Regelverk för anslutning till Säker digital kommunikation - Informationssäkerhet

Version 1.4

inera

Ett företag inom SKR

Innehåll

Revisionshistorik

VERSION	DATUM	FÖRFATTARE	KOMMENTAR
1.0	2022-02-27	Malin Domeij	Första beslutad version för tjänsten Säker digital kommunikation.
1.1	2022-03-07	Malin Domeij	Språklig korrigering i kap. 4.1.
1.2	2022-06-09	Marco de Luca	Uppdatering av regelverket avseende: kap. 3.1 Uppdaterad skrivning kring ansvar vid anslutning av underliggande organisation
1.3	2022-11-08	Marco de Luca	Uppdatering av regelverket avseende: kap. 5.4 Skrivning om slumptalsgenerator
1.4	2023-03-22	Annika Liljegren	Uppdatering av regelverket avseende: - Syfte förtydligat. Krav på tillgänglighet i lokala komponenter tillkommer som bilaga - Tillgänglighetsbilaga. - Text om självdeklaration flyttad till kap. 6. - Informationsinnehåll och ansvarsförhållande förtydligat krav inkl. komplettering med kontroll av mottagares funktionsadress samt rekommendation vid skapande av ny funktionsadress. - Tidigare avsnitt 2 Definitioner utgår (beskrivs på tjänstens informationssida inkl. komplettering med definition av eDelivery transportinfrastrukturs gemensamma regelverk). - kap. 3.1, Övergripande krav på verksamheten: förtydligande inkl. krav på godkänd accesspunkt. - kap. 3.1.2.1, Regelverk för organisationsidentifierare: förtydligat krav i enlighet med Diggs regelverk. - kap. 3.2, Informationssäkerhet: förtydligat beskrivning av berörd verksamhet samt krav på systematiskt informationssäkerhetsarbete motsvarande ISO27000. - kap. 3.3, Personuppgiftsansvar och ansvar för allmän handling: förtydligat krav. - kap. 3.2, Åtkomst till information: förtydligat krav på administratörers åtkomst i gemensamma komponenter resp. användares åtkomst i lokala komponenter. - kap. 4.2, Tid: förtydligat krav. - kap. 4.3, Kryptografiska säkerhetsåtgärder: språklig förenkling. - kap. 5.3, Krav på kryptografiska säkerhetsåtgärder: förtydligat att krav framgår i it-säkerhetsbilaga. - kap. 6, Självdeklaration: lagt till att SDK-federationsoperatör har rätt att begära in ny deklaration vid granskning eller revision och misstanke om brister i efterlevnad.

1. Syfte

Detta dokument är en del av Säker digital kommunikations (SDK) gemensamma regelverk för organisationer som har för avsikt att ansluta till och använda SDK.

Dokumentet utgör regelverket inom informationssäkerhet och specificerar de säkerhetskrav som ställs på anslutna aktörer till SDK. I bilagor beskrivs it-säkerhetskrav respektive tillgänglighetskrav på lokala komponenter.

Därutöver regleras i SDKs gemensamma regelverk t.ex. tekniska specifikationer samt anslutningsprocessen till SDK. Det gemensamma regelverket finns på tjänstens informationssida.

1.1 Definitioner

Definitioner finns i Ordlista på SDKs öppna informationsyta.

2. Informationsinnehåll och ansvarsförhållande

Nivån på informationssäkerhet inom SDK är dimensionerad för att tillgodose skyddsnivå *allvarlig* enligt informationsklassningsmodell som tillhandahålls i Myndigheten för Samhällsskydd och Beredskaps (MSB) metodstöd för systematiskt informationssäkerhetsarbete.

Detta innebär att SDK uppfyller den säkerhetsnivå som krävs för att utbyta sekretessbelagd information samt integritetskänsliga och känsliga personuppgifter. SDK ska inte användas för att utbyta information som omfattas av säkerhetsskyddslagstiftning.

Varje användarorganisation ansvarar för att genomföra informationsklassning av den information som organisationen avser att utbyta via SDK samt att genomföra nödvändiga riskanalyser. Det är varje användarorganisations ansvar att bedöma om SDK och eDelivery transportinfrastruktur har tillräcklig nivå av säkerhet för att utbyta tilltänkt information med tilltänkta mottagare.

För att undvika risk för felaktig adressering bör användarorganisationen inte återanvända funktionsadresser som tidigare har använts i ett annat syfte.

Vid osäkerhet om mottagande användarorganisations funktionsadress ansvarar sändande användarorganisation för att bekräfta korrekt funktionsadress med mottagande organisation innan personuppgifter överförs.

Vid felaktigt inkommit meddelande ska mottagande användarorganisation skyndsamt meddela sändande användarorganisation om detta.

Varje användarorganisation ansvarar för följsamhet mot andra tillämpliga lagar, förordningar och regelverk utöver SDK:s regelverk.

3. Organisation och styrning

3.1 Övergripande krav på verksamheten

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

Användarorganisationen ska vara väl insatt i de juridiska krav som ställs på organisationen utifrån användandet av SDK.

Användarorganisation som ansluter underliggande organisationer ska ha en formell relation med dessa (ingå i samma koncern). Användarorganisationen ansvarar för att även underliggande organisationer följer SDKs regelverk.

Om användarorganisationen anlitar leverantör för utförandet av en eller flera av de åtaganden som omfattas av SDKs regelverk, ska genom avtal ålägga leverantören att följa tillämpliga delar av SDKs regelverk.

Användarorganisationen ska ha en accesspunkt som är godkänd enligt eDelivery transportinfrastrukturs gemensamma regelverk.

3.2 Informationssäkerhet

Användarorganisationen ska, för de delar av verksamheten som berörs av anslutning till SDK, bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete motsvarande standarden ISO/IEC 27000-serien. Detta innebär minst att:

- Tillse att information som utbyts via SDK är identifierad och att informationsklassning har genomförts.
- Regelbundet analysera risker förknippade med anslutningen. Riskanalysen ska inkludera en åtgärdsplan som följs upp årligen.
- 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.
- Tillse att lämpliga åtgärder vidtas för att förebygga och minimera konsekvenser av incidenter. Åtgärderna ska syfta till att säkerställa kontinuitet.
- Det systematiska informationssäkerhetsarbetet 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 innehåller personuppgifter och som överförs via SDK betraktas som personuppgift även om det är krypterat.

Sändande respektive mottagande användarorganisationen är personuppgiftsansvarig för de personuppgifter som hanteras i den egna organisationens lokala komponenter och accesspunkt samt för de loggar som avser användarorganisationens administration i SDKs gemensamma komponenter.

Sändande användarorganisation är personuppgiftsansvarig för de uppgifter som överförs. Ett nytt ansvar avseende fortsatt personuppgiftsbehandling uppstår hos mottagande användarorganisation. Detta sker när mottagande användarorganisations accesspunkt har skickat transportkvittens till sändande användarorganisations accesspunkt.

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 kan betraktas som en allmän handling enligt tryckfrihetsförordningen. Det är dock upp till varje användarorganisation att göra en egen bedömning.

- Meddelandet kan anses vara expedierat av sändande användarorganisation när det är tillgängligt för teknisk bearbetning/dekryptering hos mottagarens meddelandetjänst.
- Meddelandet kan anses vara inkommen hos mottagande användarorganisation när det är tillgängligt för teknisk bearbetning/dekryptering hos mottagarens meddelandetjänst.

3.4 Likabehandling av alla anslutna parter

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

3.5 Incidenthantering, felhantering och support

Användarorganisationen ansvarar för att bedöma och anmäla incidenter enligt lagar och förordningar samt informera SDK-federationsoperatör (via ”Kontakta oss” på Inera.se) och allmänheten/de registrerade om så krävs.

Användarorganisationen ska ha etablerade rutiner för egen felhantering och support.

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

3.6 Efterlevnad av gemensamma regelverk

Om en användarorganisation uppmärksammar brister i egen eller annan användarorganisations efterlevnad av SDKs gemensamma regelverk ska användarorganisationen informera SDK-federationsoperatör (via” Kontakta oss” på Inera.se) och den användarorganisation som brister i efterlevnad.

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 dokument.

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

4. Administrativ säkerhet

4.1 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.

Användarorganisationen 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.

4.1.1 Åtkomst till gemensamma komponenter

Användarorganisationen ansvarar för att dess metadata och adressinformation i gemensamma komponenter hanteras av behöriga administratörer.

För åtkomst och autentisering ska e-legitimation som är godkänd enligt Diggs kvalitetsmärke Svensk e-legitimation (minst LoA3) användas.

4.1.2 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 användarorganisationen:

- Endast hämta adressinformation från SDK Adressbok hos SDK - federationsoperatör
- Uppdatera eventuell lokal läskopia enligt angivna tidsintervaller

4.1.2.1 Regelverk för organisationsidentifierare

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

Organisationsidentifieraren ska vara unik och säkert kunna knytas till organisationen.

Inom standarden tillåts följande typer (ICD) för SDK:

- ISO6523:0007 – Svenskt organisationsnummer
- ISO6523:0203 – eDelivery Network Participant identifier

Typen (ICD) ISO6523:0203 har samma struktur som internetdomännamn. Om det används, ska ett av användarorganisationen ägt domännamn med toppdomän ingå i organisationsidentifieraren.

4.1.3 SMP-tjänst

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

- Deltagaridentitet i eDelivery transportinfrastruktur
- SDK dokumenttyp och version

- Accesspunktsoperatörs publika certifikatsuppgifter (organisationsnamn och accesspunktsidentitet)

4.1.4 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

4.2 Åtkomst till användarorganisationens anslutande system

Användarorganisationen ansvarar för att endast behöriga användare har åtkomst till anslutande system (Meddelandetjänst, Meddelandeklient).

I första hand ska e-legitimation som är godkänd enligt Digg:s kvalitetsmärke Svensk e-legitimation (minst LoA3) användas.

Alternativt ska användarorganisation ha en autentiseringsmetod för åtkomst till anslutande system som följer tillitsramverk för Svensk e-legitimation LoA3 eller eIDAS nivå väsentlig. Detta innebär minst att följande krav ska vara uppfyllda:

- Användare ska kontrolleras mot offentligt register, såsom folkbokföringsregistret, innan eller i samband med att autentiseringsmetoden skapas.
- Vid utlämnande av autentiseringsmetod ska kontroll av fysisk legitimationshandling ske.
- Användarorganisationen ska ha rutiner för att granska sina användares åtkomstbehörigheter. Obehöriga eller användare som inte längre behöver åtkomst ska tas bort. Förändringar av behörigheter ska dokumenteras.
- Användarens identitet ska vara unik och bestående över tid.
- Användarens åtkomst ska vara personlig och knuten till den enskilda användaren och får ej delas med andra.
- Användarens åtkomst ska ske med stark autentisering och uppfylla minst 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), USB-token eller mobila certifikat med säker lagring av den privata nyckeln. SMS-kod ska ej användas.
  - Med hjälp av användaren själv (biometri), t.ex. fingeravtryck eller avläsning av iris. Biometri ska dock endast användas som PIN-kodsersättning.

5. Teknisk säkerhet

5.1 Spårbarhet

Användarorganisationen ska säkerställa att alla meddelandeöverföringar via dess lokala komponenter 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 dokument.

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

Användarorganisationen ska vid förfrågan från annan användarorganisation eller SDK-federationsoperatör vara behjälplig med att ta fram och lämna ut relevant logginformation. Detta 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 ska tillämpas för att säkerställa giltigheten hos de loggar som förs. Krav på tidssynkronisering specificeras i it-säkerhetsbilagan till detta regelverk.

5.3 Kryptografiska säkerhetsåtgärder

Metoder för skydd mot insyn och manipulation i säkerhetsprotokoll, algoritmer och nyckellängder ska tillämpas vid överföring av meddelanden via SDK. Krav på kryptografiska säkerhetsåtgärder specificeras i it-säkerhetsbilagan till detta regelverk.

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

Användarorganisationen ska ha 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

För att säkerställa efterlevnaden av SDKs regelverk krävs att varje användarorganisation genomför en egenkontroll och dokumenterar denna i en självdeklaration.

Användarorganisationen ska vid anslutning inkomma med en självdeklaration som intygar organisationens följsamhet till kraven. Självdeklarationen ska följa SDK-federationsoperatörs angivna format och vara godkänd innan anslutning till produktionsmiljö sker.

Användarorganisationen ska därefter löpande minst vart tredje år, eller 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 ny självdeklaration från användarorganisationen vid granskning eller revision av anslutna parter eller vid misstanke om att användarorganisationen brister i efterlevnad av SDKs regelverk.