

B1.4.6 – SAD Säker digital kommunikation

Dokumentationen utgör dels en övergripande beskrivning av lösningsarkitekturen för federationen Säker digital kommunikation (SDK), dels grund för lösningar som tas fram som stödjer federationen.

1. Inledning

1.1 Bakgrund

Tidigare årsarbeten med SDK har visat att behoven går att realisera tekniskt baserat på EU:s ramverk CEF eDelivery, se ref R6, samt kompletterande specifikationer och anvisningar som finns i federationen SDK. Exempel på dokumentation är regelverk för deltagarorganisationer inom SDK, it-säkerhetsbilaga och intygan om överensstämmelse framtaget för deltagarorganisationer.

Federationen Säker digital kommunikation (SDK) består bl a av ramverk, regler, rutiner specifikationer och beskrivningar och viss gemensam infrastruktur vid informationsutbyte mellan regioner, kommuner, statliga myndigheter och privata utförare av offentligt uppdrag.

Under 2015 och 2016 har flera behovsanalyser hos kommuner, regioner, privata vårdutförare respektive statliga myndigheter visat på ett stort behov av säker digital kommunikation. Idag sker informationshanteringen mellan aktörerna till stor del manuellt, med fax, brev, telefon och e-post, därför att det saknas alternativ. Det tar tid, driver kostnader och skapar osäkerhet.

Det finns bland annat stora behov inom hälso- och sjukvård, socialtjänst och skola. Behovsbilden har ytterligare konkretiserats i projektets etableringsfas hösten 2017, och aktörerna har konstaterat att behoven bygger på att:

- Informationen är känslig men ej av sådan karaktär att den avser rikets säkerhet.
- Informationen ska kunna gå över öppet nät.
- Informationen ska kunna vara ostrukturerad, för att kunna ersätta dagens fax, fysiska brev och telefonsamtal kan inte krav ställas på innehållets struktur.
- Kommunikationen ska kunna ske mellan funktionsbrevlådor som möjliggör meddelandeutbyte från en handläggare hos sändande part till en annan handläggare hos mottagande part.
- Kommunikerande parter ska kunna hitta säkra adressater, skicka, ta emot, och få kvittens på att ett meddelande överförts.
- Förutsättningarna ska vara samma för offentliga aktörer och privata utförare av offentligt uppdrag.

- Parterna ska kunna ansluta till en federation enligt fastställda regelverk utan att bilaterala överenskommelser ska behövas mellan alla olika parter.

SDK är ett samarbetsprojekt mellan Sveriges kommuner, regioner och myndigheter som har pågått sedan 2017. SDK har tagits fram av Digg och Inera i samarbete med Sveriges Kommuner och Regioner (SKR) samt enskilda kommuner, regioner och andra myndigheter.

1.2 Syfte

Säker digital kommunikation syftar till att skapa förutsättningar för en säker och enhetlig hantering av känslig information vid överföring av digitala meddelanden mellan aktörer i offentlig sektor.

Säker digital kommunikation ger följande vinster för både verksamheter och handläggare:

- ökad trygghet genom att inte personlig eller känslig information sprids till obehöriga
- snabbare handläggning och beslut
- samma spårbarhet oavsett verksamhet

1.3 Dokumentation SAD

SAD utgör dels en övergripande beskrivning av lösningsarkitekturen för federationen Säker digital kommunikation (SDK), dels en grund för lösningar som tas fram som stödjer federationen.

1.4 Om dokumentet

Dokumentet syftar till att beskriva den övergripande lösningsarkitekturen för federationen för Säker digital kommunikation.

Då arkitekturen i grunden är ett ramverk med specifikationer och standarder där samverkande delsystem tillsammans utgör hela systemlösningen, syftar detta dokument främst till att beskriva ramverket, hur samverkan sker mellan delsystemen, samt vilka ytterligare profileringar med tillhörande specifikationer som är framtagna för just syftet Säker digital kommunikation.

För ingående delsystem finns möjligheter att välja olika färdiga programvaror, eller att utveckla/anpassa programvaror, så länge dessa följer ramverksregler, gränssnittsspecifikationer osv. Dokumentet har därför inte fokus på att beskriva intern mjukvarurealisering av delsystem/komponenter.

I dokumentet beskrivs arkitekturen primärt utifrån vyerna:

- Användningsfallsvy - Arkitekturellt drivande användningsfall utifrån den grundläggande funktionalitet som ramverket tillhandahåller, och vilka delsystem som interagerar med varandra i respektive fall (kap. 4).
- Logisk vy - Logisk arkitekturell vy över den tekniska lösningen med ingående delsystem, deras respektive roller och gränsyterna dem emellan. Arkitekturens mål, drivande krav och arkitekturellt speciellt signifikanta delar beskrivs (kap. 2 och 3).

- Säkerhetsvy - Säkerhetskrav och säkerhetsmekanismer för den övergripande lösningsarkitekturen (kap. 6).
- Informationsvy - Hantering av information vid användning av federationen
Säker digital kommunikation, informationsmodeller och specifikationer för meta- och adressinformation (kap.7).

1.5 Målgrupp

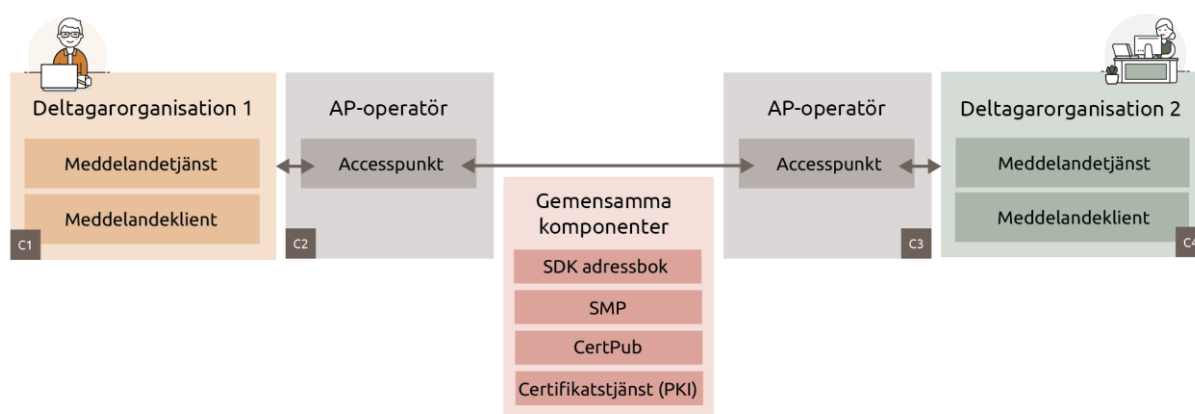
De huvudsakliga målgrupperna för detta dokument är:

- Integratörer
- Leverantörer av meddelandetjänster/applikationer
- Systemägare
- Systemförvaltare
- Systemarkitekter
- Utvecklingsteam
- Arkitekturstödsfunktioner

1.7 Termer och förkortningar

Termer och förkortningar inom SDK hittar i SDK-ordlista, se A1.6.

2. Arkitekturell översikt



Figur. Arkitekturell översikt - Säker digital kommunikation.

Den arkitekturella ansatsen för Säker digital kommunikation är att etablera ett gemensamt ramverk för säkert meddelandeutbyte baserat på standarder i så stor utsträckning som möjligt. Till ramverket ska det vara möjligt att ansluta meddelandetjänster med meddelandeklienter som användarens gränssnitt.

Anslutna meddelandetjänster kan kommunicera med varandra genom standardprotokoll, en överenskommen profilering av dessa protokoll, samt en gemensam innehållsspecifikation för själva meddelandet. Meddelandetjänsterna ansluts via s.k accesspunkter som ansvarar för att göra tekniska vägval och utföra säker robust transport till mottagande organisations accesspunkt.

Mottagarens meddelandetjänst hämtar mottagna meddelande från dess accesspunkt och gör meddelandet tillgängligt till behöriga användare i meddelandeklient. Själva meddelandeöverföringen är asynkron, vilket innebär att meddelandetjänsten kan sända meddelandet utan att behöva vänta på att få ett svar tillbaka från mottagarens system. Meddelandekvittensen skickas som ett separat meddelande tillbaka till avsändande meddelandetjänst, som sedan kan läsa av kvittensen alternativt visa larm om meddelandet inte kvitterades.

Den asynkrona modellen ger stöd för att köa meddelanden hos avsändande respektive mottagande system, för både själva transporten och de valideringssteg som behöver utföras.

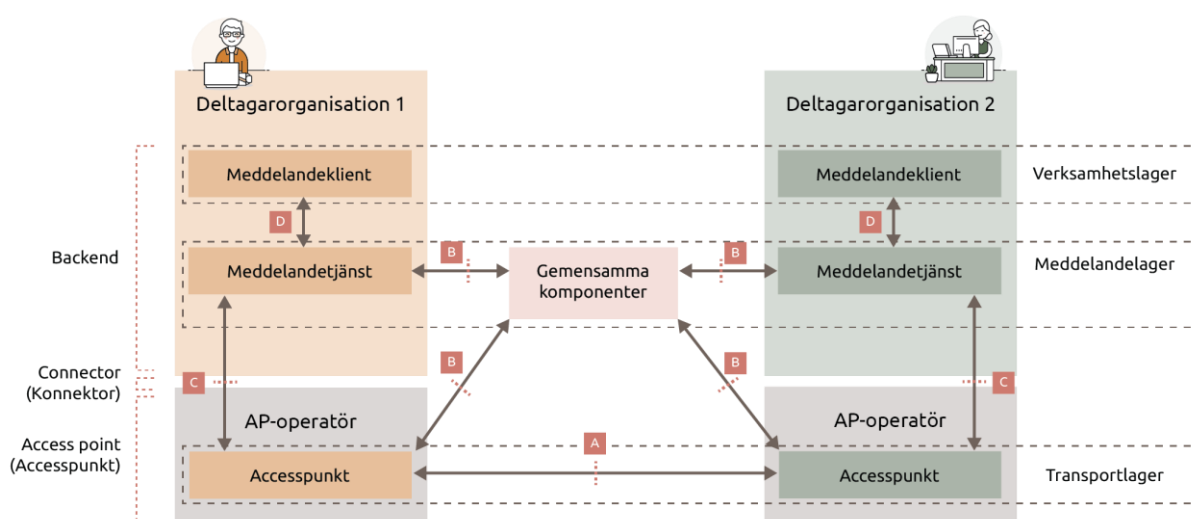
Det ingår även viss nödvändig gemensam infrastruktur i lösningen:

- För att etablera tilliten till transportinfrastrukturens AP-operatörer, behövs en betrodd certifikatsutgivare (CA) och en reglerad hantering av denna, se avsnitt 7.4 Säkerhetsmekanismer. Utgivna certifikat används för att realisera säkerhetsmekanismer som transportkryptering, e-stämpling av försändelse, AS4-meddelandekryptering mot mottagande accesspunkt.
- För att etablera tilliten till deltagarorganisationer behövs betrodda certifikatsutgivare (CA) och en reglerad hantering av dessa, se avsnitt 7.4 Säkerhetsmekanismer. Utgivna certifikat används för att realisera säkerhetsmekanismer på meddelandenivå såsom meddelandekryptering och signering. Meddelandekryptering och signering tillämpas mellan deltagarorganisationer.
- En Certifikatpubliceringstjänst (CertPub) som innehåller deltagarorganisationers publika nyckel för att möjliggöra meddelandekryptering och signering, sk. organisation till organisation kryptering/signering (O2O-certifikat).
- En källa till adressuppgifter (SDK adressbok) för de parter som kan kommunicera med varandra. Källan uppdateras av respektive deltagarorganisation, se nedan under Adresseringsmodell.
- En metadatatjänst (SMP) som innehåller tekniska uppgifter om var de olika tjänsterna för meddelandeutbyte finns (teknisk ändpunkt för leverans av meddelande), vad de tekniskt stödjer (meddelandeformat, version etc), samt vilka certifikat som mottagande accesspunkt använder.

I den referensmodell, se figur nedan figur, för meddelandeöverföringen som tagits fram finns följande huvudsakliga logiska komponenter/lager:

- **Meddelandeklient** (Verksamhetslager): hanterar gränssnittet mot användaren, hanterar koncept som "brevlåda", säker inloggning, behörighetsstyrning, besvara meddelande, konversationer (meddelandetrådning) osv.

- **Meddelandeklienten** har det primära ansvaret för lagring av inkomna och skickade meddelanden, men ansvaret kan vara delegerat till en annan tjänst för lagring.
 - Representerar en funktionsadress
 - Ansvarar för att adressera meddelandet
 - Ansvarar för att skapa och presenterar meddelanden
 - Presenterar skickade meddelande samt dess meddelandestatus/kvittens meddelande
 - Lagrar meddelanden
- **Meddelandetjänst** (Meddelandelager/meddelandeväxel): ansvarar för kryptering/dekryptering och signering/validerar signatur samt hanterar själva meddelandeöverföringen, hämta och lämna meddelanden hos accesspunkten (AP-operatör), validering av utgående/inkommande meddelanden, vid behov inom organisationen styra meddelande till rätt meddelandeklient (intern routing), svarstidsbevakning och ge stöd för omsändning av meddelandet om tidigare försök misslyckats. Meddelandetjänst integrerar med accesspunkt via gränsyta C (ej standardiserat tekniskt gränssnitt).
- **Accesspunkt** (Transportlager): hanterar extern säker kommunikation med andra parter (gränsyta A), validering och säker kvittens på transportnivå samt teknisk adressering för att nå mottagarens accesspunkt. Säkerställer insyns- och integritetsskyddad transport via kryptering, e-stämpling av försändelse och kontroll av certifikat och stämplat.
- **Gemensamma komponenter**: realiserar tjänster (gränsyta B) för adressering till organisation och funktion inom organisation, certifikatshantering, metadata om var de olika tjänsterna för meddelandeutbyte finns och vad de tekniskt stödjer.



Figur. Referensmodell för säker meddelandeöverföring.

Uppdelningen i dessa skikt och komponenter ger bl.a. följande möjligheter (där koppling till SDK arkitekturella mål, enligt avsnitt 2.1 nedan, anges inom parentes):

- Gränssytor A, B, C, D mellan komponenterna kan specificeras för att kunna samverka med olika produkter och lösningar på marknaden (arkitekturellt mål "Öppenhet och standarder"). Läs mer om gränssytor under avsnitt "6. Teknisk lösning".
- En organisation kan ha flera meddelandeklienter, t.ex. ett ärendesystem som hanterar meddelanden för en del av organisationen, och en meddelandeklient som renodlat hanterar säkra meddelanden (arkitekturellt mål "Eget ansvar för intern arkitektur och val av verktyg").
- Meddelandetjänster kan göras mer generiska och klara flera olika typer av transportlager (arkitekturellt mål "Öppenhet och standarder").
- Byte av realisering av transportlagret kan göras utan att behöva påverka övriga lager (arkitekturellt mål "Öppenhet och standarder").
- Deltagande parter kan nå adressuppgifter om alla andra deltagande parter baserat på den organisation och funktion som parten vill nå (arkitekturellt mål "Gemensamma begrepp, modeller och mönster" och "Använd strukturerad information i processen").
- Deltagande accesspunkter kan få aktuella tekniska uppgifter om mottagarens motsvarande tjänster via metadata och behöver inte uppdateras på annat sätt vid t.ex. byte av tekniska adresser.

I den framtagna lösningen utgörs transportlagret och delar av de Gemensamma komponenterna av eDelivery, ett byggblock framtaget av EU:s organisation Connecting Europe Facility (Se "R5 Connecting Europe Facility (CEF)"). Dessa byggblock realiseras av Myndigheten för digital förvaltning (Digg). Mer om detta under avsnitt Teknisk lösning.

2.1 Arkitekturella mål

Federationen Säker digital kommunikation utgår utifrån följande arkitekturella mål:

- Följsamhet mot Svenskt ramverk för digital samverkan (se Ref S1).
 - Digitala kanaler ska vara det primära alternativet, öka medborgarnas insyn och möjligheter att påverka. Det ska vara lätt att använda det säkra digitala kommunikationsalternativet för att kommunicera säkert med myndigheter och andra inblandade aktörer.
 - Öppenhet och standarder – öppna upp för externa innovatörer genom att använda öppna standarder. Basera en gemensam lösning på öppna specifikationer och gränssnitt, oberoende av specifik leverantör eller produkt. Skapa goda förutsättningar för marknaden att leverera lösningar kompatibla med säker digital kommunikation. Detta ger hög interoperabilitet.
- Rätt nivå på informationssäkerhet och integritet
 - Tillämpa informationssäkerhet riskbaserat för att få en bra balans mellan risk och skydd.

- Privacy-by-design - bygg in skyddsmekanismer genom hela kedjan från början
- Skapa god tillit till lösningen genom att via tekniska lösningar och regelverk möta kraven på konfidentialitet, riktighet, spårbarhet och tillgänglighet.
- Gemensamma begrepp, modeller och mönster. Ta fram en överenskommen och tydlig specifikation för sådant som kommunikationsmönster, organisationsidentiteter, adresseringsinformation, och meddelandets metainformation/struktur.
- Använd strukturerad information i processen
 - Enligt framtagna behovsbild för SDK ska informationen som överförs kunna vara ostrukturerad; för att kunna ersätta dagens fax, fysiska brev och telefonsamtal kan inte krav ställas på innehållets struktur som sådan. Däremot struktureras metainformation för meddelandet enligt en innehållsspecifikation, såsom avsändare, mottagare, identifierare, interna och externa referenser osv. Lösningen baseras på en infrastruktur som klarar av att också överföra strukturerad information, vilket ger möjlighet att utnyttja infrastrukturen även för mer strukturerade informationsutbyten.
- Eget ansvar för intern arkitektur och val av verktyg
 - Införande av säker digital kommunikation ska inte utgå ifrån att organisationerna ska behöva bygga om sin interna IT-arkitektur.
 - Det ska vara möjligt att göra anpassningar i existerande lokala lösningar för att ansluta till säker digital kommunikation.
- Tillgängliggör och återanvänd information och tjänster på ett enhetligt sätt
 - I den för lösningen nödvändiga gemensamma infrastrukturen gäller att gemensamma specifikationer och standarder förvaltas över tid (governance), och stödjande gemensamma IT-förmågor behöver upprätthållas.

2.2 Prioriterade områden

- Definiera en referensmodell för säker meddelandeöverföring inkl de flöden som behövs för en robust hantering av meddelanden.

- Ge verksamheter möjlighet till att registrera och använda säkra och aktuella adressuppgifter till organisationer och funktioner
- Sätta en standard och specifikationer som ger förutsättning för samverkan mellan olika leverantörer/produkter för säker meddelandehantering.
- Sätta en säkerhetsmodell med säkerhetsmekanismer som motsvarar de krav som ställs på informationssäkerheten, och har möjlighet att anpassas till förändrade krav inom IT-säkerhet.

3 Följsamhet till arkitektoniska principer

Denna SAD har inspirerats av "R1 RIV - regelverk för interoperabilitet inom vård och omsorg (Inera)", inom vilket T-boken är kortnamnet på RIV Teknisk Referensarkitektur. SDK som sådant har ett bredare nationellt perspektiv där alla offentliga aktörer och deras utförare ska kunna ingå, och har därför följt nationella riktlinjer och vägledningar. Nedan har ändå beskrivits följsamhet till delar av T-bokens styrande principer eftersom de flesta av dessa är av generell karaktär.

IT2: Informationssäkerhet	
Förutsättningar att uppfylla	Uppfyllnad
Verksamhetskritiskt IT-stöd designas för att möta verksamhetens krav på tillgänglighet vid frånfall av ett externt beroende. Ju fler beroenden till andra komponenters tillgänglighet, desto lägre egen tillgänglighet.	<p>Framtagen referensmodell för säker meddelandeöverföring bygger på en s.k. 4-hörningsmodell, där meddelandeöverföringen inte behöver passera centrala noder, utan kan gå direkt mellan organisationers accesspunkter (via AP-operatör), och vidare till verksamhetssystemen.</p> <p>Överföringen är asynkron med köhantering och omsändning vid tillfälliga fel i infrastrukturen, vilket skapar goda förutsättningar för en för användaren upplevd god tillgänglighet för systemet. Se vidare Asynkront meddelandeflöde.</p> <p>Viss gemensam infrastruktur används för att erhålla adressinformation, metadata om mottagarens system samt spärrinformation om</p>

	<p>certifikat. Gemensamma komponenter tillhandahålls med hög tillgänglighet. Systemet tål dock tillfällig otillgänglighet även för dessa komponenter, eftersom meddelanden köas i accesspunkterna och automatiska omsändningsförsök kan ställas in.</p> <p>Det är även tekniskt möjligt att använda tidigare (eller på annat sätt) erhållna adress- och metadata till mottagaren, för att skicka till en mottagares accesspunkt. En accesspunkt kan cacha sådana data för mottagare som den tidigare skickat till.</p> <p>Detta kräver dock att den aktuella accesspunktsprogramvaran kan konfigureras för detta.</p> <p>Viktiga komponenter i lösningen bör hanteras med flera kluster per tjänst, t.ex. accesspunkter och metadatatjänst.</p>
Verksamhetskritiska gemensamma stödtjänster (t.ex. tillgång till behörighetsstyrande information) erbjuder möjlighet till lokala instanser som med tillräcklig aktualitet hålls uppdaterade med gemensam master.	<p>En accesspunkt kan cacha data den hämtat för mottagare som den tidigare skickat till.</p> <p>Ansvarig för transportinfrastrukturen (Digg) reglerar transportinfrastrukturens grund-SLA samt hur Accesspunkter konfigureras gällande cache.</p>
Krav mellan integrerade parter måste regleras, informationsägaren ska godkänna att ett visst system får agera mot informationen genom ett visst integrationsgränssnitt och meddelandetyper.	Anslutning av deltagarorganisationer till SDK-federationen regleras i Beskrivning och anslutningsavtal för Säker digital kommunikation, inklusive regelverk med styrande bilagor.
Arkitekturen måste möjliggöra tillräcklig tillgänglighet vid flera samverkande system.	Se svar ovan.
En sammantagen tolkning av tillämpliga lagar och förordningars konsekvenser för teknisk	Se kapitel 6 Säkerhet.

realisering av informationsfångst, utbyte och lagring.	
Förutsättningar för spårbarhet etableras i form av loggningsregler för komponenter som deltar i säkert informationsutbyte.	Se avsnitt 6.6 Spårbarhet.
Interoperabla, internationellt beprövade och för leverantörer tillgängliga standarder tillämpas för kommunikation mellan parter som har upprättat tillit.	<p>Lösningsskonceptet bygger i grunden på CEF eDelivery (EU-kommisionens byggblock för säkra meddelande), vilken i sin tur bygger på öppna etablerade standarder som t.ex. OASIS AS4.</p> <p>Se vidare avsnitt Teknisk lösning.</p> <p>Säkerhetsmekanismerna bygger på samma sätt på väl etablerade öppna standarder, se vidare kap. Säkerhet</p>

IT3: Nationell funktionell skalbarhet	
Förutsättningar att uppfylla	Uppfyllnad
Nationella meddelandetyper med nationell täckning som funktionell omfattning. Det får inte finnas underförstådda funktionella avgränsningar till regioner, kommuner eller andra organisatoriska avgränsningar i nationella meddelandetyper.	<p>Lösningsskonceptet omfattar ett antal gemensamma meddelandetyper och APIer.</p> <ul style="list-style-type: none"> • adresseringsinformation, söka och publicera. • certifikatsinformation för kryptering och signering av meddelanden. • metadata om tekniska tjänster att skicka meddelanden till. <p>Det finns inga tekniska eller organisatoriska begränsningar för anslutande IT-system att använda integrationsprofilerna. Se vidare avsnitt 6.2.1.</p>
SLA ska definieras för tjänster och komponenter. Dessa SLA ska ta hänsyn till framtida kapacitet för avseende på	SLA krav finns definierade för alla gemensamma (Diggs transportinfrastruktur

transaktionsvolym, variationer i användningsmönster och krav på tillgänglighet, i kombination med förmåga till kontinuerlig förändring.	och SDK federationen) tjänster samt deltagarorganisationens lokala tjänster.
System och e-tjänster som upphandlas kan utökas med fler organisationer som kunder utan krav på infrastrukturella ingrepp (jämför s.k. SaaS, Software as a Service)	Ingående delar kan om så önskas logiskt delas mellan organisationer, t.ex. kan en leverantör erbjuda att dela en accesspunkt logiskt för flera organisationer.

IT4: Lös koppling	
Förutsättningar att uppfylla	Uppfylld
Meddelandeutbyte baseras på att kommunikation etableras utgående från vem som äger informationen som ska konsumeras eller berikas, inte vilket system, plattform, datalager eller tekniskt gränssnitt som informationsägaren för stunden använder för att hantera informationen. Genom centralt administrerad förmedlingstjänst skapas lös koppling mellan informationskonsument och informationsägarens tekniska lösning.	Lösningsskonceptet stödjer lös koppling via dynamisk adressering (Dynamic discovery) där avsändande part kan hitta mottagande organisations tekniska tjänst och dess kapabiliteter enbart baserat på mottagande parts organisationsidentitet, samt vetskap om vilket typ av meddelandeutbyte som ska göras. Detta möjliggörs genom de gemensamma stödtjänsterna Lokaliseringstjänst (SML) och Metadatatjänst (SMP). Se SML och SMP.
En arkitektur som skapar lös koppling mellan konsumenter och producenter, avseende adressering och standarder för kommunikation.	Lös koppling avseende adressering stöds (se svar på föregående). Lös koppling mellan sändande och mottagande parter IT-system skapas genom integrationsarkitekturen i eDelivery som bygger på att integration sker genom accesspunkter och användande av öppna standarder. Se vidare Teknisk lösning.
Nationella meddelandetyper förvaltas i en nationellt koordinerad förvaltning.	De gemensamma meddelandetyper som ingår i lösningen förvaltas nationellt av Digg.
För en process kan flera meddelandetyper ingå. Därför är det viktigt att alla meddelandetyper baseras på en gemensam referensmodell för informationsstruktur.	Processer kan spänna över flera verksamhetsdomäner

	<p>Kommunikationen baseras på en gemensam standardiserade dokumenttyper.</p> <p>En gemensam referensmodell saknas.</p>
<p>Befintliga system behöver anpassas till nationella meddelandetyper och APIer. Detta kan göras av leverantörer direkt i produkten, eller genom fristående integrationskomponenter ("anslutningar"). En anslutning bör ligga nära (logiskt vara en del av) det system som ansluts, oavsett om det är i rollen som konsument eller producent för anslutningen som genomförs.</p>	<p>Detta stöds, men är också upp till produktleverantör / part eller motsvarande att avgöra exakt hur produkten anpassas till de gemensamma integrationsprofilerna. I arkitekturen kan sk. konnektorer byggas för att göra anpassningar där behov finns.</p>
<p>Interoperabla standarder för meddelandebutbyte tillämpas, så att integration med till exempel en Web Service kan utföras utan att anropande system behöver tillföras en för tjänsteproducenten specialskriven integrationsmodul (s.k. agent).</p>	<p>Lösningsskonceptet bygger på användande av öppna globala standardprotokoll mellan sändande och mottagande parter IT-system via integrationsarkitekturen i eDelivery. Integration sker via accesspunkter som följer standarder enligt eDelivery-ramverket. Se vidare Teknisk lösning.</p>

IT5: Lokalt driven e-tjänsteförsörjning	
Förutsättningar att uppfylla	Uppfyllnad
<p>Minsta möjliga, men tillräcklig, mängd standarder och stödjande gemensamma grundbultar för nationella e-tjänstekanaler säkerställer att även utvecklingsenheter i mindre organisationer kan bidra med e-tjänster för en integrerad användarupplevelse och att en gemensam back-office för anslutning av huvudmän till e-tjänster finns etablerad. I den mån etablerade standarder med bred tillämpning i kommersiella e-tjänster finns (t.ex. för single-sign-on), bör de användas i syfte att möjliggöra upphandling av hyllprodukter.</p>	<p>För realisering av accesspunkt, meddelandetjänst, meddelandeklienter och tjänster ges möjlighet att använda etablerade branschstandarder/vanligt förekommande teknologier.</p>

<p>Utveckling sker mot globalt dominerande portabilitetsstandarder i de fall mellanvara, applikationsservrar, tillämpas. Det är möjliggöraren för nyttjande av free-ware och lågkostnadsverktyg i organisationer som inte orkar bära tunga licenskostnader för komplexa utvecklingsverktyg och driftsplattformar.</p>	<p>För realisering av meddelandeklienter och tjänster ges möjlighet att använda etablerade branschstandarder/vanligt förekommande teknologier.</p> <p>För gemensamma tjänster gäller att hela teknikstacken, inklusive infrastruktur, utvecklingsverktyg etc. om möjligt bygger på öppen källkod och etablerade komponenter, och kan användas utan kommersiella licenser.</p>
<p>Nationell (eller regional, beroende på sammanhang vård/omsorg) förvaltning är etablerad (t.ex. s.k. Portal Governance), med effektiva processer för att införliva lokalt utvecklade e-tjänster i nationella e-tjänstekanaler. Systematisk och effektiv allokering av resurser för drift är en viktig grundförutsättning.</p>	<p>SDK Federationens gemensamma komponenter förvaltas av Digg. Lokala komponenter så som Accesspunkt integreras via standardiserat förfarande.</p>
<p>Genom lokal governance och tillämpning av det nationella regelverket får lokala projekt den stöttning som behövs för att från början bygga in förutsättningar för integration i samordnade (t.ex. nationella) e-tjänstekanaler.</p>	<p>Federationsägaren (Digg) stödjer deltagarorganisationers anslutning till SDK federationen. OPEN-TEST tillhandahålls till leverantörer som önskar anpassa och verifiera sin mjukvara enligt federationens specifikationer.</p>

IT6: Samverkan i federation	
Förutsättningar att uppfylla	Uppfyllnad
<p>Att gemensamma gränssnitt i alla federativa utbyten finns framtagna och beskrivna, vilket möjliggör kostnadseffektiva och leverantörsneutrala lösningar.</p>	<p>Integration sker via standardbaserade accesspunkter och användande av öppna globala standarder.</p> <p>Gemensamma integrationsprofiler för gemensamma komponenter, innehållsspecifikation för meddelanden osv, är öppna och centralt förvaltade.</p> <p>Se vidare avsnitt 5, Teknisk lösning.</p>

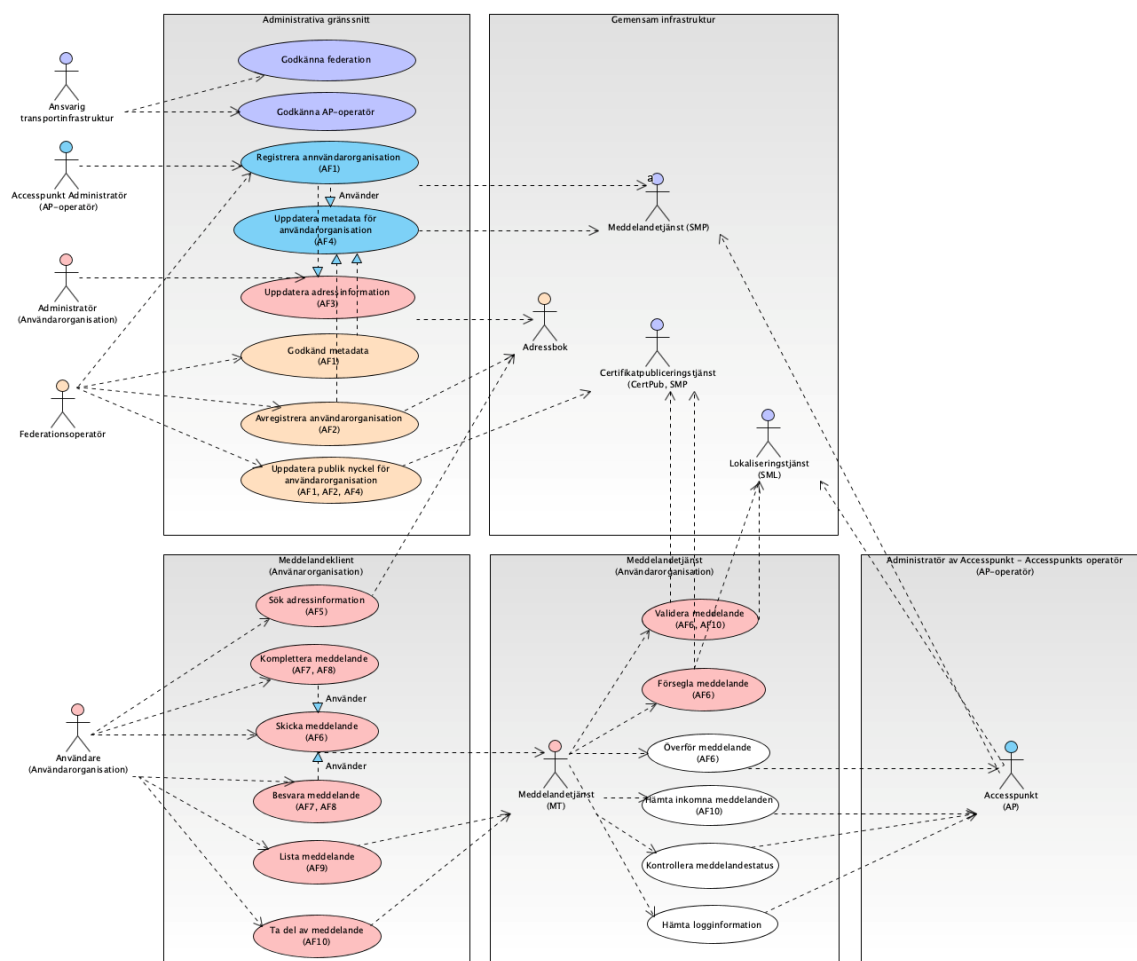
<p>Det behövs organ och processer för att godkänna utgivare av elektroniska identitetsintyg och certifikat som är giltiga i federationen.</p>	<p>Utgivare av elektroniska certifikat som är giltiga i federationen regleras av regelverk för deltagarorganisationer.</p>
<p>Aktörer i olika nät, inklusive öppna nät ska vara välkomna i elektronisk samverkan genom att samverkande komponenter är säkra.</p>	<p>Konceptet bygger på att i princip alla nätverk som har förbindelse med internet ska kunna användas. Säkerheten ligger inte i det fysiska nätverket, utan i ovanliggande protokoll/lager.</p>
<p>Att Ingående parter i federationen är överens om ett antal gemensamma ståndpunkter:</p> <ul style="list-style-type: none"> · att stark autentisering likställs med 2-faktors autentisering · att vid samverkan acceptera följande metoder för stark autentisering; eID, PKI med lagring av nyckelpar på SmartCard eller motsvarande och metoder baserade på engångslösenord, antingen genererade i en fysisk enhet eller säkert distribuerad till fysisk enhet · att tillämpa en gemensam certifikat- och utfärdarpolicy, likvärdig med SITHS, som ett minimikrav för egen eller annans PKI · att sträva mot en autentiseringslösning, framför flera olika, för att realisera stark autentisering i den egna organisationen och i federation · att tillämpa ett gemensamt ramverk för att ingå i en federation · att sträva mot att all gränsöverskridande kommunikation skall vara över Internet. Det är den egna organisationen som beslutar vilken 	<p>Samverkan regleras i ett gemensamt regelverk för anslutning.</p> <p>Bland annat regleras godkända certifikatutfärdare, tillitsnivå för autentiseringen och utfärdande av elektronisk identitetshandling till användare.</p> <p>Inriktningen är inte att styra på exakt vilka tekniska lösningar som organisationer använder vad gäller t.ex. stark autentisering av slutanvändaren, utan istället kravställs på en minsta accepterad tillitsnivå för den lösning för autentisering man använder i sin organisation. De tillitsnivåer som tillämpas är förankrade i det svenska ramverket som Myndigheten för digital förvaltning (DIGG) förvaltar.</p> <p>Den gränsöverskridande kommunikationen är nätverksneutral, alla nätverk som har förbindelse med internet ska kunna användas. Säkerheten ligger inte i det fysiska nätverket, utan realiserar i ovanliggande protokoll/lager.</p> <p>En organisations integration med SDK-lösningen kanaliseras via en integrationsinfrastruktur, en s.k. Accesspunkt, med möjlighet till övervakning och kontroll av trafikflödet organisationen deltar i.</p>

<p>tillgänglighet som är tillräcklig för anslutningen</p> <ul style="list-style-type: none"> · att sträva efter att möjliggöra kontroll av trafik till och från den egna infrastrukturen i en eller få kontrollpunkter · Att utgå från att kommunikation över Internet har ett likvärdigt skyddsbehov 	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

4. Användningsfall

Här beskrivs systemet ur ett funktionellt perspektiv i form av en användningsfallmodell i syfte att lyfta fram de funktionella krav som är drivande för arkitekturen. I detta kapitel förekommer termer och begrepp som beskrivs mer utförligt i senare delar av dokumentet.

4.1 Användningsfall - översikt



Figur. Användningsfallsöversikt. Bilden illustrerar övergripande användningsfall som är drivande för arkitekturen i SDK. Bildens innehåll beskrivs i efterföljande tabell.

Grundläggande användningsfall riktade mot slutanvändare, dvs användare och administratörer framgår av nedanstående tabell.

AF	Namn	Beskrivning
AF1	Registrera deltagarorganisation	<p>AP-operatör registrerar deltagarorganisationens metadata i Metadatatjänst.</p> <p>Federationsägaren godkänner deltagarorganisation för deltagande i SDK-federationen.</p>

		<p>Resultat: En registrerad deltagarorganisation är tekniskt förberedd för att skicka och ta emot meddelanden till/från övriga registrerade deltagarorganisationer. Tillhörande metadata för kommunikationen, certifikat samt adressuppgifter är registrerade.</p>
AF2	Avregistrera deltagarorganisation	<p>Avregistrering av deltagarorganisation.</p> <p>AP-operatör</p> <p>avregistrerar deltagarorganisationen från Metadatatjänst.</p> <p>avregistrerar deltagarorganisationen från Accesspunkt.</p> <p>Federationsoperatör</p> <p>godkänner avregistrering i Metadatatjänst.</p> <p>avregistrerar deltagarorganisation i SDK adressbok.</p> <p>Resultat: En avregistrering innebär att deltagarorganisationen inte längre kan skicka / ta emot meddelanden inom SDK-federationen.</p>
AF3	Uppdatera adressinformation för deltagarorganisation	<p>Administrera adressinformation för deltagarorganisation.</p> <p>Utförs primärt av deltagarorganisationen själv via behörig administratör i deltagarorganisationen.</p>

AF4	Uppdatera metadata för deltagarorganisation	<p>Deltagarorganisationens metadata, vilken styr organisationens kommunikationsmöjligheter i SDK-federationen.</p> <p>Deltagarorganisationens AP-operatör uppdaterar metadata via ansvarig för transportinfrastrukturens (Diggs) administrativa rutiner och verktyg.</p> <p>Deltagarorganisationen anmäler uppdatering till federationsoperatörens administrativa rutiner och verktyg.</p> <p>Federationsoperatör godkänner uppdatering innan denna träder i kraft.</p>
AF5	Söka adressinformation	En Användare i en deltagarorganisation söker ut adressuppgifter för önskad mottagare.
AF6	Skicka meddelande	En Användare i en deltagarorganisation skapar och skickar ett meddelande i sin meddelandeklient.
AF7	Komplettera meddelande	En Användare i en deltagarorganisation skapar och skickar ett meddelande som kompletterar ett tidigare skickat meddelande i sin meddelandeklient.
AF8	Besvara meddelande	<p>En Användare i en deltagarorganisation besvarar ett meddelande i sin meddelandeklient.</p> <p>Användaren kan följa vilka meddelandekonversationer som denne deltagit i och vilka</p>

		meddelanden som är svar på andra meddelanden.
AF9	Lista meddelanden	En Användare i en deltagarorganisation listar meddelanden, inkomna och skickade i sin meddelandeklient.
AF10	Ta del av meddelande	En Användare i en deltagarorganisation tar del av ett meddelande i sin meddelandeklient.
	Godkänna federation	Ansvarig för transportinfrastrukturen (Digg) ansvarar för godkännande. Kontakta Digg för detaljer kring denna process.
	Godkänna AP-operatör	Ansvarig för transportinfrastrukturen (Digg) ansvarar för godkännande. Kontakta Digg för detaljer kring denna process.

I tabellen beskrivna användningsfall utgör grundläggande användningsfall riktade mot slutanvändare, dvs användare som skickar och tar emot meddelanden, samt administratörer av gemensamma komponenter. I översikten ingår även bakomliggande stödjande användningsfall, som sker på system-system-nivå. Dessa beskrivs inte som separata användningsfall i detta kapitel.

4.2 Aktörsinformation

Följande huvudaktörer är involverade i ett SDK meddelandeflöde:

Aktör	Aktörsinformation
Mänskliga aktörer	
Ansvarig för transportinfrastruktur	Aktör som godkänner och ansluter AP-operatörer. Denna roll kallas plattformsansvarig (Digg).
Administratör	Behörig administratör i deltagarorganisation.

Användare	<p>Person i en deltagarorganisation som via en meddelandeklient skickar eller tar emot meddelanden.</p> <p>Användaren är alltid starkt autentiserad och behörig, vilket måste säkerställas i meddelandeklienten.</p>
Accesspunktoperatör (AP-operatör)	Accesspunktsoperatör ansvarar för och äger en accesspunkt. Det är också accesspunktsoperatören som ansluter deltagarorganisationen till plattformen via en accesspunkt
Systemaktörer	
Lokaliseringstjänst (SML)	<p>Komponenten ansvarar för att skapa och uppdatera DNS poster som pekar ut Metadatatjänst (SMP).</p> <p>Skapar, uppdaterar och tar bort adress till aktuell Metadatatjänst för deltagarorganisationen.</p>
DNS	Innehåller lokaliseringssuppgifter (NAPTR record) till Metadatatjänst (SMP).
Metadatatjänst (SMP)	Metadatatjänsten innehåller information om deltagarorganisationernas Accesspunkter och vilka tekniska tjänster som organisationen tillhandahåller för säker kommunikation inom SDK federationen.
Certifikatpubliceringstjänst (CertPub)	Federationens tillförlitliga källa för anslutna deltagarorganisationers publika nyckel. Komponentens används för kryptering, signering samt validering av signatur.
SDK adressbok	SDK Adressbok är en tjänst som innehåller adressuppgifter för anslutna deltagarorganisationer, inklusive deras adresserbara funktioner.
Administrativa gränssnitt	Administrativa användargränssnitt för att administrera uppgifter om Accesspunktens metadata, deltagarorganisationens certifikat (O2O) och adressinformation. Gränssnitten erbjuds primärt som ett grafiskt gränssnitt för Administratörer.
Accesspunkt	Accesspunkt är en teknisk komponent som en deltagarorganisation använder för att kommunicera med

	andra deltagarorganisationer inom SDK via plattform för eDelivery
Meddelandetjänst/Meddelandeväxel	Meddelandetjänsten är en komponent som mottager, validerar och tillgängliggör meddelande för användaren via en meddelandeklient. Meddelandetjänsten kan i meddelandeutbyte anta rollerna sändare respektive mottagare.
Meddelandeklient	Meddelandeklient är gränssnittet mot Användaren. Meddelandeklient kan vara ett integrerat verksamhetssystem, eller ett särskilt system ämnat för säker meddelandeöverföring.

4.3 Logisk realisering - användningsfall

Ett urval av användningsfallen i översikten ovan beskrivs mer ingående i detta avsnitt.

4.3.1 AF1 – Registrera deltagarorganisation

4.3.1.1 Textuell beskrivning

Förutsättning:

- AP-operatör och federationsoperatör tillämpar stark autentisering samt är auktoriserad.
- AP-operatör är godkänd av ansvarig för transportinfrastrukturen (Digg).

Aktiviteter:

- AP-operatör registrerar deltagarorganisationens metadata i Metadatatjänst.
- Federationsoperatör godkänner registrerat metadata i Metadatatjänst.
 - Registrerar deltagarorganisationens publika nyckel för Organisation-till-organisation kryptering och signering (O2O). Registrering sker via federationsoperatörens administrativa rutiner och verktyg.
 - Registrerar godkänd deltagarorganisationen i SDK:s gemensamma komponent SDK Adressbok.
 - Tilldelar deltagarorganisationens administratör behörighet till SDK adressbok.

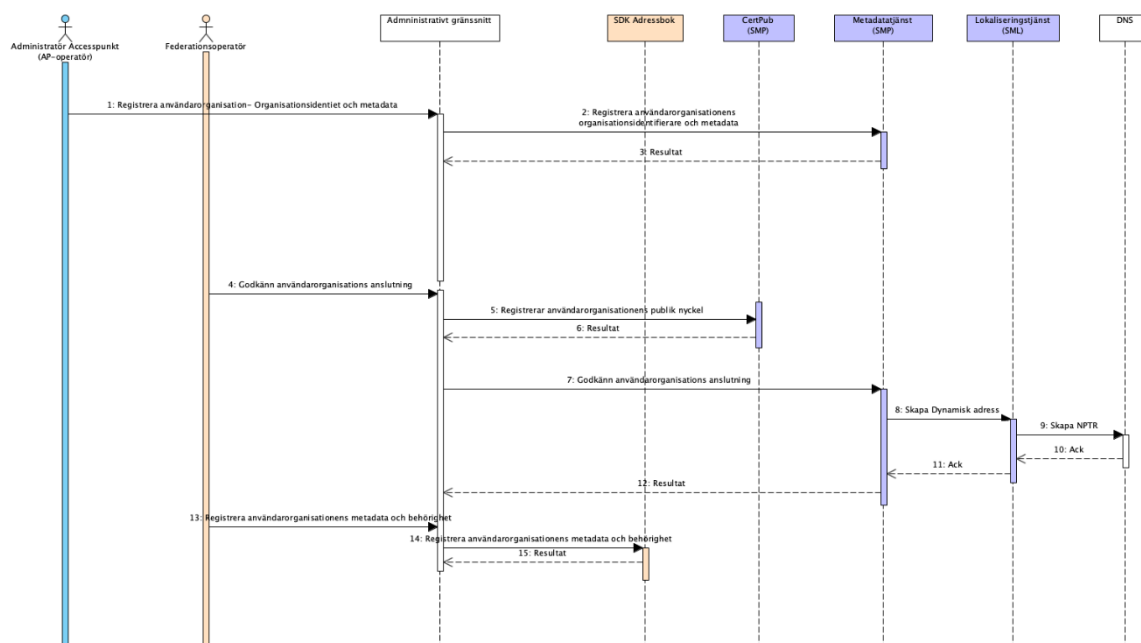
Resultat: Registrerad deltagarorganisation är tekniskt förberedd för att skicka och ta emot meddelanden till/från övriga registrerade deltagarorganisationer.

- Tillhörande metadata för kommunikation, certifikat samt adressuppgifter är registrerade.

Följande systemaktörer är involverade:

Aktör	Hanterar information
Administrativa gränssnitt	Gemensamt administrativt användargränssnitt för att registrera uppgifter om deltagarorganisation.
Metadatatjänst (SMP)	<p>Deltagarorganisationens tekniska kommunikationsmöjligheter (kapabiliteter)</p> <ul style="list-style-type: none"> • Organisationsidentitet. • Tjänstetyp (anger att man har förmågan till att kommunicera via SDK). • Dokumenttyp (anger vilket meddelandeformat som används) • URL till Deltagarorganisationens accesspunkt. • Accesspunktens säkerhetscertifikat för signering och kryptering.
Lokaliseringstjänst (SML)	<p>Komponenten ansvarar för att skapa och uppdatera DNS poster som pekar ut deltagarorganisationens Metadatatjänst (SMP).</p> <ul style="list-style-type: none"> • Skapar adress till aktuell Metadatatjänst för deltagarorganisationen.
DNS	Innehåller lokaliseringssuppgifter (NAPTR record) för adress till Metadatatjänst (SMP).
SDK Adressbok	<p>Adressuppgifter för deltagarorganisationen.</p> <ul style="list-style-type: none"> • Organisationsidentitet, organisations namn, beskrivning. • Funktionsidentiteter, funktionsnamn, beskrivning. • Attribut sökning och filtrering
Certifikatpubliceringstjänst	Deltagarorganisationens publika nyckel för XHE kryptering och signering.
Accesspunkt	Deltagarorganisationens konfigurerings i Accesspunkt (AP) tas bort. Illustrerar ej i sekvensdiagram

4.3.1.2 Sekvens



Figur: Sekvensdiagram - registrering av deltagarorganisation och tillhörande meta- och adressdata.

4.3.2 AF2 – Avregistrera deltagarorganisation

4.3.2.1 Textuell beskrivning

Förutsättning:

- AP-operatör och federationsoperatör tillämpar stark autentisering samt är auktoriserade.

Aktiviteter:

- AP-operatör
 - avregistrerar deltagarorganisationen från metadatatjänst.
 - avregistrerar deltagarorganisationen från accesspunkt.
- Federationsoperatör
 - godkänner avregistrering i metadatatjänst.
 - avregistrerar deltagarorganisation i SDK adressbok.

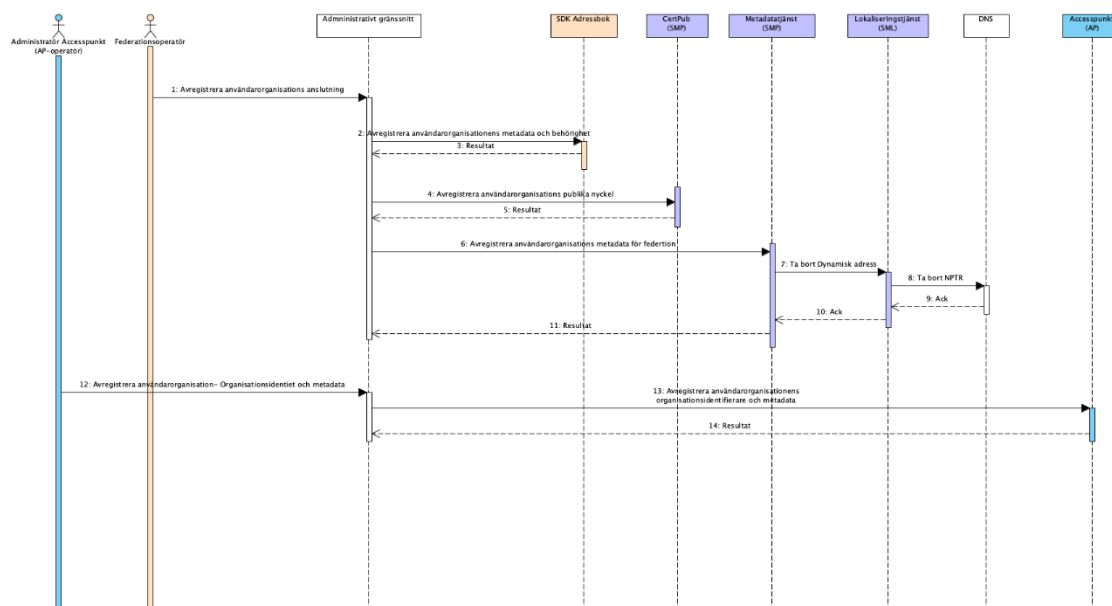
Resultat: Avregistrering innebär att kommunikation med deltagarorganisationen inte längre blir möjlig.

Följande systemaktörer är involverade:

Aktör	Hanterar information
Administrativa gränssnitt	Gemensamt administrativt användargränssnitt för att registrera uppgifter om deltagarorganisation.

Metadatatjänst (SMP)	Metadata för Deltagarorganisationen tas bort.
Lokaliseringstjänst (SML)	Lokaliseringsuppgifter för Deltagarorganisationen motsvarande tjänsten SDK tas bort.
DNS	Lokaliseringsuppgifter (NAPTR record) för Deltagarorganisationen tas bort.
SDK adressbok	Deltagarorganisationens adressposter tas bort i SDK adressbok.
Certifikatpubliceringstjänst (CertPub)	Deltagarorganisationens publika nyckel för XHE kryptering och signering.
Accesspunkt	Deltagarorganisationens konfiguration i accesspunkt (AP) tas bort.

4.3.2.2. Sekvens



Figur: Sekvensdiagram - avregistrering av deltagarorganisation och tillhörande meta- och adressdata.

4.3.3 AF3 – Uppdatera adressinformation för deltagarorganisation

4.3.3.1 Textuell beskrivning

Förutsättning:

- Deltagarorganisationens administratör tillämpar stark autentisering samt är auktoriserad.

- En deltagarorganisation kan endast administrera sina egna adressuppgifter. Det krävs att deltagarorganisationen som sådan först är registrerad (se AF1).

Aktiviteter:

- Administration av adressuppgifter för deltagarorganisation utförs primärt av deltagarorganisationen själv genom behörig lokal administratör som använder gemensamt administrativt gränssnitt för SDK.

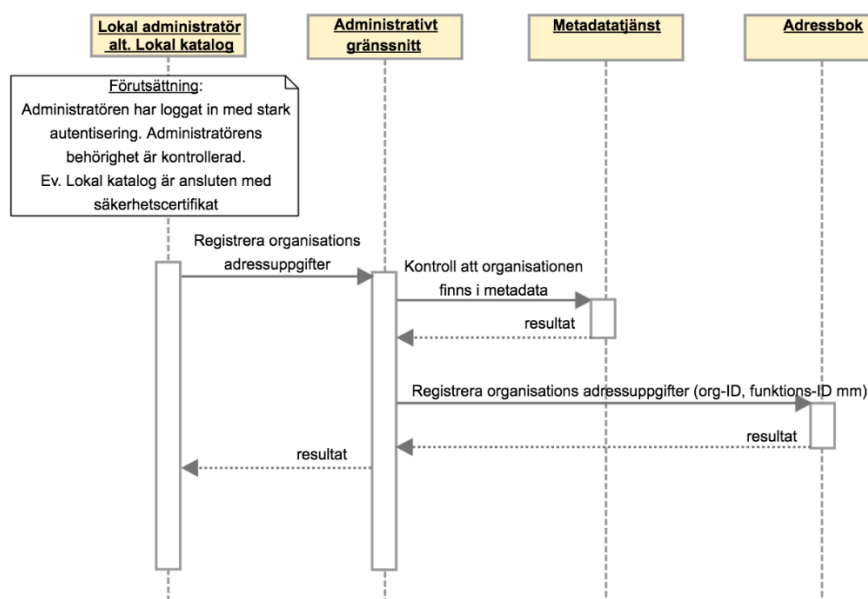
I sekvensdiagrammet nedan visas endast schematiskt en av de möjliga varianterna att administrera uppgifterna. Se vidare avsnitt 5, Teknisk lösning.

Följande systemaktörer är involverade:

Aktör	Hanterar information
Administrativa gränssnitt	Gemensamt administrativt användargränssnitt för att registrera uppgifter om deltagarorganisation.
Deltagarorganisationens egna katalogsystem.	Deltagarorganisationens egna katalogsystem. Kan utgöra källa (master) för adressuppgifter för deltagarorganisationen om den ansluts till tekniskt administrativt gränssnitt för Adressboken. I dagsläget saknas api för denna hantering.
SDK Adressbok	Adressuppgifter för Deltagarorganisationen. <ul style="list-style-type: none"> • Organisationsidentitet, organisations namn, beskrivning. • Funktionsidentiteter, funktionsnamn, beskrivning. • Attribut sökning och filtrering
Metadatatjänst (SMP)	Används för kontroll av att organisationen är registrerad som godkänd deltagarorganisation för SDK.

4.3.3.2 Sekvens

AF - Uppdatera adressinformation för användarorganisation



Figur: Sekvensdiagrammet illustrerar administration av adressuppgifter. Notera att registrering och uppdatering av deltagarorganisationens adressuppgifter kan ske via Lokalt administratör direkt i administrativt gränssnitt.

4.3.4 AF4 – Uppdatera metadata för deltagarorganisation

4.3.4.1 Textuell beskrivning

Förutsättning:

- Administratör accesspunkt (AP-operatör) och federationsoperatör tillämpar stark autentisering samt är auktoriserade.

Aktiviteter:

- Deltagarorganisationens AP-operatör uppdaterar metadata via ansvarig för transportinfrastrukturens (Diggs) administrativa rutiner och verktyg.
- Deltagarorganisationen anmäler uppdatering till federationsoperatörens administrativa rutiner och verktyg.
- Federationsägare godkänner uppdateringar innan dessa träder i kraft.

Följande ändringar ska godkännas av federationsoperatören:

- Ändring av metadata som innebär ändring av dokumenttyp.
- Ändring av deltagarorganisationens publika nyckel för organisation-till-organisations kryptering och signering

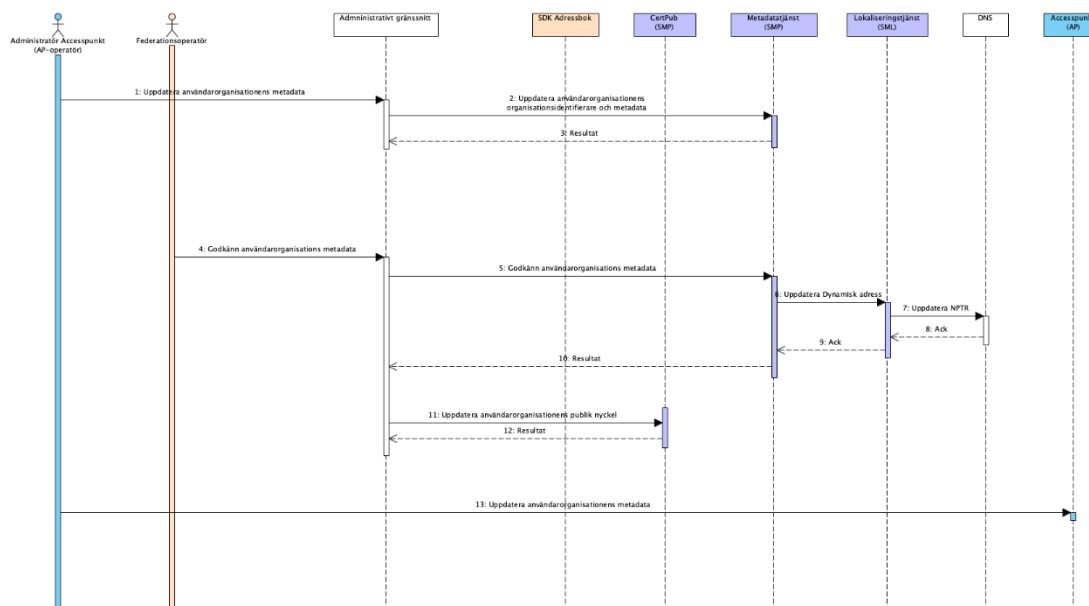
Följande ändringar hanteras av AP-operatör utan federationsoperatörens godkännande.

- Metadata som berör befintlig anslutning t.ex. AP certifikat och teknisk adress.

Observera att inte alla metadatauppdateringar påverkar lokaliseringstjänst och DNS.

Aktör	Hanterar information
Administrativa gränssnitt	Gemensamt administrativt användargränssnitt för att registrera uppgifter om deltagarorganisation.
Metadatatjänst (SMP)	Metadata för Deltagarorganisationen uppdateras.
Lokaliseringstjänst (SML)	Lokaliseringsuppgifter för Deltagarorganisationen motsvarande tjänsten uppdateras. Observera att denna tjänst påverkas olika beroende på vilken metadata som uppdateras.
DNS	Lokaliseringsuppgifter (NAPTR record) för Deltagarorganisationen uppdateras. Observera att denna tjänst påverkas beroende på vilken metadata som uppdateras.
Certifikatpubliceringstjänst (CertPub)	Deltagarorganisationens publika nyckel för XHE kryptering och signering uppdateras. Observera att denna tjänst påverkas beroende på vilken metadata som uppdateras.
Accesspunkt	Deltagarorganisationens konfiguration i Accesspunkt (AP) tas bort. Illustrerar ej i sekvensdiagram. Observera att denna tjänst påverkas beroende på vilken metadata som uppdateras.

4.3.4.2 Sekvens



Figur: Sekvensdiagrammet illustrerar administration av metadata.

4.3.5 AF5 – Söka adressinformation

4.3.5.1 Textuell beskrivning

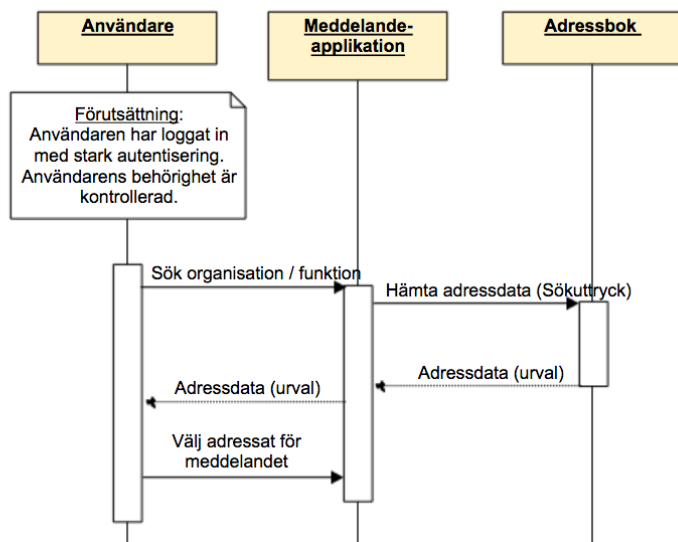
En Användare eller lokal komponent (meddelandeklient) i en deltagarorganisation söker/slår upp adressinformation för den/de mottagare som användaren avser skicka säkert meddelande till. Användaren kan använda sök- och filtreringsvillkor för att få fram eftersökta uppgifter.

Följande systemaktörer är involverade:

Aktör	Hanterar information
SDK Adressbok	Adressuppgifter för Deltagarorganisationen. <ul style="list-style-type: none"> Organisationsidentitet, organisationsnamn, beskrivning. Funktionsidentiteter, funktionsnamn, beskrivning. Attribut sökning och filtrering
Meddelandeklient (Meddelandetjänst)	Meddelandeklient är gränssnittet mot Användaren. Meddelandeklient kan vara ett integrerat verksamhetssystem, eller ett särskilt system ämnat för säker meddelandeöverföring. Även komponenten Meddelandetjänst kan söka i SDK Adressbok t.ex. för att validera adress.

4.3.5.2 Sekvens

AF - Sök adressinformation



Figur: Sekvensdiagrammet illustrerar att söka ut adressinformation för önskad mottagare (adressat). Även komponenten meddelandetjänst (MT) kan söka i SDK Adressbok för att t.ex. validera en adress.

4.3.6 AF6 – Skicka meddelande

4.3.6.1 Textuell beskrivning

Förutsättningar:

- Användare tillämpar stark autentisering samt är auktoriserade.
- Användaren har adresserat meddelandet, se AF5.

Aktiviteter:

- En Användare i en deltagarorganisation skapar och skickar ett meddelande via sin Meddelandeklient.
- Meddelandetjänsten krypterar och signerar meddelandet.
- Det krypterade och signerade meddelandet överförs till deltagarorganisationens Accesspunkt och vidare till mottagande organisations Accesspunkt. Vid överföring mellan Accesspunkter krypteras och förseglas meddelandet (AS4).

Mottagande Accesspunkt dekrypterar och verifierar meddelandet varvid mottagarorganisationens Meddelandetjänst hämtar upp meddelandet (förutsatt att allt gått bra). Meddelandetjänsten dekrypterar- och kontrollerar signatur samt validerar meddelandet till struktur och innehåll. Meddelandet förmedlas till den meddelandeklient (Verksamhetssystem) som ansvarar för meddelandets funktionsadress. Meddelandet tillgängliggörs tekniskt för behörig användare.

I flödet ingår även kvittens/felhantering på både transport- och meddelandenivå för att åstadkomma en garanterad leverans.

- Kvittens i transportlagret sker när meddelande tekniskt är korrekt överfört till mottagande Accesspunkt.
- Kvittens i meddelandelagret sker när meddelandet är dekrypterat, signatur validerad samt meddelandets struktur och innehåll är validerat.
- Meddelandekvittensen skickas som ett nytt meddelande tillbaka till den ursprungliga avsändande deltagarorganisation.

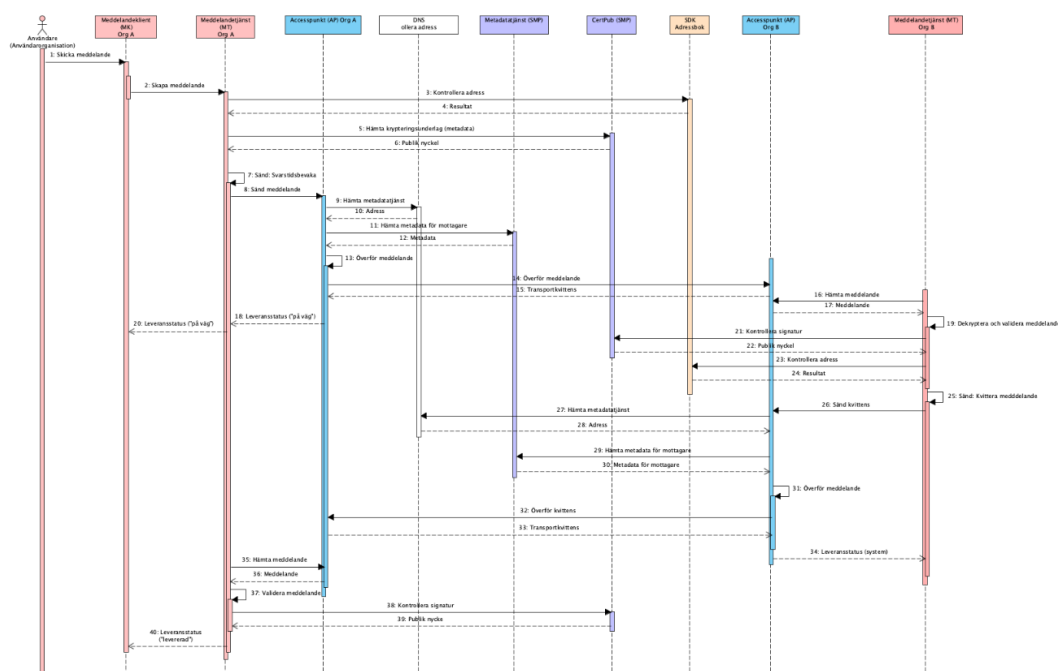
Att söka ut / ange mottagande organisations adressuppgifter föregår användningsfallet och är inte medtaget i denna beskrivning, se AF5.

Följande systemaktörer är involverade:

Aktör	Hanterar information
Accesspunkt - Org A (sändare)	<p data-bbox="544 853 943 882">Avsändande Accesspunkt hanterar</p> <ul style="list-style-type: none"> • tar emot meddelande från Meddelandetjänst. • lokaliserar och slår upp metadata om mottagande organisation, inklusive mottagande Accesspunkts certifikat. • kontrollerar giltighetstid och revokeringsstatus för mottagande Accesspunkts certifikat. • förseglar AS4 meddelandet med digital signatur, baserat på sändande Accesspunkts privata nyckel. • krypterar AS4 meddelandet med mottagande Accesspunkt som mottagare, baserat på mottagande Accesspunkts certifikat. • säkerställer att transporten krypteras till mottagande Accesspunkt (Transport Layer Security). • skickar AS⁴ meddelande till mottagande Accesspunkt.
Accesspunkt - Org B (mottagare)	<p data-bbox="544 1480 943 1509">Mottagande Accesspunkt hanterar</p> <ul style="list-style-type: none"> • tar emot AS4 meddelande från avsändande Accesspunkt, krypterad på transportnivå (Transport Layer Security). • validerar mottaget AS4 meddelande på transportnivå. • dekrypterar mottaget meddelande. • verifierar AS4 meddelandets försegling, dvs. kontrollerar att det är oförvanskat, inklusive kontroll av giltighet och revokeringsstatus på aktuellt signaturcertifikat. • tillgängliggör AS4 meddelande för ansluten Meddelandetjänst.

Metadatatjänst (SMP)	Tillhandahåller tekniska metadata om mottagande deltagarorganisation och dess Accesspunkt (Org B).
DNS	Används för att hitta mottagande deltagarorganisations Metadatatjänst.
Meddelandetjänst - Org A (sändare)	Paketerar, innehållsvaliderar, krypterar och överför XHE meddelande till sin Accesspunkt. <ul style="list-style-type: none">Mottagande deltagarorganisations publika nyckel hämtas från certifikatpubliceringstjänsten (CertPub).
Meddelandetjänst - Org B (mottagare)	Hämtar meddelande från sin Accesspunkt. Dekrypterar XHE meddelandet, innehållsvaliderar, validerar meddelandets signatur, utför intern routing vid behov, och tillgängliggör meddelande för Användare via en meddelandeklient. Meddelandekvittens skall endast signeras.
Meddelandeklient	Meddelandeklient är gränssnittet mot Användaren. Meddelandeklient kan vara ett integrerat verksamhetssystem, eller ett särskilt system ämnat för säker meddelandeöverföring.

4.3.6.2 Sekvens



Figur: Sekvensdiagrammet illustrerar att skicka ett meddelande från organisation A till B.

4.3.7 AF7 och AF8 – Komplettera och besvara meddelande

4.3.7.1 Textuell beskrivning

Att komplettera och besvara ett meddelande sker med samma mekanismer som för användningsfall "AF6 - Skicka meddelande". När ett meddelande kompletteras eller besvaras ska dock alltid det tidigare meddelandet som kompletteras/besvaras refereras, vilket bygger upp en tråd av meddelanden och svar på meddelanden. En användare kan i sin meddelandeklient således följa vilka meddelandekonversationer som denne deltagit i. Se SDK Innehållsspecifikation, B1.3.3 där beskrivs vilka attribut som skall refereras vid komplettering/besvarande.

4.3.7.2 Sekvens

Se sekvens för användningsfall "AF6 - Skicka meddelande". Meddelandetjänsten kopplar ihop skickade meddelanden med tidigare meddelanden genom kopplingsidentifikatorer.

Se avsnitt 5.1.9 "Stöd för spårbarhet, svar och konversationer" samt SDK Innehållsspecifikation" för detaljerade beskrivningar.

4.3.8 AF10 – Ta del av meddelande

4.3.8.1 Textuell beskrivning

Meddelandeklienten (MK) hämtar meddelande meddelandetjänst (MT). Meddelanden kan hämtas genom att tillämpa Rekommendation API MT/MK för SDK, se specifikation R21 Rekommendation SDK API MT/MK.

Förutsättning:

- Användare tillämpar stark autentisering samt är auktoriserade.

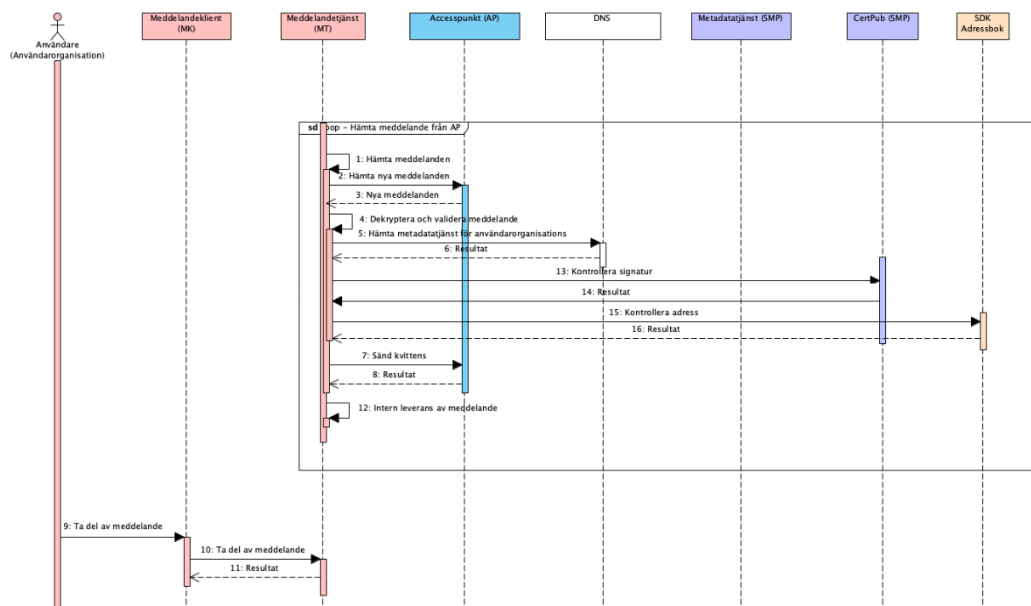
Aktiviteter:

- Deltagarorganisationen Meddelandetjänst hämtar löpande meddelanden från dess AP-operatörs accesspunkt.
 - Alla meddelande dekrypteras och valideras.
 - Meddelanden kan överföras till meddelandetjänsten med olika tekniska lösningar(push/pull).
 - Meddelanden kan överföras till Meddelandeklienten (Verksamhetssystem) som hantera funktionsadressen (funktionsbrevlådan) genom att tillämpa rekommendationen Rekommendation SDK API MT/MK.
- En Användare använder Meddelandeklienten för att ta del av meddelanden.

Följande systemaktörer är involverade:

Aktör	Hanterar information
Meddelandeklient (MK)	Meddelandeklienten är gränssnittet mot Användaren. Meddelandeklient kan vara ett integrerat verksamhetssystem, eller ett särskilt system ämnat för säker meddelandeöverföring. Meddelanden kan hämtas genom att tillämpa Rekommendation SDK API MT/MK.
Meddelandetjänst (MT)	Paketerar, innehålls validerar och skickar meddelande till Accesspunkt. Meddelandetjänsten kan tillgängliggöra meddelanden kan hämtas genom att tillämpa Rekommendation SDK API MT/MK.
Accesspunkt	Kommunicerar (överför meddelanden) med accesspunkter inom federationen.

4.3.8.2 Sekvens

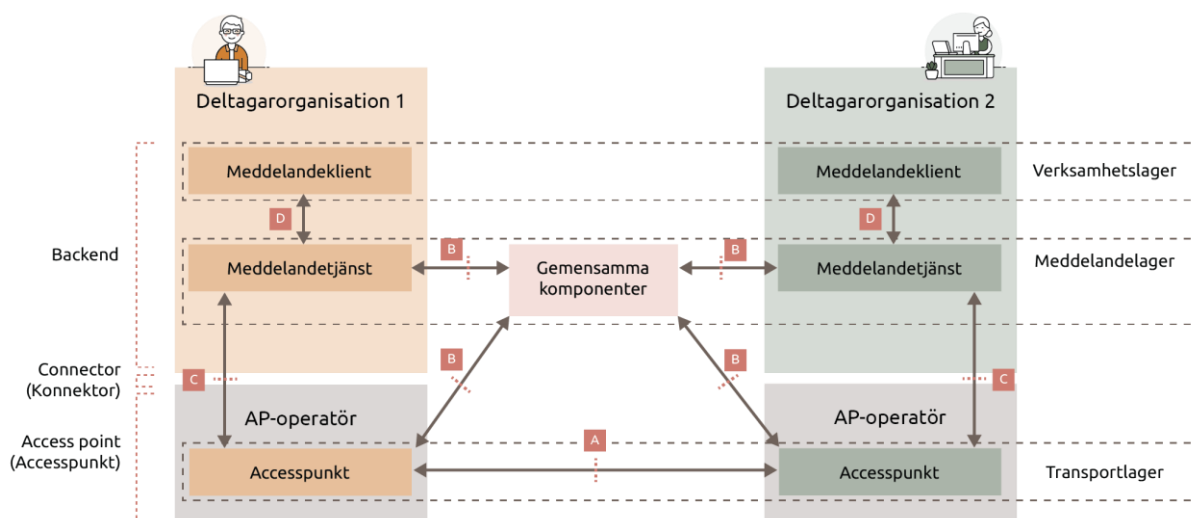


Figur: Sekvensdiagrammet (steg 9) illustrerar hur ett meddelande hämtas till Meddelandeklienten. Sekvensen föregås av "Hämta meddelande från AP"

5. Teknisk lösning

5.1 Beskrivning av arkitekturellt signifikanta delar av lösningen

5.1.1 Referensmodell för säker meddelandeöverföring och dess gränssytor



Figur: Referensmodell för säker meddelandeöverföring.

Referensmodellen för säker meddelandeöverföring syftar bland annat till att definiera ett antal gränssytor mellan olika delkomponenter i lösningen, fördela ansvar mellan olika lager och komponenter samt möjliggöra att olika produkter och lösningar för säker meddelandehantering lättare kan samverka. Gränssytorna underlättar också utbyte av viss produkt, t ex i transportlagret, genom att en annan produkt realiserar motsvarande transportprotokoll och gränssnitt mot meddelandetsjans.

5.1.1.1 Gränssyta A

Gränssyta A motsvarar transportprotokollet för att säkert överföra meddelanden mellan parter (organisationer). Gränssyta A måste vara standardiserad så att alla accesspunkter som realiserar gränssnittet blir interoperabla med varandra och säkert kan utbyta meddelanden.

Det är tekniskt möjligt att stödja flera olika transportprotokoll parallellt, vald teknisk lösning har stöd för att konfigurera vilket transportprotokoll och version som gäller för den aktuella överföringstypen (dokumenttypen). Förutom att det ger en större flexibilitet, generalitet och framtidssäkring av det tekniska ramverket ger det även visst stöd för att hantera nya versioner av transportprotokollet.

Gränssyta A realiserar genom protokollet OASIS ebMS 3.0 AS4, eller kort "AS4", som är en av OASIS-profilerad standard baserad på WebService-protokoll för kommunikation och säkerhet. Se vidare [hur eDelivery realiserar transportlagret](#),

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery>

- Anslutna Accesspunkter inom SDK-federationens realiserar Digg AS4 specifikation. Se Ref. R15 Transportinfrastruktur Beskrivning och Ref. R16 Digg, eDelivery - Transportprofil AS4.

5.1.1.2 Gränsyta B

Gränsyta B är en samlingsbeteckning för de gränssnitt som behövs mot gemensamma komponenter.

Gränssnitten kan delas in i:

- Gränssnitt för adressuppgifter till organisation och funktion (verksamheter). Se bilaga SDK adressbok API-dokumentation SDK Adressbok Informationsspecifikation för mer information om gränssnitten.
- Gränssnitt för uppslag av var de tekniska tjänsterna finns (lokaliseringstjänster se Ref. R12 SML Komponentspecifikation).
- Gränssnitt för uppslag av metadata och säkerhetscertifikat för mottagares tekniska tjänster (se Ref. R13 SMP Komponentspecifikation).
- Gränssnitt för kontroll av säkerhetscertifikat (CRL/OCSP, se Ref. R14 Digg, eDelivery - PKI för Accesspunkter Tjänstebeskrivning).
- Gränssnitt för kontroll av deltagarorganisationens certifikat, se Ref. R18 Digg, eDelivery - Certifikatspublicering - REST-bindning till SMP.

5.1.1.3 Gränsyta C

Gränsyta C består av de systemgränssnitt (API:er) som accesspunkten erbjuder meddelandetjänster.

Accesspunkter kan erbjuda flera olika tekniska "smaker" på gränssnitten, t ex Webservice/SOAP, HTTP/REST, JMS, S-FTP.

Gränssnitten tillhandahåller dock samma grundfunktionalitet till meddelandetjänsten: skicka meddelande, kontrollera status för meddelanden, hämta nya inkomna meddelanden, hämta logginformation osv.

En komponent som realiserar ett visst gränssnitt mot accesspunkten kallas även för en Konnektor.

En accesspunktsprodukt kan erbjuda ett ramverk för att utveckla nya konnektorer inom ramen för en accesspunkt, för att på så sätt kunna erbjuda nya tekniska gränssnitt mot accesspunkten. T.ex. har produkten Domibus (CEF:s referensimplementering för accesspunkt) ett ramverk för att utveckla konnektorer som plug-ins till Domibus.

Om den aktuella accesspunktsprogramvaran saknar ett sådant ramverk, och behov finns att lägga till ett tekniskt gränssnitt i ytan C, kan man behöva ta fram en fristående programvarukomponent som agerar adapter framför accesspunkten, dock inom skalskyddet för denna.

5.1.1.4 Gränsyta D

Gränsyta D består av de systemgränssnitt (Rekommendation SDK API MT/MK) som meddelandetjänst (API producent) erbjuder meddelandeklienter (API konsument).

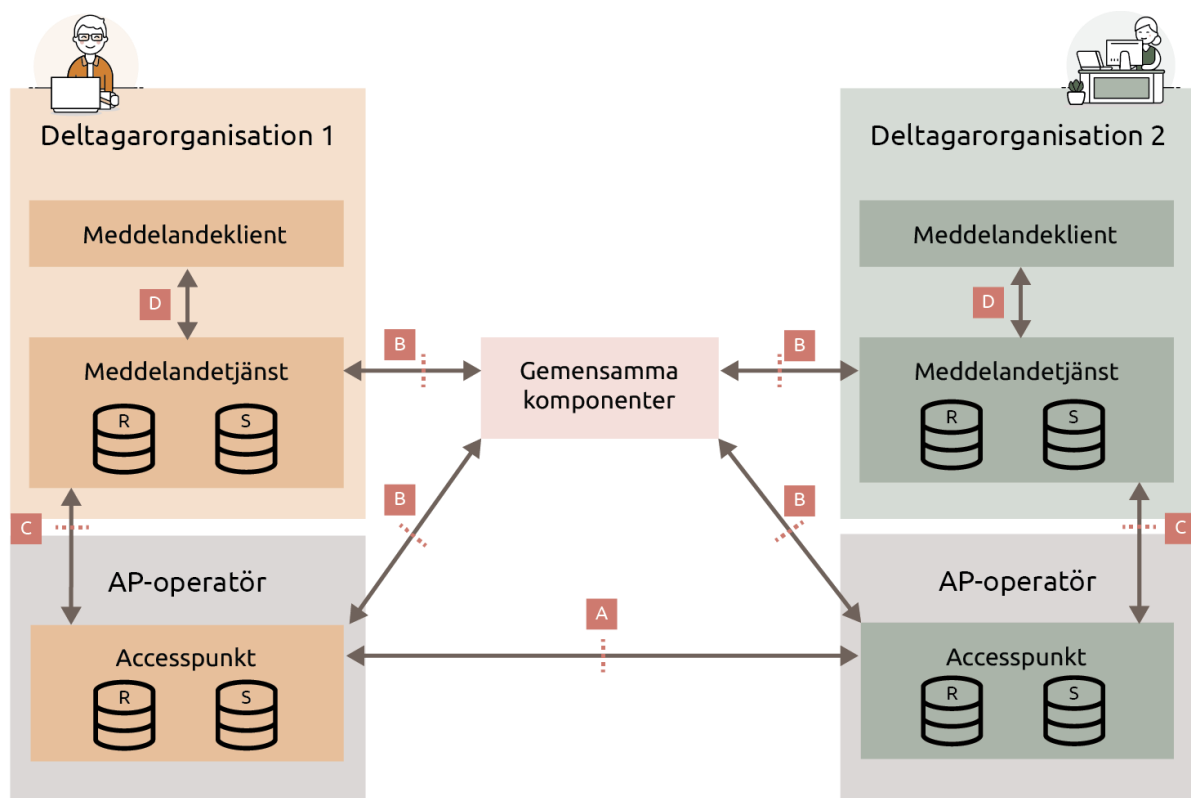
Meddelandeklient kan t ex vara ett anpassat verksamhetssystem eller paketerade slutanvändarprodukter särskilt utformade för säker meddelandehantering.

Rekommendation SDK API MT/MK (REST API) stödjer följande operationer:

- Skicka meddelande
- Hämta meddelande
- Radera meddelande

Rekommendation SDK API MT/MK (REST API) är beskrivet (kontrakt) enligt specifikationen openAPI, version 3.1.x, och är utformat enligt/inspirerat av JSON:API, se specifikation R21 Rekommendation SDK API MT/MK.

5.2 Asynkront meddelandeflöde



Figur: Meddelandeflödet är asynkront med stöd för köhantering i både meddelandelagret och transportlagret.

I bilden representerar "S" en kö för sändning (Sender) och "R" en kö för mottagning (Receiver). Meddelandeflödet enligt referensmodellen är asynkront, vilket t.ex. betyder att ett meddelande kan läggas på kö för sändning och producenten av meddelandet kan direkt gå vidare till nästa meddelande eller andra aktiviteter. Köhantering realiseras i både meddelandelagret och transportlagret. På så sätt skapas lös

koppling mellan de olika lagren och mellan komponenter i en viss realisering av modellen. I meddelandelagret (meddelandetjänst) kan det dessutom förekomma separata köer för respektive meddelandeklient.

Det kan även vid behov förekomma köhantering i respektive meddelandeklient beroende på hur meddelandeklient och meddelandetjänst realiserats i organisationen. Om t.ex. verksamhetssystem med egen lagring ansluts till en separat meddelandetjänst är det lämpligt att ha köhantering även i verksamhetssystemet. Notera att ett enskilt anrop, t.ex. anropet mellan sändande och mottagande accesspunkt, har ett synkront svar som kvittens på själva anropet.

Den asynkrona överföringsmodellen och köhanteringen ger följande kvalitativa fördelar:

- Ett mer robust system för meddelandeöverföring, där enskilda noder kan vara nere kortare tider utan att meddelandeöverföringen som sådan bryts. Detta kan öka den för användare upplevda tillgängligheten i systemet markant. Jämför ekosystemet för SMTP-baserad e-post.
- Inbyggda möjligheter att sända om meddelanden som inte kunnat levererats t.ex. p.g.a. att någon del av tekniken tillfälligt är otillgänglig.
- Bättre skalbarhet, större potential att kunna hantera större laster (meddelandeflöden), eftersom mottagande system kan validera och processa inkomna meddelanden i separata processer, och inte kopplat i realtid vid mottagandet av meddelandet.

5.2.1 Validering, felhantering och kvittens

Deltagarorganisationer ansvarar för att korrekta meddelanden överförs inom SDK-federationen. För att säkerställa detta finns ett gemensamt regelverk för "Validering, felhantering och kvittens". Enligt detta ska deltagarorganisationer validera och kontrollera meddelanden vid såväl sändande som mottagande av meddelanden. Meddelandetjänsten är normalt den komponent som behöver ha förmåga att tillämpa regelverket.

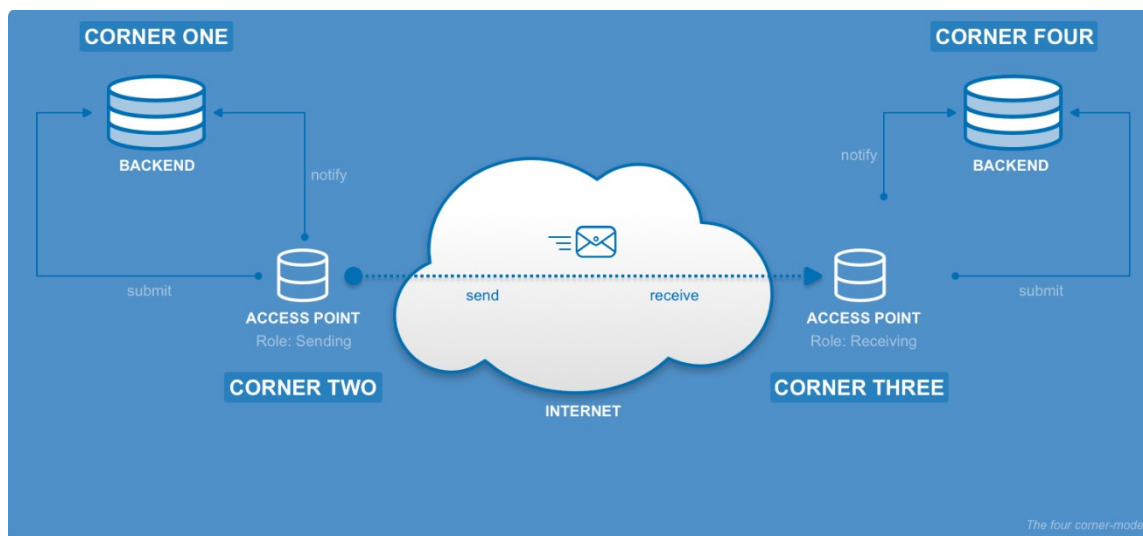
Regelverket innehåller kontroller såsom:

- Följsamhet mot regler i specifikation
- Meddelandevalidering (schema och schematron)
- Skydd mot skadlig kod (skanning)
- Kontrollera avsändare och mottagare

Se Specifikation Validering, felhantering och kvittens, B1.3.2".

5.2.2 eDelivery realiserar transportlagret

I den framtagna lösningen utgörs transportlagret och delar av de gemensamma komponenterna av eDelivery (Se Ref. R6 CEF eDelivery), ett byggblock framtaget av EU:s organisation Connecting Europe Facility (CEF).

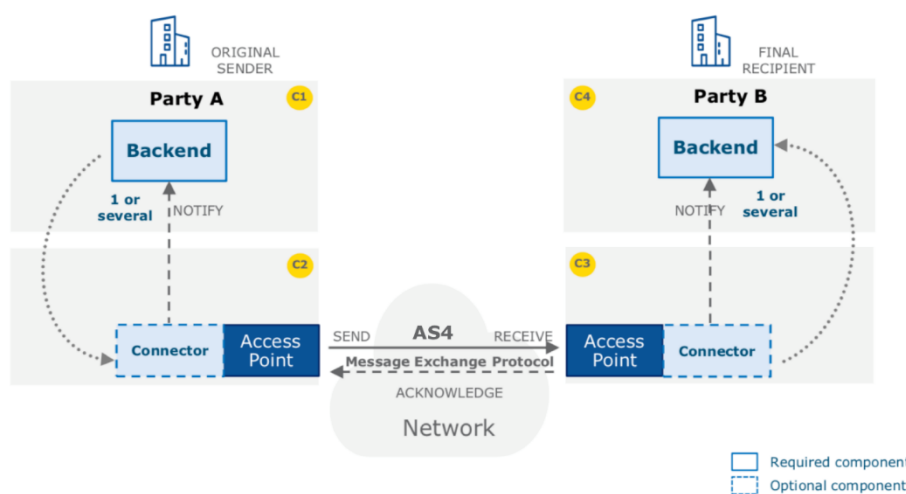


Figur: Byggblocket eDelivery för säkert utbyte av dokument och data mellan parter. Källa: CEF.

eDelivery syftar till att utgöra ett generellt byggblock för säker robust överföring av dokument och data mellan parter över internet, eller annat privat nätverk, och följer en sk fyrhörningsmodell där sändande system via sin accesspunkt skickar till mottagande system via dess accesspunkt. Kommunikationen behöver alltså inte gå över en central hub som i 3/5-hörningsmodeller.

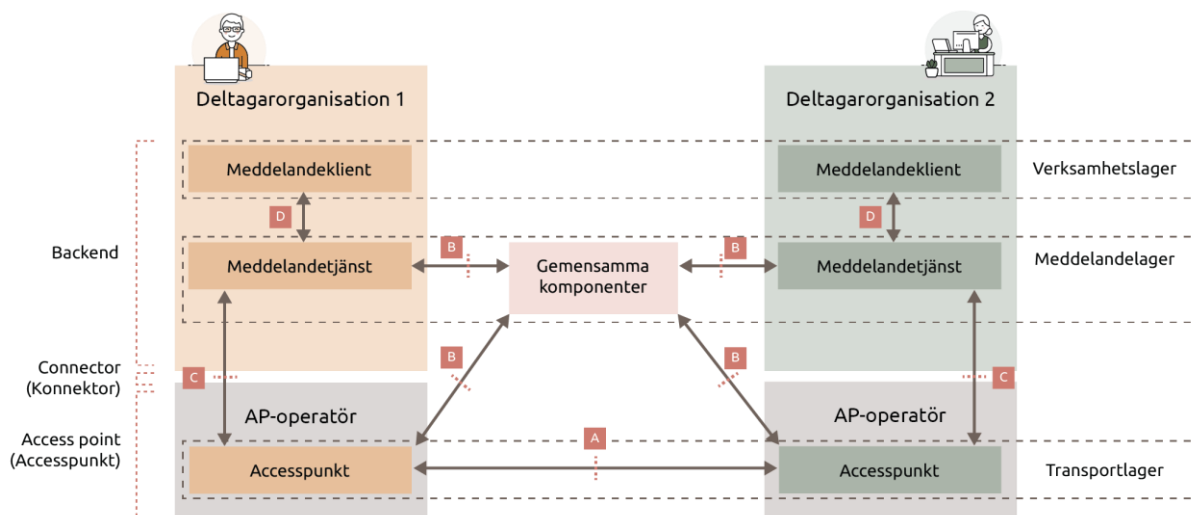
Egenskaper:

- Alla till alla – ”peer-to-peer”
- Generisk transportinfrastruktur - Olika meddelanden och dokumenttyper kan överföras
- Överföring sker asynkront
- Varje ansluten deltagarorganisation (party) registrerar vilka dokumenttyper som kan utbytas



Figur: eDeliverys 4-hörningsmodell för säker robust transport. Källa: CEF. C1/C4 – deltagande parter anslutna system (backend), t.ex. anpassat verksamhetssystem eller en renodlad meddelandeklient, som användare använder för att skicka och ta emot. C2 – sändarens accesspunkt. C3 – mottagarens accesspunkt.

Om man placerar in eDeliverys begrepp, Access point, Connector, Backend och Corner 1 - 4, i referensmodellen för säker meddelandeöverföring ovan, får vi följande bild:



Figur: eDeliverys 4-hörningsmodell mappad mot referensmodellen för säker meddelandeöverföring.

5.2.2.1 Transportprotokollet AS4

eDelivery-ramverket ger stöd för att i princip använda flera olika transportlager för olika typer av överföringar, men det transportprotokoll som är det primärt stödda av CEF är AS4 (Se "R7 OASIS AS4 transportprotokoll").

AS4-protokollet har bl.a. följande egenskaper:

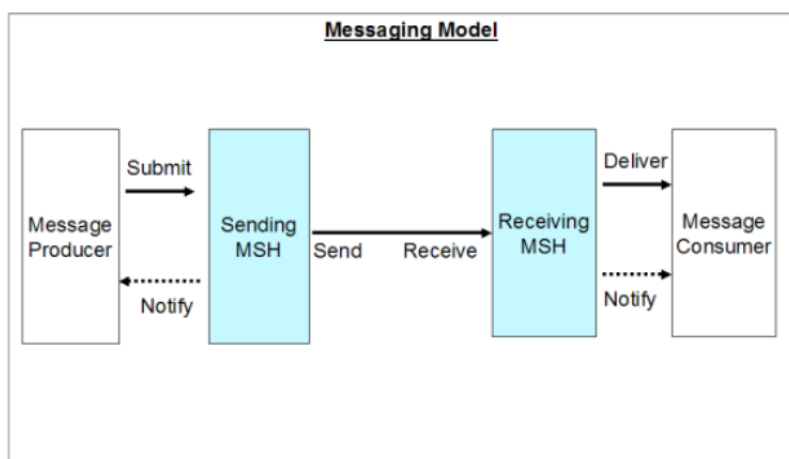
- Transporten är baserad på WebService-stacken över HTTP.
- Transporten är oberoende av formatet på nyttolasten (payload agnostic). AS4 kan utväxla olika typer av nyttolast, t.ex. XML, JSON, HL7, PDF, binära format osv.
- Inbyggt stöd för komprimering av nyttolast (payload compression)
- Konfidentialitet för meddelandet genom stöd för både transport- och meddelandekryptering mellan accesspunkter
- Dataintegritet dvs. skydd mot förvanskning eller förlust av meddelande under transport, bl.a. genom e-stämpel (e-seals)
- Säker signerad kvittens av överfört meddelande (transport receipt / evidence of delivery) levereras synkront.
- Stöd för duplikateliminering för att säkerställa att ett meddelande levereras en och endast en gång.



Figur. AS4 översikt. Källa CEF.

5.2.2.2 Profilen eDelivery AS4

I SDK har AS4 tillämpats utifrån den rekommenderade profilering för eDelivery som CEF tillhandahåller, eDelivery AS4, samt Diggs profilering av AS4-protokollet. Se Ref. R16 eDelivery - Transportprofil AS4.



Figur. Kommunikationsmönster enligt eDelivery AS4. Källa CEF.

Profilen eDelivery AS4 preciserar bl.a.:

- Att kommunikationsmönstret är envägs/PUSH (one-way PUSH), vilket innebär att meddelandet tekniskt överförs från avsändande system till mottagande system. En meddelandekvittens (meddelande mottagen), skickas

som ett eget anrop i den andra riktningen. AS4-protokollet stödjer även PULL, dvs. att mottagande system först får ett anropsmeddelande från avsändaren innehållande en länk där mottagande system hämtar meddelandet.

Det senare mönstret (PULL) utvärderades i en förstudie för SDK, en nackdel som lyftes var problematiken för avsändaren att ansvara för att tillgängliggöra meddelanden för andra parter över tid.

AS4 stödjer även tvåvägskommunikation där primära syftet är att leverera svar med innehåll på en begäran (request/response).

- Hur AS4 ska tillämpas i eDeliverys 4-hörningsmodell, t.ex. hur avsändande system (original sender - corner 1) respektive mottagande system (final recipient - corner 2) hanteras.
- Vilka säkerhetsmekanismer som är obligatoriska, t.ex. e-stämpling och meddelandekryptering.
- Hur nyttolasten paketeras (i separata MIME-delar).

Profilen "eDelivery - Transportprofil AS4" (Se R16) beskriver avvikelser från underliggande eDelivery AS4 profil:

- Vilken version av eDelivery AS4 profil som skall tillämpas
- Meddelanden skall kuverteras enligt XHE. Se R17 DIGGDIGGDIGG, eDelivery - Kuverteringsprofil XHE
- Konfigureringar av Processing mode (P-mode)
- Tillämpning av PKI för AS4 meddelandekryptering av signering
- Tillämpning av TLS
- Valideringstillägg av meddelanden, funktionalitet som inte ingår i en standard mjukvara enligt CEF eDelivery Conformance Testing.

5.2.2.3 Profilering och specifikationer för Säker digital kommunikation

SDK-federationen tillämpar Diggs AS4 profilering med precisering enligt SDK federationens tekniska anpassningar mot plattform för eDelivery, B1.4.4.

Transportprotokollet kapslar sedan in själva meddelandet (nyttolasten) som går mellan avsändande och mottagande parter (organisationer). Nyttolastens struktur återfinns i SDK Innehållsspecifikation, se B1.3.3".

För sammanställning av använda integrationsprofiler för meddelandeöverföringen se avsnitt 5.4.1, Nyttjade integrationsprofiler.

5.3.3 Lokaliseringstjänst och metadatatjänst

eDelivery realiserar även två gemensamma komponenter i lösningen som hanterar uppslag av mottagande parter och deras accesspunkter, för att avsändande part dynamiskt ska hitta fram till mottagande parts accesspunkt enbart med kännedom om vilken organisation man vill skicka till.

5.3.3.1 Lokaliseringstjänst - eDelivery Service Metadata Locator (SML)

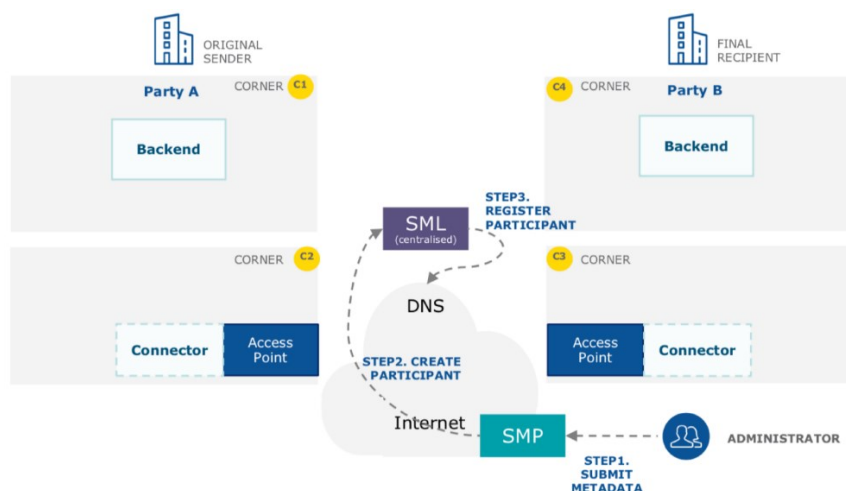
Lokaliseringstjänsten SML är en central komponent som möjliggör att accesspunkterna dynamiskt kan hitta mottagande organisations Metadatatjänst enbart baserat på mottagande parts organisationsidentitet, samt vetskap om vilket typ av meddelandeutbyte som ska göras, i detta fall SDK meddelandeutbyte.

SML kan ses som ett förssystem som hjälper till att registrera organisationer som ska delta i ett meddelandeutbyte. Registreringen av en organisation resulterar i en speciell post i nätverkstjänsten DNS (Domain Name System). När ett meddelandeutbyte ska ske slår avsändande accesspunkt upp mottagande parts post i DNS och får tillbaka adressen (URL) till aktuell Metadatatjänst. Notera att posterna i DNS är av typen Name Authority Pointer - NAPTR, se vidare Dynamic Delegation Discovery System (DDDS) Part Four. En NAPTR post skapa i DNS enligt Hash (Participant ID) + Participant ID Scheme + SML Domain.

5.3.3.2 Metadatatjänst - eDelivery Service Metadata Publisher (SMP)

Metadatatjänsten SMP håller mottagarens tekniska kommunikationsmöjligheter (kapabiliteter) i ett eDelivery-nätverk (t.ex. SDK federation). I SMP registreras en deltagande organisation och dess tekniska tjänster, dvs. tekniska adresser till accesspunkter, vilket transportprotokoll som stöds, och vilken typ av meddelandeutbyte och version dessa kan hantera. Även säkerhetscertifikat till accesspunkterna registreras i och hämtas från SMP. En avsändande accesspunkt slår mot SMP och kan med uppgifterna säkerställa att mottagaren kan hantera den typ av meddelandeutbyte som avses. På så sätt underlättas interoperabiliteten i eDelivery-nätverket (t.ex. SDK federation) över tid.

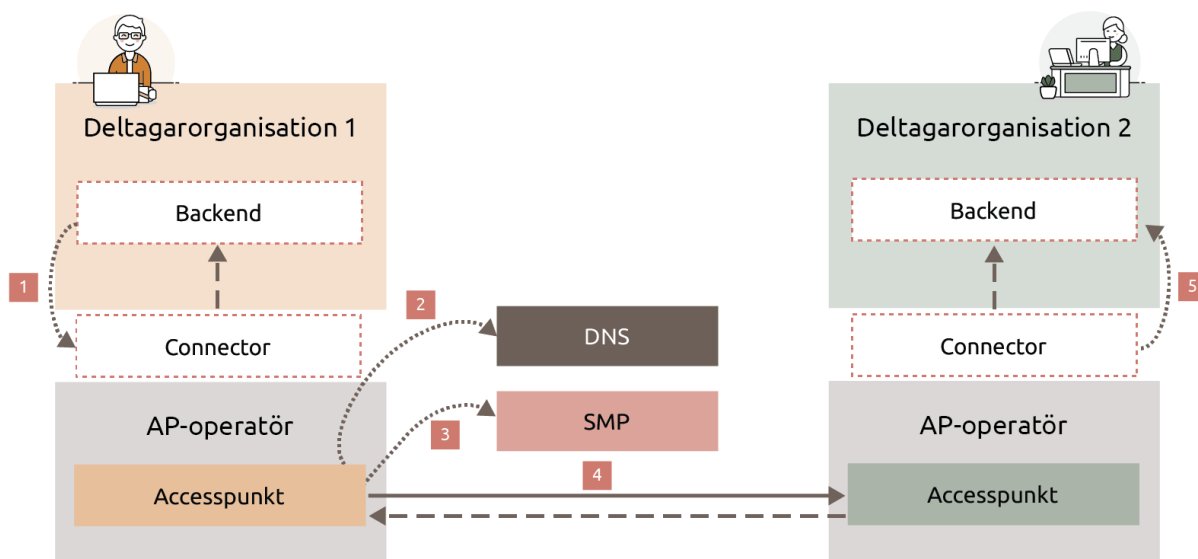
I eDelivery kan det finnas flera SMP-tjänster, t.ex. olika SMP för olika typer av meddelandeutbyten som e-faktura, säkra meddelanden (SDK), socialförsäkringsuppgifter osv, men SMP-tjänsten kan även konsolideras till en nationellt gemensam SMP. I Sverige hanteras en gemensam SMP-tjänst av Myndigheten för digital förvaltning, DIGG (<https://www.digg.se>), och SDK har registrerats som en underdomän inom den tjänsten.



Figur: Registrering av en deltagarorganisation inkl. metadata för deltagande i meddelandeutbyte. Källa CEF.

Uppgifterna registreras först i SMP och går sedan automatiskt vidare till SML och DNS.

Notera att all administration av SML/DNS sker via behörigt SMP-system som först har tilldelats ett säkerhetscertifikat.



Figur: Dynamiskt uppslag av en mottagande organisation (Party B) via DNS i ett visst meddelandeutbyte. Accesspunkten får adress till mottagarens SMP-tjänst (steg 2), från vilken hämtas de tekniska uppgifterna om vilken typ av meddelandeutbyte som mottagaren stödjer (steg 3).

5.3.4 Certifikatspubliceringstjänst (CertPub)

För att stödja insynsskydd (i form av meddelandekryptering och signering) mellan kommunicerande deltagarorganisationer (C1/C4) realiserar Digg tjänsten CertPub (Se Ref. R18 eDelivery - Certifikatspublicering - REST-bindning till SMP). Tjänsten är en utökning av SMP där information om respektive deltagarorganisationers certifikats publika nyckel publiceras.

Tjänsten möjliggör tillämpning av "Transportmodell - Utökad Bas", se Ref. R17 Digg, eDelivery - Kuverteringsprofil XHE som stärker säkerheten då själva meddelandet krypteras och signeras. Meddelande krypteras innan det hanteras av Diggs transportinfrastruktur, dvs mellan accesspunkter via AP-operatörer. Detta innebär att endast avsedd mottagande deltagarorganisation (C4) kan ta del av (dekryptera) meddelandet.

Certifikatspubliceringstjänst tillämpar samma tekniska lösning för dynamiskt uppslag (dynamic discovery) som metadatatjänst - eDelivery Service Metadata Publisher (SMP).

5.3.5 Adresseringsmodell

En avgörande faktor för att verksamheter ska kunna använda SDK-federationen som ett fullvärdigt alternativ för säker digital kommunikation är:

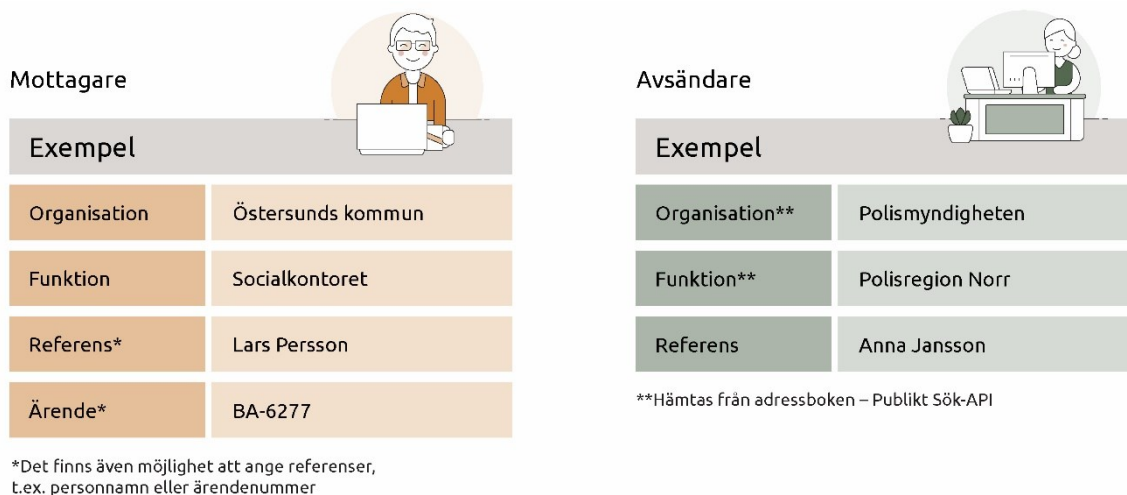
- förmågan att hitta säkra adressater för de mottagare verksamheten behöver nå, och att kunna lita på korrektheten i dessa adresser.
- förmågan att säkerställa vem avsändaren av ett meddelande är.

En utmaning i detta är hur en verksamhet får tillgång till adressuppgifter till övriga parter och att upprätthålla kvalitet i dessa uppgifter.

Funktionellt kan verksamhetskraven något förenklat sammanfattas i:

1. att det ska gå att skicka meddelande till (adressera) en viss **organisation**
2. att det ska gå att skicka meddelande till (adressera) en **funktion** inom en viss organisation, liknande en funktionsbrevlåda.
3. att det ska gå att referera till medarbetare i respektive organisation.
4. att det ska gå att referera till interna referenser, t ex ärendenummer, hos respektive part.

OBS! Verksamheterna behöver i praktiken kunna adressera ett meddelande till flera funktioner/organisationer samtidigt (sändlista). Dock är en specifik meddelandeöverföring i SDK tekniskt sett alltid adresserad till endast en mottagare, alltså en kombination av organisation och funktion, t.ex. socialkontoret i Storkommun. Däremot finns inga hinder att en meddelandeklient stödjer att ange en sändlista. I SDK Innehållsspecifikation, B1.3.3 beskrivs vilka attribut som skall refereras vid sändlista.



Figur: Adressera och ange referenser för ett SDK-meddelande (konceptuellt).

De två första kraven, adressera organisation och funktion, ingår i SDK adresseringsmodell. De senare kraven ingår i SDK Innehållsspecifikation, dvs. hanteras som märkning av ett meddelande som adresseras till en funktion i en organisation, där märkningen hanteras vidare inom organisationens meddelandetjänst/applikation.

eDelivery ger ett grundläggande stöd att adressera säkert till en organisation via stödtjänsterna SMP och SML. Funktionaliteten är dock ganska begränsad när det gäller att söka och beskriva organisationer, även om det teknisk skulle vara möjligt att utöka strukturerna.

Det saknas direkt stöd i eDelivery för att hantera den inre nivån med funktioner inom respektive organisation. Det finns exempel på tillämpningar av eDelivery som har lagt till en katalogfunktionalitet där det ges bättre möjligheter att beskriva organisationer, söka på organisationer osv.

Av ovanstående skäl har det i SDK-federationen lagts till en gemensam tjänst för att hantera och söka på adressater, SDK adressbok, vilken beskrivs mer nedan.

5.3.6 Principer för adressering

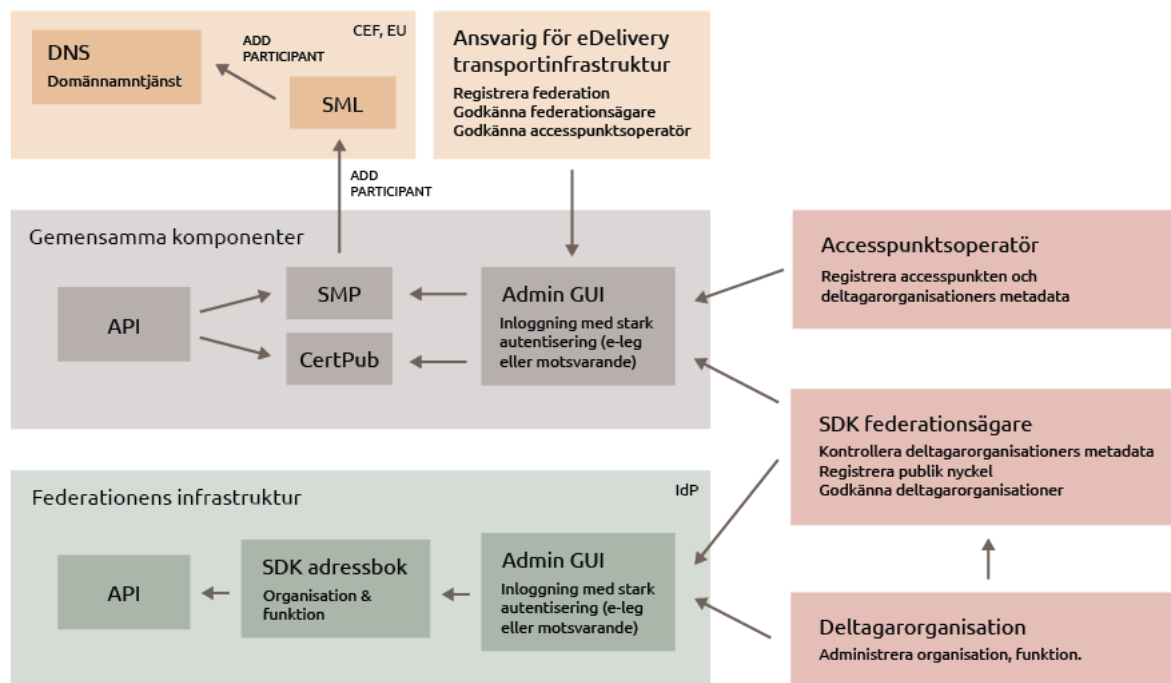
Följande principer har definierats för hantering av adressinformation i SDK:

- Varje organisation ansvarar för sin egen adressinformation, distribuerad administration ska vara möjlig.
- Det ska gå att administrera adressinformation
 - via ett gemensamt administrativt gränssnitt för behöriga användare inom organisationen
 - alternativt ansluta ett eget system med befintlig adresskälla (typiskt en katalogtjänst).
- Gemensamma integrationsprofiler (api:er) tas fram
 - för att från meddelandeklienter kunna söka adressuppgifter för mottagare
 - för att från eget system med befintlig adresskälla kunna publicera/uppdatera adressuppgifter för mottagare (API för uppdatering saknas)
- Dynamisk adressering baserat på organisation och efterfrågad typ av meddelandeutbyte (för SDK är detta "säkert meddelande", men kan vara t.ex. e-faktura eller dylikt i andra sammanhang).

Principerna syftar bl a till att:

- Möjliggöra hög datakvalitet genom att hålla uppdatering av uppgifterna så nära källan (organisationen själv) som möjligt.
- Undvika onödig dubbelregistrering av uppgifter.
- Möjliggöra att snabbt komma igång med säker meddelandeöverföring för organisationer med en eller ett fåtal funktionsbrevlådor.
- Undvika att exponera organisationens interna organisationsstruktur i adressboken, genom att exponerade funktioner inte direkt behöver motsvara den interna strukturen.
- Göra det enklare att hantera att organisationer gör tekniska ändringar IT-systemen, t.ex. byter den tekniska adressen för accesspunkten, genom den dynamiska adresseringen baserat på organisation.

5.3.6.1 Underhålla adressinformation



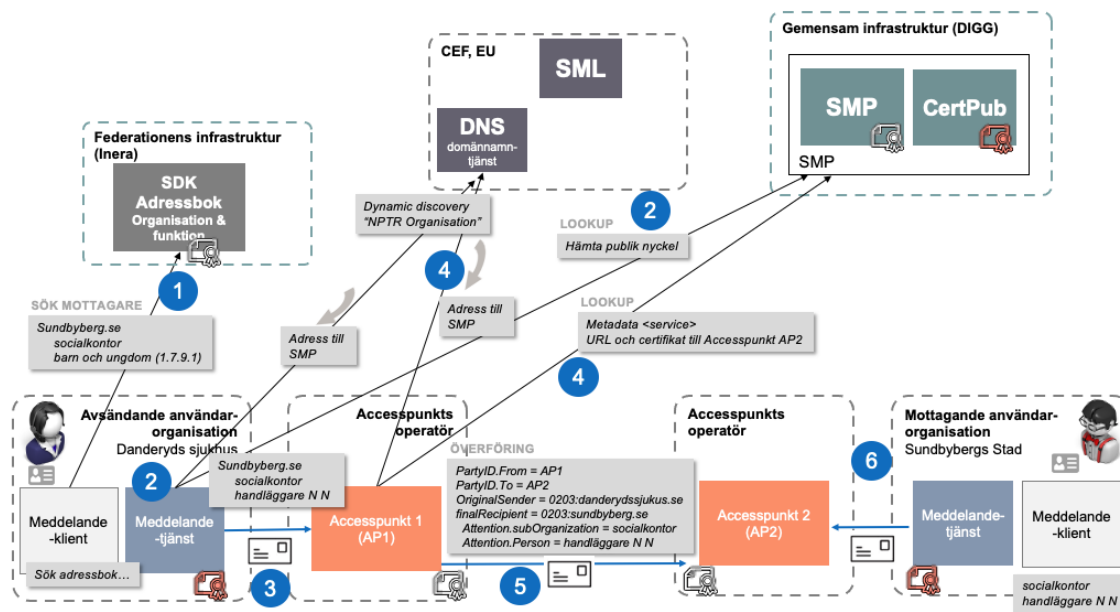
Figur: Underhåll av adressinformation för SDK meddelandeutbyte.

Bilden ovan beskriver de komponenter som behövs för att realisera funktioner för att registrera och underhålla adressinformation för SDK meddelandeutbyte.

För att administrera adressuppgifter för en organisation behöver organisationen först läggas upp i SMP-tjänsten tillsammans med annan metadata.

Adressboken är ett register med utökade adressuppgifter för respektive deltagande organisation. Organisationsidentifieraren i SMP-tjänsten återfinns även i adressboken och används för att koppla organisationens metadata till adressuppgifterna.

5.3.6.2 Använda adressinformation



Figur: Hur adressinformation används när ett meddelande skickas, exempelflöde.

Bilden ovan beskriver ett exempelflöde för hur adressuppgifter, och i viss mån även referenser, används när ett meddelande adresseras och skickas. I exemplet ovan ska en sändare skicka ett meddelande till socialkontoret i Sundbybergs Stad.

Förutsättning: Lars använder en meddelandetjänst för att i detta exempel skicka till Sundbybergs Stad.

Flödet består i huvudsak av följande steg:

1. Lars söker på "sundbyberg.." och systemet slår i SDK Adressbok och hittar Sundbybergs Stad samt de funktioner som kommunen lagt upp som mottagare.
2. Lars väljer funktionen "Socialkontor" i kommunen och skickar sedan meddelandet.
 - Meddelandetjänsten skapar ett NAPTR uppslag utifrån hash av identifieraren "0203:sundbyberg.se" samt SML zon, vilken används för att göra ett DNS-uppslag. Tillbaka kommer adressen till den SMP-tjänst som hanterar Sundbybergs Stad.
 - Meddelandetjänsten hämtar "Sundbybergs Stads" publika nyckel från Certifikatpubliceringstjänsten (CertPub). Adresserar och skapar meddelandet som krypteras och signeras.
3. Meddelandetjänsten skickar meddelandet vidare till accesspunkten.
4. När meddelandet ska skickas av accesspunkten, skapas ett NAPTR uppslag utifrån hash av identifieraren "0203:sundbyberg.se" samt SML zon, vilken används för att göra ett DNS-uppslag. Tillbaka kommer adressen till den SMP-tjänst som hanterar Sundbybergs Stad.
 - Accesspunkten gör uppslag mot SMP-tjänsten och får tillbaka nödvändig metadata för att kunna skicka meddelandet till Sundbybergs Stad accesspunkt (AP2).
5. Accesspunkten (AP1) skickar meddelandet till mottagande accesspunkt (AP2) baserat på uppgifterna från SMP.

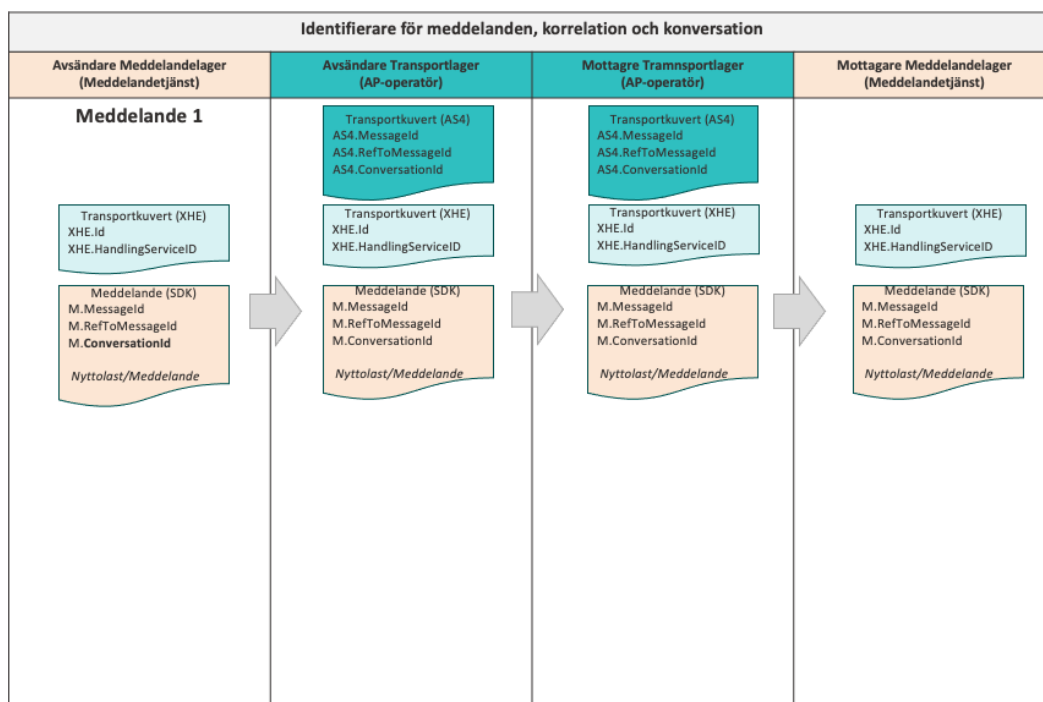
6. Sundbybergs Stad meddelandetjänst fångar upp inkommit meddelande, kontrollerar avsändare mot SDK Adressbok och tillgängliggör det för den funktionsbrevlåda som adresserats. Här kan behöriga medarbetare logga in och få tillgång till meddelandet.
 - Eventuella referenser som angivits för meddelande, t.ex. specifik handläggare eller ärendenummer, hanteras av mottagande organisation, t.ex. för att knyta meddelandet till ett internt ärende.

5.3.7 Stöd för spårbarhet, svar och konversationer

I ramverket för SDK finns produktberoende stöd för att:

- unikt spåra ett meddelande på meddelande- och transportnivå (AS4.MessageId).
- koppla svar till det meddelande som svaret avser (M.refToMessageId).
- koppla kvittens till det meddelande som kvittensen avser (M.MessageId)
- koppla samman ett meddelandeflöde i en konversation (meddelandetråd) (M.conversationId).

Stödet är realiserat genom att det finns ett antal identifierare dels i transportlagret (transportkuvert) och dels i meddelandelagret (meddelandekuvett).



Figur: Identifierare som stöd för spårbarhet, korrelation och konversationer i meddelandeöverföring. Observera att bilden inte illustrerar XHE-paketering som krypterar och signerar meddelandekuvett.

5.3.7.1 Identifierare i transportlagret

eDelivery AS4 header Identifierare	Beskrivning
T.MessageId[1..1]	Unikt id för meddelande enligt RFC5322
T.RefToMessageId[0..1]	Kopplar (korrelerar) transportkvittens till meddelande. Sätts till MessageId för meddelandet som kvitteras.
T.ConversationsId[1..1]	Globalt unik identifierare för en konversation (tråd).

XHE header Identifierare	Beskrivning
<u>T.XHE.ID</u> [1..1]	Meddelandets identitet ska vara globalt unikt och i UUID-format.

5.3.7.2 Identifierare i meddelandelagret (nyttolast header)

Identifierare	Beskrivning
M.MessageId[1..1]	Unikt id för meddelandet enligt RFC4122 (UUID).
M.RefToMessageId[0..1]	Kopplar (korrelerar) meddelanden på meddelandenivå. Sätts till MessageId för meddelandet som besvaras. Ger stöd för ordningsföljd inom en konversation (tråd). Används inte om meddelandet inte är ett svar på ett annat.
M.ConversationsId[1..1]	Unikt id för en konversation (tråd). Alla meddelanden inom samma konversation delar samma ConversationId. För första meddelandet i en konversation sätts denna till samma värde som MessageId.

5.3.7.3 Spårbarhet till visst meddelande

För att kunna spåra hur ett visst meddelande flödar hela vägen från avsändaren till mottagaren behöver ett meddelande kunna identifieras i alla lager från verksamhet, meddelande till transport.

- M.MessageId i meddelandelagret sätts av sändande meddelandetjänst som unik identifierare av verksamhetsmeddelandet.

- T.XHE.ID sätts av sändande meddelandetjänst till samma som id som M.MessageId.
- T.MessageId i transportlagret sätts som en separat unik identifierare för denna specifika överföring av meddelandet. En ev. omsändning av ett meddelande mellan två accesspunkter har samma T.MessageId.
- Meddelandelagret erhåller T.MessageId från transportlagret när meddelandet överförs för att skickas.

Meddelandelagret har krav på att logga både M.MessageId och T.MessageId för meddelandet för att få spårbarhet genom hela meddelandeflödet.

OBS! Meddelande-id i resp. lager hålls isär för att få en renare skiktad modell där det blir lättare att sända om meddelanden vid fel (exakt samma meddelande kan skickas om), samt underlättar att vid behov nyttja olika transportlager för meddelandeöverföring.

5.3.7.4 Transportkvittens

Mottagarens accesspunkt skickar automatiskt och synkront, efter validering av transportkuvertet, ett ”signalmeddelande” innehållande transportkvittens (SignalReceipt) tillbaka till avsändarens accesspunkt.

T.RefToMessageId på transportnivån används för att koppla samman meddelande och transportkvittens.

5.3.7.5 Meddelandekvittens

- Mottagarens Meddelandetjänst skickar automatiskt, efter dekryptering och validering av meddelandet struktur och innehållen en meddelandekvittens tillbaka till avsändaren.
- M.RefToMessageId på meddelandenivå används för att koppla samman meddelanden och meddelandekvittens.
- DocumentReference.Id sätt till XHE.Id (M.MessageId) för det meddelande som kvitteras.
- Meddelanden kvitteras med “ACCEPTED” (Accepteras) eller “REJECTED” (Accepteras ej) .

5.3.7.6 Besvara meddelande och konversationer

När en användare väljer att svara på ett tidigare erhållet meddelande, skapas en koppling mellan det nya meddelandet och det meddelande som besvaras. Samtidigt kopplas meddelandena samman i en meddelandekonversation (tråd).

- Avsändarens Meddelandeklient använder ConversationId för att gruppera meddelanden i konversationer (trådar).
- När ett meddelande besvaras, sätts RefToMessageId för det meddelande som besvaras.
- Inom respektive konversation (tråd) visar RefToMessageId sekvensen av meddelanden i tråden - vilket meddelande som besvarar vilket.

- Användarens Meddelandeklient kan använda RefToMessageId för att sortera meddelanden i en logisk ordningsföljd inom en konversation/tråd.

5.3.7.7 Komplettera meddelande

- Att komplettera ett meddelande innebär att två meddelanden kopplas till samma meddelande (messageId) via RefToMessageId.
- När ett meddelande kompletteras, sätts meddelandeId från det första meddelandet till RefToMessageId .
- Ett meddelande kan kompletteras flera gånger (begränsande regel saknas).
- Samma "ConversationId" från det första meddelandet återanvänds. Detta för att gruppera meddelanden i konversationer (trådar).

5.3.7.8 Skicka meddelande till flera mottagare

Att skicka ett meddelande till flera mottagare innebär att varje mottagare får ett nytt meddelande. Mottagaren kan inte se att samma meddelande har skickats till flera mottagare.

- Varje meddelande får ett nytt meddelande med ett nytt "messageId"
- Befintlig konversation kan återanvändas eller en ny konversation kan skapas.

5.4 Integration med omvärlden

Meddelandeklienter (klienter) integrerar med:

1. Gemensamt adressregister - SDK adressbok.
2. Identifieringstjänst (Identity Provider, IdP) för att hantera stark autentisering för inloggade användare i meddelandeklienten, och som även kan stödja en effektiv behörighetshantering i applikationerna.
3. En katalogtjänst för medarbetare och organisation som kan ge stöd för funktioner som
 - a. att knyta behörighet och funktionalitet till funktionsbrevlådor,
 - b. att välja medarbetare som egna referenser för meddelanden,
 - c. att skicka notifiering t.ex. via e-post eller sms vid inkomna meddelanden som berör en eller flera medarbetare.

Det är ett lokalt ansvar exakt hur organisationen realiserar identitet och åtkomst i sin organisation, se bilaga för IT-säkerhet inom SDK.

För rekommenderade mönster för hur realisera identitet- och åtkomsthantering i meddelandeklienten, se "R3 Referensarkitektur - Identitet och åtkomst". Det rekommenderas även att följa Referensarkitektur för Kataloginformation för utformning av kataloglösningar.

Meddelandetjänst integrerar med:


1. Gemensamt adressregister (SDK Adressbok).
 - a. Meddelandetjänsten validerar meddelandets utgående och inkommande funktionsadress.

2. DNS för dynamiskt uppslag av Certifikatspubliceringstjänst-tjänst.
3. Certifikatspubliceringstjänst (CertPub - Se Ref. R18 eDelivery - Certifikatspublicering - REST-bindning till SMP)
 - a. Gemensamt register innehållande anslutna deltagarorganisationers publika nyckel.
 - i. Meddelandetjänst hämtar mottagarens publika nyckel för meddelandekyptering (Se Ref. R19 eDelivery - Transportmodell - Utökad Bas)
 - ii. Meddelandetjänsten hämtar avsändarens publika nyckel för att validera meddelandets signatur (Se Ref. R19 eDelivery - Transportmodell - Utökad Bas)
4. Certifikatstjänster (Certifikatsutgivare - CA) för att skapa tillit till och kontroll av giltighet för O2O-certifikat (spärrtjänster).

Accesspunkter integrerar med:

- DNS för dynamiskt uppslag av SMP-tjänst.
- Metadatatjänst (SMP) för uppslag av metadata för mottagarens tekniska förmågor avseende säkert meddelandeutbyte.
- Certifikatstjänster (Certifikatsutgivare - CA) för att skapa tillit till och kontroll av giltighet för säkerhetscertifikat (spärrtjänster). Se Ref. R10 PKI för Accesspunkter Tjänstebeskrivning.

5.4.1 Nyttjade integrationsprofiler

Namn	Källa	Beskrivning
AS4 Profile of ebMS 3.0	AS4-profile-v1.0-os.pdf (OASIS)	AS4 är en standardprofilering av protokollet ebXML 3.0 för B2B meddelandeöverföring.
eDelivery AS4 profil	Digg, eDelivery transportprofil AS4 (C3.2.1)	
eDelivery SMP specifikation	SMP Komponentspecifikation, C3.4.1	Specifikationer för en SMP Metadatatjänst i eDelivery
eDelivery SML specifikation	SML Komponentspecifikation, C3.4.2	Lokaliseringstjänst i eDelivery
Dynamic Delegation Discovery System (DDDS)	RFC 3401-3404  RFC 3404: Dynamic Delegation Discovery System	Specifikation för hur DNS-systemet med hjälp av sk. NAPTR records kan användas för att slå upp adresser till specifika tjänster kopplade till t.ex. organisationsidentifierare eller andra nycklar.

	(DDDS) Part Four: The Uniform Resource Identifiers (URI)	Används i eDelivery dynamisk adressering via (SML/DNS)
API för att hämta/söka adressuppgifter från SDK Adressbok	SDK Adressbok - Teknisk guide användning av adressbokens API	Specifikationer för läsbart API för att hämta och söka adressuppgifter för deltagarorganisationer i SDK Adressbok.
Certifikatpubliceringstjänsten	Se R18 eDelivery - Certifikatpublicering - REST-bindning till SMP, C3.4.5	Specifikation som beskriver det publika gränssnitt som ger möjlighet att hämta en deltagarorganisations certifikat. Publicerade certifikat kan användas i två syften – signeringscertifikat och certifikat för kryptering. Kryptering och signering mellan Deltagarorganisationernas system görs i enlighet med Kuverteringsspecifikationen (XHE).
Kuverteringsprofil i XHE	eDelivery - Kuverteringsprofil XHE, C3.2.2	Specifikation av XHE-paketering av meddelanden inom Diggs transportinfrastruktur
SDK Innehållsspecifikation	Se "B2 SDK Innehållsspecifikation"	Specifikation av struktur för nyttolast för SDK-meddelande
Meddelandekvittens	eDelivery – Meddelandespecifikation: Meddelandekvittens, C3.2.4	Specificerar struktur och innehåll för meddelandekvittenser inom Diggs transportinfrastruktur.

5.4.2 Nyttjade plattformsfunktioner

Se sammanställning av använda gemensamma och lokala komponenter under avsnitt 5.4 Integration med omvärlden ovan.

5.5 Felhantering

För principer och ansvarsfördelning kring felhantering se Ref. B12 Specifikation Validering, felhantering och kvittens samt Stöd för spårbarhet, svar och konversationer ovan.

Felhantering och kvittenser hanteras både på transportnivå och meddelandenivå. På transportnivå specificeras hanteringen av transportprotokollet, se avsnitt 5.1.4 eDelivery realiserar transportlagret. På

meddelandenivå styrs detta av Specifikation Validering, felhantering och kvittens, B1.3.2 där Meddelandespecifikation Meddelandekvittens, C3.2.4, används för att kvittera meddelanden eller signalera fel.

- Respektive produkt som realiserar en accesspunkt ansvarar för att dokumentera de felmeddelanden, fel- och statuskoder som accesspunkten tillhandahåller till meddelandetjänster.
- Respektive produkt som realiserar en meddelandetjänst ansvarar för att dokumentera de felmeddelanden, fel- och statuskoder som meddelandetjänsten tillhandahåller till meddelandeklienter.

5.6 Realisering av användargränssnitt

Respektive produkt som realiserar en meddelandeklient ansvarar för att realisera gränssnittet mot slutanvändaren. Användargränssnitten ska kräva stark autentisering och uppfylla kraven enligt Regelverk för deltagarorganisation inom SDK, se A1.2.

Webbaserat användargränssnitt finns framtaget för underhåll av metadata och adressuppgifter i de gemensamma komponenter (SMP, CertPub och SDK Adressbok). Det har utformats så att moderna webbläsare kan användas och med standard HTML i största möjliga utsträckning. Användargränssnittet ska kräva stark autentisering och uppfylla kraven enligt Regelverk för deltagarorganisationer inom SDK, se A1.2.

6 Säkerhet

6.1 Säkerhetsklassificering av information

En kartläggning av externa krav vid kommunikation via Säker digital kommunikation har gjorts, vilken även innefattar lagkrav, se Regelverk för deltagarorganisation A1.2.

Risikanalys avseende informationssäkerhet utförs löpande för lösningskonceptet där både SDK-federationen (Digg) och transportinfrastruktur (Digg) ingår. För att vidta lämpliga skyddsåtgärder krävs att analyser görs av de risker som finns i gemensamt lösningskoncept. Riskminimering i den tekniska lösningen

Nedan följer ett urval av åtgärder för att minimera risk i lösningen:

- Datakvalitet för adressuppgifter
 - Huvudprincipen är att varje deltagande organisation administrerar sina egna uppgifter för att undvika "mellanhänder" där så möjligt. Administration sker via behöriga starkt autentiserad administratör.
 - Spårbarhet via loggning.

- Skydd mot skadlig kod
 - Federationen har tagit fram och principer för validering och felhantering som varje anslutande meddelandetjänst har att förhålla sig till. Principerna ingår i det gemensamma regelverket för meddelandeutbyte inom SDK, som varje part behöver följa. Principerna innebär att en anslutande meddelandetjänst ansvarar för innehållsvalidering inkl. scanning av skadlig kod, både innan ett meddelande skickas och efter att ett meddelande mottagits av meddelandetjänsten. Se vidare avsnitt Validering och felhantering.
- Tillgänglighet
 - Meddelandeöverföringen bygger på en s.k. 4-hörningsmodell, där meddelandeöverföringen inte behöver passera centrala noder, utan kan gå direkt mellan deltagarorganisationers AP-operatörer som tillhandahåller accesspunkter, och vidare till verksamhetssystemen. Överföringen är asynkron med köhantering och omsändning vid tillfälliga fel i infrastrukturen, vilket skapar goda förutsättningar för en för användaren upplevd god tillgänglighet för systemet. Se Asynkront meddelandeflöde.
 - Viktiga komponenter ska sättas upp i enlighet med de SLA-krav som ställs av SDK-federationen (Digg) respektive ansvarig för Plattform för eDelivery (Digg). Detta innebär att flera kluster per tjänst (redundans), t.ex. accesspunkter och metadatatjänst behöver sättas upp.
 - Transportinfrastruktur (Digg)
 - Lokaliseringstjänst (SML): ej nödvändig för att sända/mottaga meddelanden; komponenter vid administration av uppgifterna (när ny organisation ska registreras, tas bort eller om uppgiften skulle vara fel i SML).
 - Domännamnssystem (DNS): kritisk gemensam komponent; har en distribuerad arkitektur där EU:s instans är dubblerad.
 - Metadatatjänst (SMP): kritisk gemensam komponent för att sända/mottaga meddelanden. Flera instanser (kluster) kan skapa redundans.
 - Certifikatpubliceringstjänst (SMP): kritisk gemensam komponent för att möjliggöra kryptering/signering och validering av signaturer för meddelanden. Flera instanser (kluster) kan skapa redundans.
- Accesspunktsoperatör (AP-operatör).
 - Varje accesspunkt är kritisk för att sända/mottaga meddelanden för den organisation som är ansluten till accesspunkten i fråga. Vid tillfälliga avbrott ska Accesspunkt och meddelandetjänster köa meddelanden för omsändning.

- SDK-federationen (Digg)
 - Adressbok (SDK Adressbok): kritisk gemensam stödtjänst för att möjliggöra adressering av meddelanden. Flera instanser (kluster) kan skapa redundans.
- Konfidentialitet
 - I lösningen ingår både transport- och meddelandekryptering för att minimera risken för att obehöriga kan läsa information som skickas över SDK.
 - Transportkryptering (TLS)
 - Kravställs för intern och extern trafik (C1-C2-C3-C4)
 - AS4 meddelandekryptering (WS-Security AP till AP)
 - a. Kravställs mellan deltagarorganisationers AP-operatörer som tillhandahåller Accesspunkt (C2-C3).
 - b. EU-organisationen CEF har ett certifieringsprogram (CEF eDelivery Conformance Testing) med tillhörande testsviter som syftar till att bedöma om programvara och implementering för accesspunkter möter kraven som är specificerade för eDelivery.
 - Payloadkryptering (kryptering och signering av nyttolast, SDK meddelandet)
 - a. Kravställs innan meddelandet sänds till AP-operatörer för leverans (C1-C4).

För ytterligare beskrivning av de säkerhetsmekanismer som ingår i lösningskonceptet för SDK, se Säkerhetsmekanismer nedan.

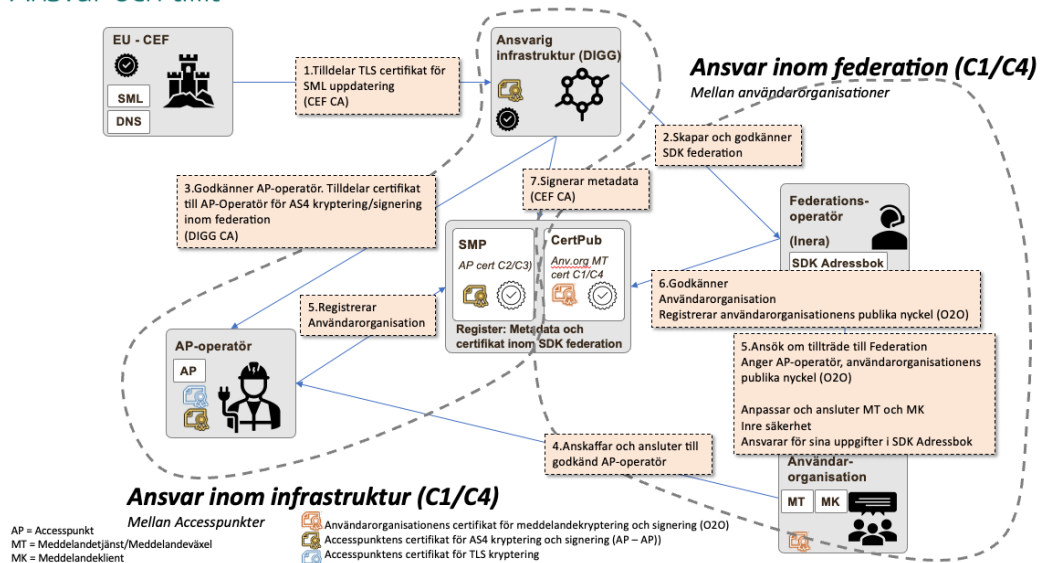
6.2 Säkerhetsmekanismer

6.2.1 Tillitsmodell och ansvar

Att ansluta en deltagarorganisation för meddelandeöverföring inom SDK federationen omfattar efter godkännande bland annat att tillit behöver skapas till aktörer inom SDK federationen och dess transportinfrastruktur.

I praktiken skapas tillitskedjor till godkända certifikatsutgivare samt signerat metadata i gemensamma komponenter (SMP, CertPub).

Ansvar och tillit



Figur: Illustrerad tillitsmodell och ansvar.

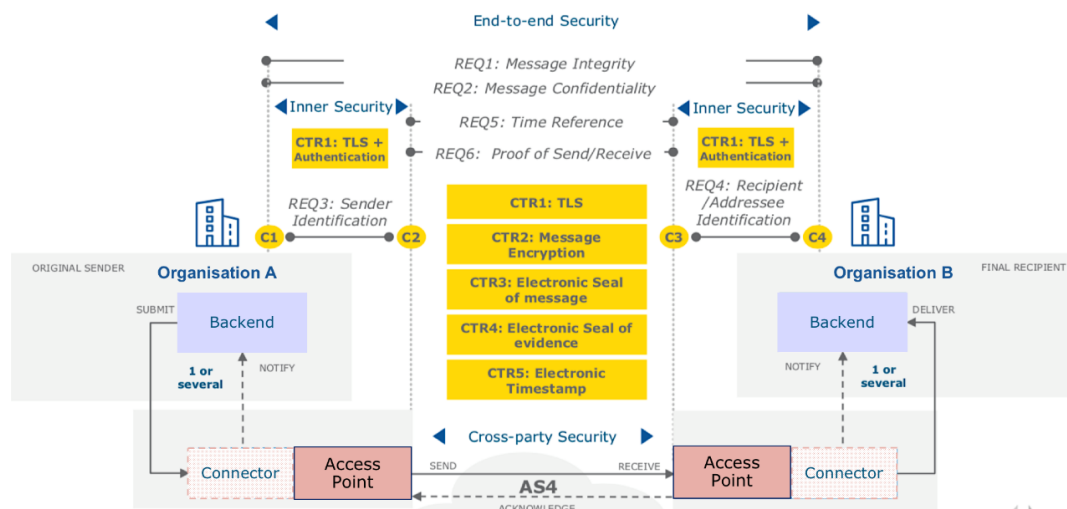
Aktör	Ansvar
Deltagarorganisation (C1/C4)	<p>Ansluter och anskaffar:</p> <ul style="list-style-type: none"> Avropar leverantörer och beställer anpassningar Anskaffar AP-operatör (eller agerar själv AP-operatör)) Ansöker och ansluter till SDK federationen Anskaffar och registrerar certifikat för organisation till organisation (O2O) kryptering och signering <p>Komponenter</p> <ul style="list-style-type: none"> Meddelandeklient Meddelandetjänst <p>Hanterar</p> <ul style="list-style-type: none"> Deltagarorganisationen ansvarar för inre säkerhet (enligt regelverk för anslutning och IT-säkerhetsbilaga) Administrerar uppgifter i SDK Adressbok
Federation/federationsoperatör (SDK)	<p>Federationsoperatör ansvarar för kundkännedom och godkänner deltagarorganisationens anslutning till federationen.</p> <p>Avtal, regelverk, ramverk och tekniska specifikationer</p> <ul style="list-style-type: none"> Ansvarar för <i>gemensamma regelverk inom federationen</i>

	<ul style="list-style-type: none"> • Tekniska specifikationer så som SDK meddelandespecifikation <p>Komponenter</p> <ul style="list-style-type: none"> • <i>Gemensamma komponenter (adressbok, testklient)</i> <p>Hanterar</p> <ul style="list-style-type: none"> • Kontrollerar deltagarorganisationens metadata så som certifikat. • Kontrollerar deltagarorganisationens AP-operatörs metadata. • Anslutningsprocess där deltagarorganisationens följsamhet till regelverk och specifikationer kontrolleras • Support och incidenthantering
AP-operatör (C2/C3)	<p>Ansvarar anslutning av komponent accesspunkt till transportinfrastruktur</p> <p>Avtal, regelverk och och tekniska ramverk.</p> <ul style="list-style-type: none"> • Följsamhet till transportinfrastrukturens regelverk, ramverk och tekniska specifikationer • Ansöker och ansluter till transportinfrastruktur <p>Komponenter</p> <ul style="list-style-type: none"> • Tillhandahåller accesspunkt för anslutning till transportinfrastruktur (eDelivery)
Ansvarig transportinfrastruktur	<p>Ansvarig för federationens transportinfrastruktur:</p> <p>Avtal, regelverk och tekniska ramverk.</p> <ul style="list-style-type: none"> • Sätter krav och avtalar med accesspunktsoperatörer (AP-operatör) • Sätter krav på federationer som vill nyttja denna • Ansvarar för eDelivery området i Sverige. <p>Komponenter</p> <ul style="list-style-type: none"> • Ansvarar för komponenter SMP, SML och DNS (SML och DNS finns hos CEF/DIGITAL) • CA för Accesspunkter (PKI) • Teknisk säkerhet • Signerar godkänt metadata i komponent SMP.

Ansvarig för EU/CEF/DIGITAL eDelivery byggblock	<p>EU-kommissionen levererar en instans av SML till Digg. De drifrar SML:en.</p> <p>Avtal, regelverk och tekniska ramverk.</p> <ul style="list-style-type: none"> eDelivery specifikationer (SML, SMP, AS4) <p>Komponent</p> <ul style="list-style-type: none"> SML DNS <p>Hanterar</p> <ul style="list-style-type: none"> Registreringar olika transportinfrastrukturs registreringar i SML och DNS
-------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6.2.2 Säkerhetsarkitektur för meddelandeöverföring

Basen för säkerhetsarkitekturen för SDK bygger på CEF eDeliverys säkerhetsmodell, som i sin tur består av säkerhetsmekanismer som möter krav i eIDAS-förordningen, se "R8 eIDAS-förordningen" för en sk Electronic Registered Delivery Service.



Figur: Säkerhetsmekanismer (CTRL1-5) vid överföring av meddelanden mappade mot eDelivery 4-hörningsmodell samt mot krav (REQ1-6) i eIDAS-förordningen.

Modellen delar in arkitekturen i säkerhetsområden kopplade till eDeliverys 4-hörningsmodell enligt följande tabell:

Säkerhetsområde	Mappat mot eDelivery	Beskrivning
Inre säkerhet (Inner Security)	Säkerhetsmekanismer mellan C1 och C2, resp. C3 och C4.	Säkerhetsmekanismer vid informationsöverföring mellan organisationens backend-system och accesspunkten.
Organisationsöverskridande säkerhet (Cross-party security)	Säkerhetsmekanismer mellan C2 och C3	Säkerhetsmekanismer vid informationsöverföring mellan olika organisationers AP-operatörs accesspunkter.
End-to-end-säkerhet (End-to-end security)	Säkerhetsmekanismer mellan C1 och C4	Säkerheten vid informationsöverföring mellan sändande organisations backend-system (ursprungligt avsändande system) och mottagarens anslutna backend-system.

Den organisationsöverskridande säkerheten hanteras primärt mellan meddelandetjänster(C1/C4) som tillämpar meddelandekryptering och signering (tillämpar R19 eDelivery - Transportmodell - Utökad Bas) innan meddelanden distribueras deltagarorganisationens AP-operatörens accesspunkter och understöds av AS4-protokollets säkerhetsmekanismer.

Den inre säkerheten regleras av krav på IT-säkerhetsfunktioner genom regelverk för anslutning för SDK informationsutbyte och tillhörande IT-säkerhetskrav. Även accesspunkten måste stödja dessa säkerhetsmekanismer.

Nedanstående tabell beskriver säkerhetsmekanismer (CTR1-5) vid överföring av SDK-meddelanden mer i detalj.

Säkerhetsmekanism	Engelsk term (källa eDelivery)	Säkerhetsområde	Beskrivning (källa CEF eDelivery)
Konfidentialitet - Transportkryptering för insynsskydd under överföring	CTR1: Transport Layer Security (TLS)	Inre samt organisationsöverskridande	Transport Layer Security (TLS 1.2 or 1.3) with Mutual authentication protocol is used, following "Best Practice" guidelines.

			<p>Sender identification is provided by means of</p> <p>using the digital certificate of C2, allowing C3 to identify C2 (and vice versa)</p> <p>using the digital certificate of C1, allowing C2 to identify C1 (same for C4-C3)</p>
Meddelandekryptering, extra lager säkerhet för meddelandet under överföring.	CTR2: Message Encryption	Organisations-överskridande	<p>C2 encrypts the payload of the message using AES-GCM with a random secret key, and the random key with the public key of C3 using RSA-OAEP.</p> <p>Message encryption follows WS-Security using W3C XML Encryption. The used cipher suite for symmetric encryption is: AES GCM-mode, and for asymmetric: RSA-OAEP. This should follow the “Best Practice” guidelines.</p>
Elektronisk stämpel, skydd mot förvanskning av meddelande	CTR3: Electronic Seal of message	Organisations-överskridande	<p>C2 applies an electronic seal to the message header and payload using its own private key which guarantees integrity protection. The seal is verified by C3 using C2 public key for authenticity and non-repudiation of the message payload and headers. Electronic sealing follows WS-Security with W3C XML Signing. The cipher suite is RSA-SHA256.</p>

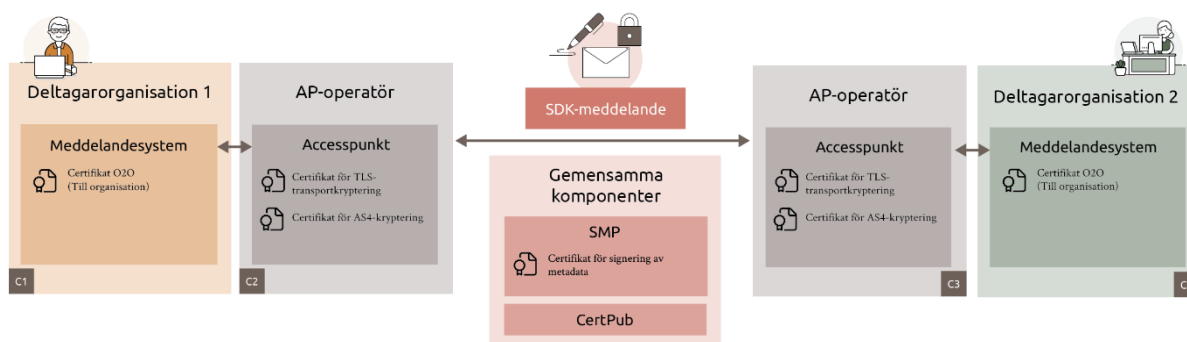
Elektroniskt bevis (kvitto) på överföring av ett visst meddelande	CTR4: Electronic Seal of evidence	Organisations- överskridande	Electronic seal is applied to the receipt (transportkvittensen). Upon reception and verification of a message from C2, C3 generates an evidence receipt based on message identification information (e.g., message identifier, timestamp, and sender metadata) with a new timestamp and a reference to the received message, applies an electronic seal and returns the sealed evidence to C2. The receipt is sent automatically to C2 as a “signal” message response to the initial message. Electronic sealing follows WS-Security with W3C XML Signing. The used cipher suite is: RSA-SHA256.
Tidsstämpling	CTR5: Electronic Timestamp	Organisations- överskridande	Timestamp is placed at the WS-Security header, and it is electronically sealed for integrity protection. At this moment, by default, it is not a qualified time stamp and it relies on the system clock. Stämplingen baseras på accesspunktens systemklocka. Krav finns i regelverk för anslutning för att accesspunkten synkroniseras mot en tillförlitlig tidskälla.

För en detaljerad beskrivning hur säkerhetsmekanismerna mappar mot reglering i eIDAS (R8 eIDAS-förordningen), se “R9 eDelivery Security Controls Guidelines”.

6.2.3 Säkerhetscertifikat för meddelandeöverföring

För att åstadkomma de beskrivna säkerhetsmekanismerna krävs ett antal säkerhetscertifikat för kommuniserande IT-system och en tillit till dessa certifikat (trust).

- Transport kryptering (TLS)
- Signering av metadata i Metadatatjänst (SMP) och Certifikatspubliceringstjänst (CertPub, del av SMP)
- AS4 meddelande kryptering (WS-Security AP till AP)
- Payload kryptering och signering (Kryptering och signering av nyttolast, SDK meddelandet)



Figur: Säkerhetscertifikat som stöd för säker överföring av meddelanden.

Område	Säkerhetsmekanism	Certifikat
Organisationsöverskridande säkerhet (Cross-party security)	Transport kryptering (TLS) Transportkryptering för intern och extern trafik (C1-C2-C3-C4)	Godkända certifikat regleras av ansvarig för transportinfrastrukturen (Digg). Godkända certifikat regleras i R16 eDelivery - Transportprofil AS4.
Organisationsöverskridande säkerhet (Cross-party security)	AS4 meddelande kryptering (WS-Security AP till AP) AS4 kryptering och signering mellan deltagarorganisationers AP-operatörer som	Certifikat representerar AP-operatörens identitet (C2/C3) Godkända certifikat regleras av ansvarig för transportinfrastrukturen (Digg). Godkända certifikat regleras i R14

	<p>tillhandahåller Accesspunkt (C2-C3).</p> <p>EU-organisationen CEF har ett certifieringsprogram (CEF eDelivery Conformance Testing) med tillhörande testsviter som syftar till att bedöma om programvara och implementering för accesspunkter möter kraven som är specificerade för eDelivery.</p>	<p>eDelivery - PKI för Accesspunkter</p> <p>Tjänstebeskrivning.</p>
<p>End-to-end-säkerhet</p> <p>(End-to-end security eller Organisation-till-organisation, O2O)</p>	<p>Payload kryptering och signering (Nyttolast, SDK meddelandet)</p> <p>Meddelande kryptering och signering av meddelandet innan det sänds till deltagarorganisationens AP-operatörer för leverans (C1-C4).</p>	<p>Certifikat representerar deltagarorganisationens identitet (C1/C4).</p> <p>Godkända certifikat regleras av federationsägaren.</p>

6.2.4 Säkerhetsarkitektur för organisation-till-organisation säkerhet

Basen för organisation-till-organisation (End-to-end security) säkerhet baseras på "Transportmodell - Utökad Bas" där meddelandet krypteras och signeras av deltagarorganisationens meddelandetjänst. Meddelande krypteras innan det lämnas till transportinfrastruktur (dvs deltagarorganisationens AP-operatör). Det innebär att endast avsedd mottagande deltagarorganisation kan ta del av (dekryptera) meddelandet. Mottagaren kan också kontrollera avsändarens identitet genom meddelandets signatur i kombination med kontroller mot certifikatspubliceringstjänsten (CertPub).

“eDelivery - Kuverteringsprofil XHE” specificerar hur signering och kryptering skall tillämpas av meddelandetjänst. Se R17 eDelivery - Kuverteringsprofil XHE.

Övergripande flöde:

- Sändarens meddelandetjänst (C1) krypterar och signerar meddelandet innan meddelandet lämnas till deltagarorganisationens AP-operatörs accesspunkt.
 - Mottagarens (deltagarorganisation) publika nyckel hämtas från federationens tillförlitliga källa för metadata Certifikatspubliceringstjänsten (CertPub). Se R18 eDelivery - Certifikatspublicering - REST-bindning till SMP
- Mottagarens meddelandetjänst (C4) hämtar meddelandet från Accesspunkt samt dekrypterar meddelandet och validerar sändarens signatur.
 - Sändarens publika nyckel hämtas från federationens tillförlitliga källa för metadata Certifikatspubliceringstjänsten (CertPub). Se R18 eDelivery - Certifikatspublicering - REST-bindning till SMP
 - Utför spärrkontroll av sändarens certifikat.

6.2.5 Säkerhet vid administration och sökning av adressinformation och metadata

Adressuppgifterna i sig, organisationens kontaktyta/adress osv, är till för att utbytas med andra parter och betraktas enligt informationssäkerhetsklassning som publika uppgifter (Nivå 0 – Försumbar). Det är dock mycket viktigt att dessa skyddas emot förvanskning eller obehörig manipulation, dvs dataintegriteten är i central. Dataintegritet hanteras primärt genom att enbart behörig och starkt autentiserad administratör har rättighet att uppdatera uppgifterna.

Administratörsbehörighet för deltagarorganisationer tilldelas av federationsägaren i central förvaltning för gemensamma komponenter. Myndigheten Digg ansvarar här för tilldelning av konton och behörigheter i SMP-tjänsten och certifikatpubliceringstjänsten. Federationsoperatör (Digg) för SDK ansvarar för konton och behörigheter avseende SDK adressbok. En lokal administratör begränsas till att administrera uppgifter som hör till den egna organisationen.

Det är även mycket viktigt att det går att lita på den källa som levererar uppgifterna. Detta hanteras genom att tjänsterna är säkrade med certifikat; vid uppslag kan klienter verifiera avsändaren. Service metadata och Certifikatspubliceringstjänst (CertPub) är dessutom signerad när det hämtas från SMP-tjänsten.

6.3 Insynskydd (kryptering)

Krav på skyddsmekanismer, algoritmer och nyckellängder för kryptering osv, finns specificerade i IT-säkerhetsbilagan som ingår i regelverk för deltagarorganisationer inom SDK. Riktlinjerna baseras på best-practise och riktlinjer från normerande organisationer för IT-säkerhet som <https://www.enisa.europa.eu>.

6.4 Riktighet

Skyddsmekanismer för säkerställande av riktighet med avseende på överförd information, metadata och adresseringsdata specificeras i IT-säkerhetsbilagan. Förutom det skydd som krypteringen ger under transport, används även elektronisk stämpel mellan accesspunkterna, en digital signatur som ger extra skydd mot förvanskning av meddelanden och kvittenser.

6.5 Autentisering

Kontroll av användarnas elektroniska identiteter vid användande av SDK finns kravställt i regelverk för deltagarorganisationer inom SDK.

Alla ingående systemkomponenter ska autentiseras enligt regelverk för deltagarorganisationer. Av IT-säkerhetsbilagan regleras vilka certifikatutfärdare som är godkända. AP-operatörer och deras accesspunkter måste godkännas och certifikat måste registreras innan de kan användas för meddelandeutbyte inom SDK federationen.

6.6 Spårbarhet (loggning)

I regelverk för deltagarorganisationer inom SDK finns krav på spårbarhetskrav specificerat. Spårbarhet sker i form av loggning i accesspunkter.

7 Informationshantering

7.1 Informationsmodeller

7.1.1 Informationsmodell för adressinformation

Se adressbokens sök-API för detaljerad information om adressboken. SDK adressbok medger att varje deltagarorganisation kan ha noll eller flera adresserbara funktioner. I praktiken bör det sättas krav på att minst en funktionsadress registreras per organisation för att öka tydligheten vad som kan adresseras för deltagarorganisation, t.ex. en registratorfunktion.

Deltagarorganisationer och funktioner kan l a bvidare beskrivas med:

- en unik identifierare
- kortfattat namn
- en längre beskrivande text, t.ex för att beskriva vad funktionen representerar

Funktioner kan vidare fördes med:

- en eller flera kategorier
- Sökord från standardiserade kodverk

Sökord och sökkoder, utifrån definierade kodverk, kan användas för att filtrera och söka ut mottagare och dess funktioner baserat på vad funktionen hanterar eller kan associeras med. Det är upp till varje deltagarorganisation att bestämma vilka funktioner som ska finnas i adressboken.

Primärt identifieras en organisation med en domänidentifierare, t ex <http://sollentuna.se> för Sollentuna kommun. Ytterligare identifierare kan också registreras, t ex svenskt organisationsnummer för svenska organisationer.

7.1.2 Informationsmodell för SDK meddelande

Ostrukturerat meddelande innehållande avsändare, mottagare, refererad person, refererat ärende, rubrik, text och bilagor. Se SDK Innehållsspecifikation, B1.3.3.

7.1.3 Informationsmodell för meddelandekvittens

Kvittensmeddelande för att kvittera meddelande mottaget eller meddelandet ej mottaget. Se "R20 Digg, eDelivery – Meddelandespecifikation: Meddelandekvittens".

7.2 Informationens ursprung

7.2.1 Information som konsumeras

- Inkommande meddelanden som skickas från en deltagarorganisation tas emot av mottagande deltagarorganisations meddelandetjänst och presenteras i meddelandeklient.
- Inkommande meddelandekvittens som skickats av mottagande deltagarorganisation för att kvittera meddelande, tas emot av mottagande deltagarorganisations meddelandetjänst och presenteras i meddelandeklient.
- Adressinformation hämtas från SDK till en Meddelandetjänst och Meddelandeklient när användare söker efter adressater.
- Metadata (tekniska uppgifter) hämtas från metadatatjänst av accesspunkt vid sändning av meddelande.
- Publik nyckel för meddelandekryptering och validering av avsändarens signatur hämtas från certifikatpubliceringstjänsten (CertPub). Se R18 eDelivery - Certifikatpublicering - REST-bindning till SMP.

7.2.2 Information som skapas

- Meddelande skapas av användare i en organisation.
- Meddelandekvittens skapas av meddelandetjänst i en organisation.
- Adressinformation registreras i SDK Adressbok via behörig administratör.
- Metadata (tekniska uppgifter) registreras i Metadatatjänst.

- Deltagarorganisations publik nyckel för meddelandekryptering och validering av signatur registreras i certifikatpubliceringstjänsten (CertPub). Se R18 eDelivery - Certifikatpublicering - REST-bindning till SMP.
- Spårbarhetsloggar skapas.