Regelverk för anslutning till Säker digital kommunikation – Informationssäkerhet

Version 1.3 (2022)

1 Innehåll

Revisionshistorik

Version	Datum	Författare	Kommentar
1.0 (2022)	220227	Malin Domeij	Första beslutad version för tjänsten Säker digital kommunikation.
1.1 (2022)	220307	Malin Domeij	Språklig korrigering i avsnitt 4.1.
1.2 (2022)	220609	Marco de Luca	Uppdatering av regelverket avseende: Avsnitt 3.1 • Uppdaterad skrivning kring ansvar vid anslutning av underliggande organisation
1.3 (2022)	221108	Marco de Luca	Uppdatering av regelverket avseende: Avsnitt 5.4 • Skrivning om slumptalsgenerator

1. Bakgrund och syfte

Detta dokument utgör Säker digital kommunikations (SDK) gemensamma regelverk inom informationssäkerhet. Regelverket är framtaget för organisationer som har för avsikt att ansluta till SDK och specificerar de säkerhetskrav som ställs på anslutna aktörer till SDK.

I bilaga beskrivs it-säkerhetskrav, vilka är en integrerad del av detta regelverk. Därutöver regleras krav på t.ex. användarorganisationers lokala komponenter inklusive tillgänglighet samt anslutningsprocess till SDK i SDKs övriga gemensamma regelverk.

I federationsdeklaration beskrivs krav som gäller för SDK som tillämpning av eDelivery transportinfrastruktur (Plattform för eDelivery).

Regelverket syftar till att etablera gemensamma säkerhetskrav för hantering av uppgifter klassade upp till (och innefattande) konsekvensnivån *allvarlig* enligt Myndigheten för samhällsskydd och beredskap, MSB:s modell för klassificering av information.

För att säkerställa efterlevnaden av detta regelverk krävs att varje användarorganisation ska genomföra en egenkontroll och dokumentera denna i en självdeklaration som ska tillsändas SDK-federationsoperatör. Självdeklarationen ska ha godkänts av SDK-federationsoperatör inför anslutning till produktionsmiljö.

Dokumentet utgör den första versionen av regelverket för tjänsten Säker digital kommunikation 2022. Det kan komma att revideras med anledning av ytterligare dokumentation från DIGG som ej finns tillgänglig, förändrad säkerhetsmodell och förändrade ansvarsförhållanden mellan DIGG som ansvarig för eDelivery transportinfrastruktur respektive Inera som SDK-federationsägare- och operatör av SDK. Man bör även förvänta sig att det kan uppstå behov av uppdateringar de första åren när SDK införs hos användarorganisationer.

1.1 Informationsinnehåll och ansvarsförhållande

Informationssäkerheten inom SDK är dimensionerad för att svara mot de risker som uppgifter av allvarlig konsekvensnivå kan förväntas medföra.

Myndigheten för samhällsskydd och beredskap föreskriver och tillhandahåller metodstöd för förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. MSB:s förskrifter och metodstöd tillhandahåller stöd för bedömning och hantering av information.

Sveriges Kommuner och Regioner, SKR:s informationsklassningsverktyg KLASSA ger stöd i användarorganisationens egen bedömning av uppgifters känslighetsgrad. Verktyget ger även exempel på kategorier av uppgifter som allmänt bör betraktas tillhöra konsekvensgraden *allvarlig,* såsom särskilda kategorier av personuppgifter enligt kapitel 9 Dataskyddsförordningen (GDPR).

Respektive användarorganisation ansvarar för den egna klassningen och för bedömningen av vilken information som kan överföras i digitala meddelanden via SDK och eDelivery transportinfrastruktur. Det är således varje användarorganisations eget ansvar att själva göra en bedömning av konsekvensnivån i informationsinnehållet innan det skickas, och om SDK och eDelivery transportinfrastruktur kan användas för att förmedla uppgifterna till mottagaren.

Respektive användarorganisation ska analysera och vidta åtgärder som följer av lagar och förordningar som gäller organisationen och dess anslutning till SDK, t.ex. vad avser incidenthantering och logghantering.

2. Definitioner

Term	Beskrivning
Ansvarig för eDelivery transportinfrastruktur	I Sverige ansvarar Myndigheten för digital förvaltning, DIGG, för eDelivery transportinfrastruktur.
Accesspunkt	Accesspunkten utgör respektive användarorganisations anslutningspunkt till eDelivery transportinfrastruktur. Accesspunkten är den anslutningspunkt som en användarorganisation använder för att överföra meddelanden till andra användarorganisationer i SDK via eDelivery transportinfrastruktur.
Accesspunktsoperatör	Accesspunktsoperatör avser den roll som ansluter användarorganisationen till eDelivery transportinfrastruktur via en accesspunkt.
Användarorganisation	Användarorganisation avser den organisation som har anslutit eller har för avsikt att ansluta till SDK i syfte att överföra digitala meddelanden till andra användarorganisationer. Användarorganisation i SDK motsvarar deltagare i eDelivery transportinfrastruktur.
Berörd verksamhet	Berörd verksamhet är den eller de verksamheter inom en användarorganisation som använder eller ska använda SDK.
eDelivery transportinfrastruktur (Plattform för eDelivery)	eDelivery transportinfrastruktur avser gemensamma komponenter, regelverk och specifikationer som tillhandahålls för anslutning till eDelivery av ansvarig för eDelivery transportinfrastruktur.
eDelivery transportinfrastrukturs gemensamma komponenter (Plattformstjänster)	eDelivery transportinfrastrukturs gemensamma komponenter utgörs av bland annat SMP-tjänst (Service Metadata Publisher), SML-tjänst (Service Metadata Locator) och Certifikatpubliceringstjänst. Dessa är gemensamma tjänster där användarorganisations metadata registreras för anslutning, vilket krävs för överföring av meddelanden via SDK.
Federationsdeklaration	Är den dokumentation som SDK-federationsägare genomför och tillhandahåller till ansvarig för eDelivery som ett led i

	etablering av SDK som tillämpning av eDelivery transportinfrastruktur och därefter löpande enligt anvisning från ansvarig för eDelivery.
Lokala komponenter	Lokala komponenter utgör de komponenter som användarorganisation använder för att etablera sin förmåga att ansluta till och överföra meddelanden via SDK: Accesspunkt, Meddelandetjänst samt Meddelandeklient. Anslutande system är ett samlingsbegrepp för Meddelandetjänst och Meddelandeklient.
Säker digital kommunikation (SDK)	SDK avser SDKs gemensamma komponenter, miljöer och regelverk inklusive tekniska specifikationer och anslutningsprocess som tillhandahålls för anslutning till och överföring av digitala meddelanden.
SDKs gemensamma komponenter (Federationstjänster)	SDKs gemensamma komponenter utgörs bl.a. av SDK Adressbok. Detta är en tjänst där användarorganisations metadata i form av organisatoriska adressuppgifter registreras för uppslagning vid överföring av meddelanden via SDK.
SDKs gemensamma regelverk	SDKs gemensamma regelverk utgörs bl.a. av detta regelverk inom informationssäkerhet, SLA tillgänglighet, tekniska specifikationer samt anslutningsprocess.
SDK-federationsoperatör	SDK-federationsoperatör är den organisation som förvaltar SDK och tillhandahåller SDKs gemensamma komponenter, miljöer och regelverk. För närvarande är Inera både SDK-federationsägare- och operatör.
SDK-federationsägare	SDK-federationsägare ansvarar för federationen gentemot ansvarig för eDelivery transportinfrastruktur. SDK-federationsägare kan utse SDK-federationsoperatör. För närvarande är Inera både SDK-federationsägare- och operatör.
Självdeklaration	Är den dokumentation av egenkontroll som användarorganisation genomför och tillhandahåller till SDK-federationsoperatör som ett led i anslutningsförfarandet, och därefter löpande minst vart tredje år.

3. Organisation och styrning

3.1 Övergripande krav på verksamheten

En användarorganisation som inte är ett offentligt organ ska drivas som registrerad juridisk person.

En användarorganisation ska ha en etablerad verksamhet, vara fullt fungerande i alla delar som berörs i detta dokument, samt vara väl insatt i de juridiska krav som ställs på denne utifrån användande av SDK.

En användarorganisation som ansluter underliggande organisationer ska ha en formell relation (ingå i samma koncern) med dessa och ansvarar för att dessa uppfyller Tjänstens regelverk samt den inre säkerheten i anslutande system.

En användarorganisation som på annan part har lagt ut utförandet av en eller flera av de åtaganden som omfattas av detta regelverk, ska genom avtal ålägga utförande parten (leverantören) och dess eventuella underleverantörer samma skyldigheter som åläggs användarorganisationen i relevanta delar.

3.2 Informationssäkerhet

Användarorganisation ska, för de delar av verksamheten som berörs genom anslutning till SDK, bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete där:

1. Risker förknippade med anslutningen ska regelbundet analyseras. I riskanalysen ska det ingå en åtgärdsplan.
2. Förutom det som framgår av detta regelverk ska ändamålsenliga och proportionella organisatoriska och tekniska åtgärder vidtas för att hantera risker. Åtgärderna ska säkerställa en nivå av säkerhet som är lämplig i förhållande till risken.
3. Lämpliga åtgärder för att förbygga och minimera konsekvenser av incidenter ska vidtas. Åtgärderna ska syfta till att säkerställa kontinuitet i tjänsten.
4. Arbetet med informationssäkerhet ska dokumenteras och revideras årligen.

3.3 Personuppgiftsansvar och ansvar för allmän handling

Detta avsnitt syftar till att förtydliga ansvar hos sändande respektive mottagande användarorganisation vid överföring av digitala meddelanden via SDK.

3.3.1 Personuppgiftsansvar

Ett meddelande som överförs via SDK är, förutsatt att det innehåller personuppgifter, att betrakta som personuppgift även om det är krypterat med certifikatnycklar.

Sändande respektive mottagande användarorganisation är personuppgiftsansvarig för sina respektive lokala komponenter inklusive accesspunkt.

Sändande användarorganisation ansvarar för källinformationen i meddelande som överförs. Ett nytt ansvar avseende fortsatt personuppgiftsbehandling kan uppstå hos mottagande användarorganisation.

Mottagande användarorganisation blir personuppgiftsansvarig för meddelandet om det innehåller personuppgifter när transportkvittens skickas av dess accesspunkt till sändande användarorganisations accesspunkt. Om kvittens ej sänds, uppstår inget personuppgiftsansvar hos mottagande användarorganisation.

SDK-federationsoperatör och Ansvarig för eDelivery transportinfrastruktur är inte part i användarorganisationers behandling av personuppgifter vid överföring av meddelanden via SDK och eDelivery transportinfrastruktur.

3.3.2 Allmän handling

Ett meddelande som överförs via SDK från en myndighet alternativt tas emot av en myndighet är att betrakta som en allmän handling enligt Tryckfrihetsförordningen.

Meddelandet ska anses vara utlämnat respektive inkommet när det är tillgängligt för teknisk bearbetning/dekryptering i mottagande myndighets meddelandetjänst.

Det är dock upp till varje användarorganisation att besluta när man faktiskt anser att handlingen är inkommen.

3.4 Likabehandling av alla anslutna parter

En användarorganisation ska acceptera meddelandeöverföring från alla inom SDK anslutna användarorganisationer under förutsättning att kommunikationen sker i enlighet med gällande gemensamma regelverk.

3.5 Incidenthantering

Utöver vad som framgår i avsnitt 1.1, ska en användarorganisation ansvara för att bedöma och anmäla incidenter enligt lagar och förordningar samt informera SDK-federationsoperatör och allmänheten/de registrerade om så krävs. Användarorganisation ska vid felaktigt inkomna meddelanden som utgör personuppgiftsincidenter agera skyndsamt.

SDK-federationsoperatör är användarorganisation behjälplig, genom att tillhandahålla information om och vidta åtgärder vid incidenter som avser SDKs gemensamma komponenter.

3.6 Efterlevnad av gemensamma regelverk

Utöver vad som framgår i avsnitt 1.1 och i övrigt i avsnitt 3, ska en användarorganisation ansvara för att uppmärksamma brister i egen eller annan användarorganisations efterlevnad av SDKs gemensamma regelverk samt informera SDK-federationsoperatör och annan användarorganisation.

3.7 Avveckling av SDK-anslutning

En användarorganisation som vill avsluta sin anslutning till SDK ska avregistrera samtliga uppgifter i metadata- och adressregister och frånträda avtalet om SDK med SDK-federationsoperatör.

Spårbarhetsinformation ska fortsatt hållas tillgänglig i enlighet med kraven i avsnitt 5.1 i detta regelverk.

I de fall användarorganisationen inte avregistrerar sina uppgifter kommer SDK-federationsoperatör att göra detta tidigast när alla delar i anslutningen formellt avslutats.

4. Administrativ och personalorienterad säkerhet

4.1 Åtkomst till information som förmedlas via SDK

En användarorganisation ska ha rutiner och kontroller som säkerställer att endast behöriga personer har åtkomst till den information som förmedlas genom SDK.

För åtkomst till system och tillämpningar som behandlar uppgifter som förmedlas inom SDK ska användaren använda en autentiseringsmetod som uppfyller kravet på stark autentisering. Autentiseringsmetoden ska vara utformad som en flerfaktorsautentiseringslösning (multifaktorautentisering) och uppfylla kravet för minst tvåfaktorsautentisering.

Autentiseringsmetoden ska minst uppfylla två av nedanstående krav (faktorer):

- Med någonting som användaren vet, t.ex. användarnamn/lösenord eller pinkod
- Med någonting som användaren har, t.ex. smart kort, fysisk enhet (OTP-dosa), autentiseringsapplikation (OTP), USB-token, mobila certifikat med säker lagring av den privata nyckeln, TPM-chip, eller motsvarande
- Med hjälp av användaren själv (biometri), t.ex. fingeravtryck eller avläsning av iris. Biometri ska dock endast användas som PIN-kodsersättning.

Användarorganisationen ska ha egna rutiner och kontroller avseende bl.a.:

- Utgivningsprocessen av autentiseringsmetoden ska i allt väsentligt följa tillitsramverk för Svensk e-legitimation LoA3 eller eIDAS nivå väsentlig.
- Utgivningen av autentiseringsmetod ska innefatta kontroll av en fysisk legitimationshandling.
- Användaren ska kontrolleras mot offentligt register såsom folkbokföringsregistret innan eller i samband med utgivningen av autentiseringsmetoden.
- Användarens arbetsidentitet ska vara unik och bestående över tid.
- Autentiseringsmetoden ska vara personlig och knuten till den enskilda användaren och får ej delas med andra.
- Rutiner för att spärra en användares autentiseringsmetod ska finnas upprättade och vara kända av användarna.

4.2 Hantering av metadata och adressinformation

En användarorganisation ska vid anslutning tillhandahålla och därefter vidmakthålla korrekt och uppdaterad metadata samt adressinformation för överföring av meddelanden via SDK.

Användarorganisation ansvarar för att dess metadata och adressinformation hanteras av behöriga administratörer av SDKs respektive eDelivery transportinfrastrukturs gemensamma komponenter.

Användarorganisation ska vid förändring av någon av nedanstående uppgifter utan oskäligt dröjsmål genomföra uppdatering genom de administrationsgränssnitt och andra förfaranden som tillhandahålls av SDK-federationsoperatör respektive ansvarig för eDelivery transportinfrastruktur.

4.2.1 SDK Adressbok

Metadata utgörs av sådan information som krävs för registrering i SDK Adressbok och inkluderar:

- Organisationsidentifierare (deltagaridentitet i eDelivery transportinfrastruktur)
- Organisationsnamn och organisationsnummer
- Administratörsuppgifter (namn, e-post samt personnummer och/eller HSA-id)

För adressinformation ska användarorganisation:

- Hämta information från tillförlitlig källa som anges av SDK-federationsoperatör
- Uppdatera eventuell lokal läskopia enligt angivna tidsintervaller

4.2.1.1 Regelverk för organisationsidentifierare

I enlighet med DIGGs regelverk för organisationsidentifierare ska varje organisation identifieras enligt standard ISO6523 för global identifiering av avsändare och mottagare.

Inom standarden tillåts följande typer (ICD) för SDK:

- Domänidentifieraren ska vara unik och säkert kunna knytas till den aktuella organisationen
  - ISO6523:0203
- Svenskt organisationsnummer
  - ISO6523:0007

4.2.2 SMP-tjänst

Metadata utgörs av sådan information som krävs för kontroll av användarorganisations registrerade uppgifter i SMP och inkluderar:

- Deltagaridentitet i eDelivery transportinfrastruktur
- SDK dokumenttyp och version
- Accesspunktsoperatörs publika certifikatsuppgifter (organisationsnamn och accesspunktsidentitet)

4.2.3 Certifikatspubliceringstjänst

Metadata utgörs av sådan information som krävs för registrering i Certifikatspubliceringstjänst och inkluderar:

- Deltagaridentitet i eDelivery transportinfrastruktur
- SDK dokumenttyp och version
- Publikt certifikat eller certifikatsigneringsbegäran

5. Teknisk säkerhet

5.1 Spårbarhet

Utöver vad som framgår i avsnitt 1.1 samt i ramverk och regelverk för eDelivery transportinfrastruktur, ska en användarorganisation säkerställa att alla meddelandeöverföringar via dess lokala komponenter som användarorganisationen är deltagande part i loggas. Sådan logginformation ska bevaras för att kunna användas vid felsökning samt vid utredning av informationssäkerhetsincidenter. Krav på loggning specificeras i it-säkerhetsbilagan till detta regelverk.

Tiden för bevarande av loggar ska inte understiga 12 månader och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritetssynpunkt eller har stöd i lag eller annan författning.

5.1.1 Uppföljning och granskning

Användarorganisation ska vid förfrågan från annan användarorganisation eller SDK-federationsoperatör vara behjälplig med att ta fram och lämna ut relevant logginformation, under förutsättning att den part som efterfrågat uppgifterna har ett berättigat intresse av dem och att användarorganisationen inte enligt lag eller annan författning är förhindrad att lämna ut sådana uppgifter.

5.2 Tid

Korrekt inställning och exakt funktion av datorklockor är väsentligt för att säkerställa giltigheten hos de loggar som förs. Krav på tidssynkronisering specificeras i it-säkerhetsbilagan till detta regelverk.

5.3 Kryptografiska säkerhetsåtgärder

Överföring av meddelanden via SDK ska följa de vid var tid gällande tekniska protokollspecifikationer som SDK-federationsoperatör SDK meddelar, samt de där angivna metoderna för skydd mot insyn och manipulation avseende säkerhetsprotokoll, algoritmer samt nyckellängder.

5.4 Hantering av kryptografiskt nyckelmaterial

Kryptografiskt nyckelmaterial som används för skydd av överföring av meddelanden via SDK ska skapas på ett säkert och trovärdigt sätt med slumptalsgenerator, samt skyddas vid förvaring och användning så att det inte röjs till obehöriga.

5.5 Skydd mot intrång och skadlig kod

Användarorganisation ska ha ett uppdaterat skydd mot intrång, skydd mot inkommande skadlig kod samt skydd mot spridning av skadlig kod för att undvika att påverka mottagande användarorganisation eller SDK-federationsoperatör.

6. Självdeklaration

En användarorganisation ska till SDK-federationsoperatör, dels vid anslutning och därefter löpande minst vart tredje år, tillhandahålla en självdeklaration som intygar att den anslutna organisationen genomfört kontroll att denne uppfyller kraven i detta regelverk. Självdeklarationen ska följa SDK-federationsoperatörs angivna format.

Användarorganisation ska vid väsentliga förändringar som påverkar dess anslutning, såsom byte av accesspunkt eller anslutande system, inkomma med ny självdeklaration.

SDK-federationsoperatör har rätt att begära in självdeklaration som en del i granskning av anslutna parter.