**Checklista för anslutning till SDK, Säker digital kommunikation**

Nacka kommun

Innehåll

[Innehåll 1](#_Toc420411203)

[Vad är SDK, Säker digital kommunikation? 1](#_Toc569665409)

[Fördelar med SDK 2](#_Toc2135959586)

[Vem ansvarar för införandet av SDK 2](#_Toc1618069044)

[Kartläggning av behov 2](#_Toc673763235)

[Vilka organisationer är anslutna till SDK 3](#_Toc106171876)

[Checklista för anslutning 3](#_Toc941472860)

[Informationssäkerhetsarbete 4](#_Toc1478225609)

[Kontinuitetsplan 4](#_Toc231865879)

[Arbetsrutin för bevakning av inkomna meddelanden 4](#_Toc224048745)

[Arbetsrutin för gallring 4](#_Toc546939066)

[Arbetsrutin för hantering av skyddad identitet 5](#_Toc859160326)

[Arbetsrutin för behörighetshantering 5](#_Toc1627041569)

[Skapa funktionsbrevlåda 6](#_Toc2117436697)

[Regler för incidenthantering 6](#_Toc1934392026)

[Regler för användande av SDK 7](#_Toc1518749159)

[Kontaktuppgifter till den centrala förvaltningen: 8](#_Toc506913760)

[Ytterligare information om SDK 8](#_Toc1683861280)

# Vad är SDK, Säker digital kommunikation?

SDK, Säker digital kommunikation är en tjänst för att skicka känslig information i ostrukturerad form till andra offentliga organisationer (kommuner, myndigheter och regioner). SDK är ett säkert alternativ till fax, telefon, bud, rekommenderade brev och vanliga brev.

SDK-meddelanden skickas till funktionsadresser hos mottagande organisation och inte till specifika tjänstepersoner. SDK-meddelandet är uppbyggt av ett fritextfält med möjlighet att bifoga filer. På Nacka kommun används tjänsten TDialog för att skicka SDK-meddelanden, dvs samma tjänst som används för att skicka vanliga säkra meddelanden.

# Fördelar med SDK

SDK är säkrare än att skicka fax, vanliga brev och mejl och innebär därmed en säkrare hantering för medborgarnas personuppgifter. SDK är snabbare och mer driftsäkert än alternativa lösningen vilket ger effektivare handläggning och snabbare beslut.

Ytterligare en fördel är att kommunikationen med andra offentliga aktörer blir mindre personberoende då SDK-meddelanden skickas till en funktion och inte till en specifik tjänsteman. Detta kan dock i vissa fall upplevas som en nackdel då mycket känslig information delas. Det bör beaktas att alla medarbetare som har behörighet till funktionsbrevlådan kan ta del av informationen.

SDK ger också en kostnadsbesparing avseende porton, kostnader för bud, mm.

# Vem ansvarar för införandet av SDK

Objektledare IT och Objektledare Verksamhet ansvarar för införandet av SDK inom sitt objekt. Till hjälp har objektledarna den här instruktionen och stöd från Nackas centrala förvaltning av SDK i objektet Kommungemensamma tjänster. Den centrala förvaltningen stöttar upp med kunskap, hjälper till att skapa funktionsbrevlådor, aviseringar och att lägga upp behörigheter. Den centrala förvaltningen ansvarar även för att kontrollera att verksamheterna under införandet genomför aktiviteter definierade i denna checklista. Kontakt med aktuella myndigheter kan också samordnas genom den centrala förvaltningen.

# Kartläggning av behov

Vid ett införande av SDK rekommenderar vi att ni börjar med att kartlägga hur behoven av att kommunicera känslig information med offentliga aktörer ser ut för att därefter kunna prioritera flöden för ett införande. Vi rekommenderar att kartlägga följande:

* Vilka offentliga aktörer (myndigheter, regioner och kommuner) utbyter verksamheten känslig information med?
* Vilken typ av information utbyts med respektive organisation?
* Finns det andra alternativ för kommunikation som tex SSBTEK, ENA, som t.om skulle ge ett mer strukturerat och snabbare utbyte av information än vad SDK ger?
* Uppskatta om det rör sig om små eller stora volymer i respektive informationsutbyte.
* Hur mycket tid läggs idag på informationsutbytet och skulle det förenklas med SDK?
* Vilka av identifierade organisationer och verksamheter har anslutit till SDK och vilka kommer ansluta i närtid?

Använd därefter svaren på ovan frågor för att prioritera vilka informationsutbyten som är aktuella för ett införande av SDK.

# Vilka organisationer är anslutna till SDK

SDK-meddelanden kan endast skickas till verksamheter som är anslutna till SDK. Ni behöver därför bevaka anslutningsläget för att bedöma när det skulle vara värt för er verksamhet att ansluta till SDK. Vilka aktörer som är anslutna och med vilka delar av sina verksamheten kan ni se i SDK Adressbok, där anslutna verksamheter finns registrerade med sina funktionsadresser. Adressboken finns på följande länk:

[Start - SDK Adressbok (digg.se)](https://sdk-prod.digg.se/addressbook/)

Vilka organisationer som är på gång att ansluta till SDK och vilka som anslutit kan man se på följande sida hos DIGG. Här kan man dock inte se vilka verksamheter inom organisationen som är ansluten utan det ser man som tidigare nämnts i adressboken:

[Vilka är anslutna till SDK? | Digg](https://www.digg.se/saker-digital-kommunikation/vilka-ar-anslutna-till-sdk)

Kontakta den centrala förvaltningen av SDK för att få ytterligare detaljer kring vilka som är på gång att ansluta till SDK och för att samordna kontakt med respektive offentlig aktör.

# Checklista för anslutning

Checklistan är tänkt som ett stöd till objektledarna under införande av SDK. Den är även den centrala förvaltningens redskap för att kontrollera att verksamheterna efterlever de krav som ställs på oss som deltagare i SDK-federationen. På så sätt är vi rustade för de revisioner som utförs av DIGG för att kontrollera efterlevnad av regelverket. Innan verksamheten får behörighet till sina funktionsbrevlådor behöver därför objektledarna redovisa för den centrala förvaltningen att de genomfört punkterna i checklistan.

## Informationssäkerhetsarbete

För att få ansluta till SDK måste verksamheten bedriva ett systematiskt informationssäkerhetsarbete enligt kommunens riktlinjer för informationssäkerhetsarbete. Det innebär att:

* Identifiera den information som kommer utbytas via SDK och genomföra en informationsklassning.
* Göra en riskanalys för användande av SDK
* Riskanalysen ska innehålla en åtgärdsplan för att minimera risker.
* Verksamheten ska arbeta aktivt med att vidta åtgärder enligt åtgärdsplanen.
* Verksamheten ska även vidta åtgärder för att minimera antalet incidenter och säkerställa att konsekvenser av incidenter minimeras.
* Arbetet med ovan ska dokumenteras och ses över årligen.

## Kontinuitetsplan

Verksamheten ansvarar för att ta fram en plan för hur verksamheten ska kunna bedrivas vid eventuella driftstörningar i SDK, en så kallad kontinuitetsplan.

## Arbetsrutin för bevakning av inkomna meddelanden

Verksamheten behöver upprätta en rutin för hur funktionsbrevlådorna i SDK ska bevakas. Rutinen ska dokumenteras.

Verksamheten ska utse personal med uppgiften att bevaka SDK-brevlådorna dagligen eller med den frekvens som verksamheten kräver. Avisering om inkomna meddelanden till SDK kan fås till medarbetarnas Outlook eller till arbetsgruppens TOPdesk. Den centrala förvaltningen hjälper till att ordna aviseringar.

## Arbetsrutin för gallring

Verksamheten behöver upprätta en rutin för hur gallring i SDK ska ske. Rutinen ska dokumenteras.

Gallring av meddelanden i SDK ska ske manuellt av verksamheten själva. Frågor att ta ställning till är vem i verksamheten som ska utföra gallringen? Är det handläggarna själva eller kanske en utsedd person? Hur länge ska meddelandena ligga kvar i SDK? Gallring behöver göras av både inkomna och utgående meddelanden och även utkast till meddelanden.

## Arbetsrutin för hantering av skyddad identitet

Verksamheten behöver upprätta en rutin för hantering av ärenden som berör skyddad identitet i SDK. Rutinen ska dokumenteras.

Det är upp till verksamheten att själva besluta om SDK ska användas för hantering av uppgifter som berör personer med skyddad identitet. Verksamheten bör tänka igenom för- och nackdelar säkerhetsmässig.

Att beakta vid beslut och utformning av arbetsrutin:

* SDK är säkrare än fax då endast behöriga personer kommer åt informationen i SDK.
* Alla personer med behörighet till gruppens funktionsbrevlåda i SDK kommer åt all information som skickas till gruppen. Det går inte att utföra loggkontroller på vilka personer som läst ett visst meddelande och det går inte att begränsa antalet personer som har behörighet att läsa ärenden som berör personer med skyddad identitet.
* Används SDK för hantering av ärenden som berör personer med skyddad identitet är rekommendationen att inte ange namn i meddelandet utan endast ange personnummer eller samordningsnummer.
* Som information till mottagande organisation ska avsändaren, i SDK-meddelandets fritextfält, ange om ärendet berör en person med skyddad identitet.

## Arbetsrutin för behörighetshantering

Verksamheten behöver utforma en arbetsrutin för hur behörigheter i SDK ska hanteras. Rutinen ska dokumenteras.

Vid införande av SDK hjälper den centrala förvaltningen till att ge arbetsgruppen behörighet till SDK.

Vid nyanställningar sker beställning till servicecenter av närmsta chef via en e-tjänst på servicecenters kundportal i TOPdesk. Diplom på genomförd utbildning ska bifogas beställningen.

När en anställd slutar på Nacka kommun avslutas behörigheten i SDK automatisk men om en person byter tjänst inom kommunen är det viktigt att chefen säkerställer att behörigheten till SDK avslutas genom att skicka en beställning till servicecenter med nämnd e-tjänst. För konsulter avslutas inte behörigheten automatiskt utan chefen måste beställa ett avslut av behörigheten hos servicecenter.

Skola och VSS måste även säkerställa att timanställda avslutas manuellt hos servicecenter.

Objektsförvaltningen ute i verksamheterna ansvarar för att regelbundet kontrollera att rätt personer har behörighet till SDK. Detta görs genom att begära ut en lista från den centrala förvaltningen på vilka personer på enheten som har behörighet till SDK för att därefter stämma av mot verksamheten.

**Utbilda användare**

Nya användare i SDK behöver gå en digital utbildning. Utbildningen tar ca 30 minuter och avslutas med ett test. Diplom från avklarad utbildning används som underlag vid begäran om behörighet som bevis på genomförd utbildning. Utbildningen finns på följande länk:

<https://nacka.infocaption.com/2699.guide>

Användarna kan utföra utbildningen helt på egen hand men en idé kan vara att under införandet av SDK samla arbetsgruppen till ett möte där man gemensamt går igenom gruppens arbetsrutiner kring SDK och därefter ger gruppen tid att utföra utbildningen.

## Skapa funktionsbrevlåda

Den centrala förvaltningen hjälper till att skapa funktionsbrevlådor i SDK och koppla kodord till brevlådan i SDK Adressbok. Verksamheten behöver besluta vilken beskrivning och vilka kodord som brevlådan ska ha i SDK adressbok. Kodorden ska vara en hjälp till andra organisationer att förstå vilken information som kan skickas till respektive funktionsbrevlåda. Gå in i SDK Adressbok för att se vilka kodord som finns fördefinierade. Även egna kodord kan skapas.

Det är verksamhetens ansvar att säkerställa att beskrivningar och kodord i SDK Adressbok är aktuella och korrekta. Om en brevlåda inte längre används ska centrala förvaltningen kontaktas omgående för borttag i SDK adressbok.

## Regler för incidenthantering

* Personuppgiftsincidenter kopplade till användande av SDK anmäls enligt kommunens ordinarie rutiner.
* Incidenter i form av driftstörningar och andra tekniska problem i SDK anmäls omgående till servicecenter.
* Även andra problem, så som att meddelanden ofta kommer till fel brevlåda eller att det är svårt att hitta en viss verksamhet i SDK adressbok behöver anmälas till servicecenter.

## Regler för användande av SDK

SDK-federationen har ett regelverk som vi som ansluten organisation behöver följa. Det är därför viktigt att verksamheter som ansluter till SDK efterlever följande punkter.

* Vid osäkerhet om mottagande organisations funktionsadress bör sändande organisation skicka ett frågemeddelande för bekräftelse av korrekt mottagande organisation innan personuppgifter överförs.
* Om en funktionsbrevlåda inte ska användas längre måste gruppen omgående begära borttag av funktionsbrevlådan från SDK adressbok genom att kontakta den centrala förvaltningen av SDK
* Verksamheten ska acceptera meddelandeöverföring från alla anslutna organisationer inom SDK.
* Verksamheten ska endast utbyta information via SDK som är kopplad till verksamheten, vilket innebär att exempelvis reklam eller spam inte är tillåtet.
* Mottagande organisation ska skyndsamt meddela sändande organisation vid felaktigt inkommet meddelande.
* SDK ska inte användas för att utbyta information som omfattas av gällande säkerhetsskyddslagstiftning, dvs information gällande Sveriges säkerhet.
* Verksamheten ska själva bedöma om SDK har tillräcklig nivå av säkerhet för att utbyta information med tilltänkta mottagare.
* Användarens åtkomst ska vara personlig och knuten till den enskilda användaren och får inte delas med andra.

**Sammanfattningsvis behöver verksamheten genomföra följande punkter under ett införande av SDK.**

* **Kartlägga behov**
* **Informationsklassa**
* **Utföra riskanalys**
* **Upprätta åtgärdsplan för risker**
* **Ta fram kontinuitetsplan**
* **Dokumentera rutin för bevakning av brevlådor**
* **Sätta upp eventuella aviseringar om inkomna meddelanden**
* **Dokumentera rutin för gallring**
* **Dokumentera rutin för skyddad identitet.**
* **Dokumentera rutin för behörighetshantering**
* **Kommunicera rutiner till arbetsgruppen**
* **Definiera funktionsbrevlådor**
* **Utbilda användare**
* **Beakta regler för användande av SDK**
* **Redovisa uppfyllnad av punkter i checklista till centrala förvaltningen**
* **Ordna behörighet till användare**

# Förvaltning av SDK

## Verksamhetsnära förvaltning

Efter införandet av SDK behöver lösningen förvaltas. Då SDK är en tjänst som används av hela kommunen ligger huvudansvaret för förvaltningen i objektet “Kommungemensamma tjänster”. Dock behöver verksamheten (i det verksamhetsnära objektet) ansvara för att följande förvaltningsaktiviteter utförs:

* Regelbundna kontroll av behörigheter
* Regelbundna kontroll av utförd gallring
* Säkerställa att arbetsrutiner kring SDK är uppdaterade
* Säkerställa att verksamhetens funktionsbrevlådor i SDK Adressbok är aktuella och uppdaterade.
* Ansvara för införande av ytterligare verksamhetsfunktioner i SDK

## Central förvaltning

Huvudansvaret för förvaltningen av SDK ligger i det centrala objektet Kommungemensamma tjänster. Objektet ansvarar för följande:

* Stötta verksamheterna med information om SDK
* Säkerställa framdrift av införanden av SDK
* Kontrollera att verksamheten efterlever DIGGs regelverk
* Kontakt med andra myndigheter kring SDK
* Underhålla SDK adressbok
* Lägga upp behörigheter vid införanden
* Underhålla digital utbildning och lathund
* Felanmälan till driftleverantör, tjänsteleverantör och DIGG
* Underhålla tekniska plattformen
	+ Uppgradera tjänsten
	+ Felsökning och test

## Servicecenter

Servicecenter har följande uppgifter kopplade till SDK:

* Behörighetshantering
* Kontrollera att nyanställda har utfört utbildning
* Ta emot felanmälningar från användare
* Lyfta felanmälningar till den centrala förvaltningen

# Kontaktuppgifter till den centrala förvaltningen:

Den centrala förvaltningen av SDK ligger i objektet Kommungemensamma tjänster.

Objektledare: Monica Enderstein, monica.enderstein@nacka.se

Objektspecialist: Malin Borgström, malin.borgstrom@nacka.se

Objektspecialist: Sebastian Malmberg, sebastian.malmberg@nacka.se

# Ytterligare information om SDK

Digital utbildning i SDK:

 <https://nacka.infocaption.com/2699.guide>

Lathund:

https://www.nacka.se/497043/globalassets/medarbetare/digitaliseringit/dokument/digiakademin/sdk/lathund-sdk-nacka-kommun-version-1.0.pdf

 Nacka kommuns systemsida:

[Säkra meddelanden | Nacka kommun](https://www.nacka.se/medarbetare/digitalisering/stod-for-medarbetare/jobba-sakert/sakra-meddelanden/)

DIGG:s websida:

[Säker digital kommunikation (SDK) | Digg](https://www.digg.se/digitala-tjanster/saker-digital-kommunikation-sdk)