Avsedd användning för Säker digital kommunikation (SDK)

Innehåll

1. Inledning

Syftet med detta dokument är att beskriva avsedd användning med Säker digital kommunikation (SDK): vad kan SDK användas till för slags informationsutbyte samt vem får använda och vilka krav ställs på användningen.

1.1 Bakgrund

Hanteringen av integritetskänslig information tar mycket tid idag. Medarbetare är osäkra kring hanteringen, systemen är svåra att använda, och det finns stora manuella inslag. Det är inte en fråga som en part kan lösa och det är inte heller endast en lösning som behövs. Utan vi behöver ett gemensamt sätt för hur vi utbyter känslig information i offentlig sektor och som kan användas av alla aktörer i offentlig sektor och privata utförare. Främst är detta en informationssäkerhetsfråga, men det skapar även möjligheter att effektivisera hantering av ärenden.

1.2 Syfte med SDK

Syftet är att skapa en säker, tillförlitlig och gemensam kanal för kommunikation som uppfyller lagkrav i hantering av ärenden för alla inblandade parter. Det behövs ett generellt sätt att knyta ihop olika system som idag används av offentlig sektor.

2. Mål med SDK

Målet är att det i Sverige ska finnas en standardiserad förmåga till säker digital kommunikation mellan offentliga aktörer och privata utförare av offentligfinansierad verksamhet. Det ska vara enkelt att använda sig av SDK och att ansluta sig till federation. Ingen utom avsändare, mottagare och den det berör ska kunna ta del av informationen. Avsändaren, mottagaren och den det berör är kända (identifierade) för varandra genom tillitsramverk. Informationsdelningen säkras enligt, för informationen gällande, lagar och regelverk och informationen är spårbar.

3. Vilket slags informationsutbyte stödjer SDK?

3.1 Bakgrund kring informationsutbyte

Problemet som SDK avser att lösa är den i dag ostrukturerade informationen (fritext/dokument, etcetera) som hanteras i myndighetsutövningsärenden mellan olika aktörer. Dagens strukturerade informationsutbyte ingår inte i SDK eller dess tänkta lösning. Informationen i SDK går mellan organisationer, är domänöverskridande (till exempel hälso- och sjukvård, socialtjänst, skola), och är känslig (personuppgifter, uppgifter som kan omfattas av sekretess).

3.2 Informationsklassificering

SDK är avsett att användas för informationsutbyte/meddelandeöverföring av information upp till en klassificering såsom känsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Detta innebär en konsekvensbedömning såsom betydande konsekvens vad gäller informationssäkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet, enligt MSB:s modell:

- Konfidentialiteten är bedömd till: Behov av att överföra känsliga personuppgifter/sekretessuppgifter
- Riktighet är bedömd till: Uppgifterna ligger ofta till grund för olika beslut och åtgärder.
- Tillgänglighet är bedömd till: Behov av att kunna använda lösningen i sin dagliga verksamhet.

Nivån baseras på att SDK ska stödja tillräcklig säkerhet i ett omfattande informationsutbyte.

SDK ska inte användas för informationsutbyte där informationen är av högre känslighetsgrad.

Användarorganisationer som ansluter till SDK ansvarar för att genomföra en konsekvensbedömning av meddelandeinnehållet som sänds/tas emot och huruvida SDK kan användas för meddelandeöverföringen.

SDK:s tillitsramverk anger även krav på kontroll av en användares elektroniska identiteter, där verifiering av identitet ska göras genom fullgod svensk identitetshandling och identifiering ska göras genom stark autentisering. Med stark autentisering menas att krav uppfylls enligt tillitsramverk för svensk e-legitimation eller krav enligt tillitsnivå 3, vilket motsvarar eIDAS nivå Väsentlig.

3.3 Användningsfall och målgrupp

SDK riktar sig till primär- och sekundärkommuner, statliga myndigheter, samt de privata aktörer som har ett offentligt uppdrag. De som kan använda SDK är de som anslutit sig genom att teckna avtal gällande tillitsfederation och informationssäkerhet samt uppfyller de tekniska förutsättningarna. Samma förutsättningar gäller oavsett utförare (offentlig respektive privat utförare av offentligfinansierad verksamhet) och alla ingår i samma federation och ett fastställt tillitsramverk.

SDK är tänkt att användas för:

- Sektorövergripande kommunikation av känslig information vid myndighetsutövning mellan kommuner, regioner och statliga myndigheter.
- Sektorövergripande kommunikation av känslig information vid myndighetsutövning som utförs av privata utförare av skattefinansierad verksamhet.
- ”Inomsektoriell” kommunikation av känslig information kommun till kommun, region till region, statlig myndighet till statlig myndighet samt mellan verksamheter inom dessa med sekretessgränser mellan sig.
- För kommunikation till privatpersoner av känslig information vid myndighetsutövning finns befintlig lösning Mina meddelanden att använda/förhålla sig till.
- Ska andra aktörer, till exempel försäkringsbolag, kunna ansluta till SDK så behöver detta beredas och beslutas av styrgruppen.