen nedan visar uppskattade kostnader för en kommun på 70 000 invånare.

Typ av kostnad	Min (kr)	Max (kr)
Engångs avgift anslutning till SDK	56 000	60 000
Engångskostnad implementering /Installation	50 000	100 000
Årlig licenskostnad	100 000	150 000

I rapporten är den totala kostnaden för kommunsektorn uppskattad. Tabellen nedan visar total för dessa tre kostnadstyper.

Typ av kostnad	Min (kr)	Max (kr)
Engångs avgift anslutning till SDK	18 000 000	19 000 000
Engångskostnad implementering /Installation	14 000 000	29 000 000
Årlig licenskostnad	13 000 000	19 000 000

Enligt regeringsuppdraget ska en analys, för hur olika finansieringsmodeller påverkar anslutningen till SDK, göras. DIGGs bedömning är att kostnader för anslutning till SDK, installationskostnad och årlig hyrlicenskostnad till eventuella tredjepartsleverantör är hämmande för anslutning till SDK. Dessa kostnader kommer att för många kommuner vara högre än kostnaden för en eventuell avgift för användningen av själva SDK.

DIGG kan som tillhandahållare av SDK välja att ansluta deltagare avgiftsfritt. DIGG bedömer att detta främjar viljan att ansluta sig och sannolikt ökar anslutningstakten. Denna kostnad finansieras via föreslaget förstärkt förvaltningsanslag till DIGG. Dock kan installationskostnad och årlig hyrlicenskostnad till tredjepartsleverantör vara en så stor andel av den totala kostnaden att det fortsatt är hämmande för anslutning.

8 Fortsatt etablering och främjande

8.1 Etablering av SDK hos DIGG

DIGG har, för att kunna ta det ansvar för SDK som regeringsuppdraget beskriver etablerat ett uppdragsteam och ett myndighetsgemensamt arbete för att förbättra förmågan till livscykelhantering.

Målen är att DIGG fram till september 2023, i nära samarbete med SKR, Inera och andra relevanta parter, ska:

- Etablera och bedriva en välfungerande, säker och effektiv verksamhet hos DIGG för att ansvara för och tillhandahålla helheten av SDK. Det innebär att etablera de förmågor som behövs för att säkerställa användarnära,

verksamhetsnära och teknisk utveckling och förvaltning av SDK-federationen och plattformen.

- DIGG ska inom ramen för detta omhänderta de verksamhetsmässiga och tekniska tjänster och produkter som idag finns hos Inera för att kunna tillhandahålla hela infrastrukturen.
- Arbeta tillsammans med SKR och Inera med att främja införandet och anslutning.
- Etablera och underhålla de forum som behövs för att DIGG ska agera professionellt i sina externa kontakter inom infrastrukturen och genom dessa kan informera och samla in behov och synpunkter. Även de forum som behövs för att hantera löpande drift och förvaltning.
- Arbeta strukturerat och löpande med de utmaningar och risker, inklusive informationssäkerhetsrisker och säkerhetskrav, som uppkommer för att etablera och omhänderta infrastrukturen.
- Tillsammans med SKR och Inera samt andra berörda parter planera för infrastrukturens utveckling och förvaltning efter september 2023. Detta presenteras i den långsiktiga planen för Ena – Sveriges digitala infrastruktur.
- Följa upp och redovisa införandet, användningen och dess effekter. Följa upp kostnader för omställning för offentlig sektor samt löpande driftkostnader.
- Redovisa uppdraget till regeringen.

8.2 Samverkan och främjande

Det pågår ett aktivt och löpande arbete med att stödja införande och anslutning utifrån nuvarande struktur och ansvarsfördelning, med DIGG som ansvarig för plattformen och Inera för SDK federationen. Exempel på det är främjande aktiviteter som stödjer anslutning av deltagare och accesspunktsoperatör till infrastrukturen. Återkommande träffar, kunskapsöverföring och handledning har varit några av nycklarna i anslutningsförfarandet. Det har kunnat kombineras med utveckling av vägledningar, lathundar, rollbeskrivningar och stödjande material för målgruppen accesspunktsoperatörer. Likaså utveckling och användning av digitala kanaler i syfte att stödja deltagare och andra aktörer och i anslutning till SDK:s miljöer och tjänster.

Under andra kvartalet etablerade DIGG tydligare samverkan med regeringsuppdragets nämnda myndigheter[16]. Det är samma myndigheter som i sina regleringsbrev fått i uppdrag att förbereda anslutning till infrastrukturen. I anslutning till det anmälde även Skatteverket intresse av att ingå i samverkan, vilket de också bjudits in till. De flesta myndigheterna har identifierat och återkommit till DIGG med kontaktpersoner för ledning, verksamhet, teknik och juridik. I maj samlade DIGG myndigheterna till ett gemensamt möte för att få en gemensam lägesbild, informera om DIGGs uppdrag och fånga myndigheternas behov och förutsättningar. Resultatet har legat till grund för den fortsatta riktningen och planeringen.

Med det som ingångsvärde och för arbetet i sin helhet har DIGG, SKR och Inera utvecklat ett närmare samarbete och former för främjande som omfattar såväl kommuner, regioner som statliga myndigheter. Det är en förutsättning för det som efterfrågas för att kunna införa och utbyta säker digital kommunikation. Det är också en förutsättning för den kunskapsöverföring som behövs när det handlar om behovsfångst och främjandeinsatser. DIGGs samverkan med nämnda myndigheter kommer under hösten knytas närmare det främjande som DIGG åläggs i regeringsuppdraget. Arbetet kommer att planeras, genomföras och följas upp tillsammans med Inera. Exempel på insatser i samverkan är återkommande myndighetsmöten, samlad statusvy för anslutning, tillgång till gemensamt digitalt samarbetsrum, leverantörskontakter och identifiering av möjliga testverksamheter.

För statliga myndigheter som inte har i uppdrag att förbereda anslutning, men som är intresserade behöver information och kommunikation fortsätta att förbättras och utvecklas.

Som ett led i det fortsatta arbetet och för att möta behov av anslutning hos de som ska utbyta information behöver DIGG, SKR och Inera en gemensam införandestrategi, som vägleder hur kommande insatser bör riktas för att nå största effekt.

[16] Arbetsförmedlingen, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Polismyndigheten, Kriminalvården, Skolverket, Socialstyrelsen, Statens institutionsstyrelse

8.3 Fortsatt samråd med MSB och Riksarkivet

DIGG avser i det fortsatta arbetet samråda med MSB och Riksarkivet rörande infrastrukturens utformning. Genom att ytterligare beskriva den befintliga infrastrukturen och löpande informera om DIGGs övertagande samt eventuell vidareutveckling och riskreducerande åtgärder. Det är av vikt för DIGG att fördjupa dialogen och söka stöd hos dessa aktörer. DIGG bedömer också att det kan stödja deltagare i bedömningar av anslutning.

8.4 Försäkringskassan som driftspartner och stöd vid övertagande av SDK

För att tillhandahålla SDK kommer DIGG behöva stöd av Försäkringskassan som driftsleverantör. Dialog och samarbete med Försäkringskassan gällande SDK pågår. DIGG ser bland annat behov för stöd inom följande områden:

- Arkitektkompetens inom infrastrukturområdet
- Etablera infrastruktur för applikationsdrift
- Etablera modell för produktionsövervakning avseende att applikationen är uppe och tillgänglig för externa parter 24/7.
- Etablera incidenthantering enligt Försäkringskassans beredskapsverksamhet
- Etablera modell för säkerhetsövervakning avseende applikationen 24/7 (SOC).
- Penetrationstester av slutlig lösning.
- Kompetens och stöd inom design och deployment för applikationens driftslösning.

8.5 Finansiering framåt

DIGG har utifrån hittills insamlade erfarenheter och kunskap rörande genomförandet av det regeringsuppdraget identifierat att kostnaderna för genomförandet överstiger de 6 miljoner som DIGG initialt fick för genomförandet av uppdraget. DIGG har därför begärt ytterligare 12 miljoner för 2022 och regeringen har beslutat om en ändring av regeringsuppdraget för att DIGG skulle ha möjlighet att genomföra sitt uppdrag (I2022/01074). Total kostnad för DIGGs genomförande under 2022 är estimerad till 18 miljoner kr.

För 2023 bedömer DIGG att satsningen behöver förstärkas ytterligare då DIGG och Inera kommer behöva upprätthålla dubbla tekniska miljöer och förvaltningsorganisationer under en tid. Dessa är dock estimat som med ökad

kunskap kan komma att förändras. Vidare tillkommer kostnader för drift hos Försäkringskassan.

DIGG bedömer för 2023 kostnader om 24 miljoner. Ineras kostnader bedöms ligga på samma nivå som 2022.

DIGG bedömer att en fortsatt satsning på främjande krävs för att uppnå nyttorna med infrastrukturen och även säkerhetskraven, 10 miljoner för 2023 och 2024, som bör fördelas mellan DIGG och SKR, där organisationernas respektive roller tydliggörs.

I sammanhanget vill DIGG informera om att myndigheten lämnat in estimat om ökade kostnader för bland annat SDK och Ena i hemställan till MSB rörande regeringsuppdrag om åtgärder inom civilt försvar om 10 miljoner årligen som beror av vilket säkerhetsnivå infrastrukturen bedöms behöva upprätthålla.

9 Bilagor

Bilaga 1. Rättslig analys