EKONOMISTYRNINGSVERKET

Utdrag - Förfrågningsunderlag statliga ramavtal ekonomisystem oktober 2016, avsnitt 5 och 6

5 Krav på Tjänsten - Anbudsområde C – Operatörstjänst för distribution av kundfaktura

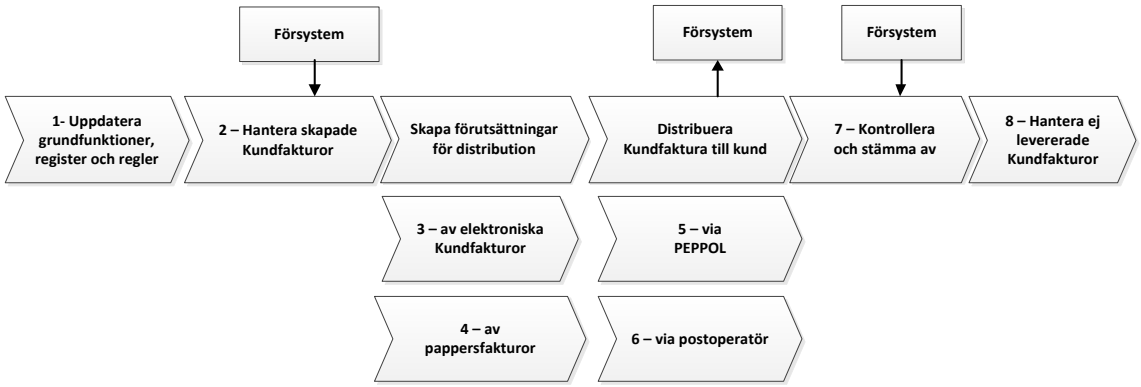
Syftet med Operatörstjänst för distribution av kundfaktura är att hantera distribution av fakturor till myndigheternas kunder, såväl i form av elektroniska fakturor (e-fakturor) som genom fakturautskrift, frankering och distribution via postoperatör. ESV efterfrågar en modern lösning som kan möta både dagens krav och kommande krav.

Sedan 2008 finns krav på att alla myndigheter ska ha kapacitet att fakturera elektroniskt och senast den 1 november 2018 ska de kunna använda PEPPOL:s infrastruktur för att skicka och ta emot elektroniska meddelanden.

Myndigheterna behöver en enkel lösning för att fakturera sina kunder via PEPPOL. E-fakturering ska gå lika enkelt som att skicka e-post, utan krångliga konfigureringar av partsuppsättningar. Den elektroniska adressen samt aktuellt fakturaformat är en naturlig del av kundinformationen i ekonomisystemet.

Se även avsnitt 6 Icke-funktionella krav, kravlista för Anbudsområde C.

5.1 J - Operatörstjänst för distribution av kundfaktura



Operatörstjänst för distribution av kundfaktura hanterar kundfakturaflödet. Från att ta emot myndighetens Kundfakturor i elektronisk form till att säkerställa att de når kunden på angivet sätt. Tjänsten omfattar även utskrift och förmedling av Kundfakturor via postoperatör samt vid behov andra typer av förmedlingssätt för elektroniska Kundfakturor som Leverantören kan erbjuda.

Operatörstjänst för distribution av kundfaktura tar emot Kundfakturor från ekonomisystem som ingår i ESV:s ramavtal, men även från andra system och lösningar.

Processen bygger på att Leverantören är ansluten till PEPPOL:s infrastruktur samt anlitar en postoperatör.

5.1.1 Uppdatera grundfunktioner, register och regler

Uppdateringen av grundfunktioner, register och regler handlar till exempel om att publicera uppgifter i Operatörstjänstens eget eller i ett externt SMP-register (Service Metadata Publisher) och att ange vad som ska signalera utskrift på eventuella kundanpassade fakturablanketter.

Myndigheten väljer om Leverantörens SMP eller extern SMP ska användas. Om myndigheten redan använder PEPPOL och därmed har en befintlig accesspunkt och SMP (Service Metadata Publisher) för utväxling av andra meddelanden än de som är aktuella för detta ramavtal kan Leverantörens accesspunkt använda denna externa SMP istället för den egna. På motsvarande sätt kan Leverantören tillåta att myndigheten använder Leverantörens SMP för registrering av mottagningsformat som hanteras i annan accesspunkt.

5.1.2 Ta emot elektroniska Kundfakturor

Operatörstjänst tar emot elektroniska Kundfakturor som myndigheten skapar i sitt ekonomisystem, Ekonomisystem med lokal drift eller annat Försystem, och ger myndigheten stöd för att verifiera att mottagandet har fungerat.

Fakturorna har något av de det format som myndigheter ska kunna skicka enligt aktuella föreskrifter, till exempel SFTI Svefaktura BIS 5A 2.0, och innehåller de uppgifter som behövs för att de ska kunna förmedlas till kund på rätt sätt. Fälten på fakturan används i enlighet med SFTI:s rekommendationer och vägledningar och de skickas förpackade i ett tekniskt kuvert.

5.1.3 Skapa förutsättningar för distribution

Elektroniska Kundfakturor valideras enligt de regler som finns för distribution via PEPPOL. Övriga Kundfakturor skrivs ut och frankeras enligt reglerna.

5.1.4 Distribuera Kundfaktura till kund

Elektroniska Kundfakturor distribueras via PEPPOL till kundens mottagningspunkt. Övriga Kundfakturor skrivs ut, frankeras och förmedlas via en postoperatör till kundens fysiska fakturaadress.

5.1.5 Kontrollera och stämma av

Myndigheten har stöd för att stämma av att Tjänsten har distribuerat de Kundfakturor som har tagits emot.

Leverantören hanterar och agerar på PEPPOL:s kvittenser på distribuerade elektroniska fakturor. Myndigheten får en tydlig beskrivning av eventuella distributionsproblem som de själva måste hantera.

5.1.6 Hantera ej levererade Kundfakturor

Myndigheten kan hantera eventuella distributionsproblem genom att till exempel kontakta kunden för att få en korrekt adress, partsidentitet eller fysisk fakturaadress. Leverantören hanterar eventuella tekniska problem.

5.1.7 Principer för meddelandeutväxling

Nedanstående principer ska tillämpas för informationsutbyte med andra operatörer och motsvarande.

- Affärsparterna kan använda vilken operatör de vill förutsatt att de är anslutna till PEPPOL:s infrastruktur.
- Det utväxlingsformat för meddelanden som används mellan operatörerna överenskoms mellan affärsparterna. I vissa avseenden regleras för PEPPOL användning av specifika format (PEPPOL BIS).
- Operatörerna agerar på uppdrag av respektive affärspart.
- Respektive affärspart står endast för kostnaderna för sin egen operatör.
- Ett meddelande anses vara mottagaren tillhanda då det nått den operatör som mottagaren har angivit som sin mottagningspunkt.
- Det format som utväxlats är att betrakta som det mottagna formatet (operatörer kan inte använda annat format än det som affärsparterna angett).
- Konvertering av det mottagna formatet till annat format får endast göras på explicit uppdrag från myndigheten.
- Alla utgående meddelanden valideras före avsändning. Eventuella valideringsfel flaggas upp och återkopplas till användaren.
- Alla inkommande meddelanden valideras. Eventuella valideringsfel rapporteras tillbaka till avsändaren (antingen affärsparten eller dess operatör). Återkoppling kan göras via e-post, telefon eller med strukturerat kvittensmeddelande som exempelvis PEPPOL MLR.

Leverantören erbjuder en accesspunkt och SMP som är godkänd och ansluten till PEPPOLs infrastruktur. Regler för samtrafik beskrivs i PEPPOLs infrastrukturavtal och dessa måste följas. Det innebär att operatören alltid måste stödja aktuella versioner av protokoll, kvittenser och format i accesspunkten.

Detta ramavtal förhindrar inte Leverantören att erbjuda tjänster till andra än de som omfattas av ramavtalet. Leverantören äger dock inte rätt att begära eller ta ut ersättning av myndighets kund och eller annan aktör som kunden anlitar för tjänster kring elektroniskt informationsutbyte, för deras deltagande i myndighets användning av Tjänsten enligt detta ramavtal.

6 Icke-funktionella krav

Avsnitten nedan beskriver icke-funktionella krav för de tre Anbudsområdena.

För varje huvudrubrik nedan återfinns motsvarande huvudrubrik i kravspecifikationen avseende icke-funktionella krav. För underrubrikerna nedan finns inte alltid någon motsvarande underrubrik i kravspecifikationen avseende icke-funktionella krav.

Se även kravlistor för respektive anbudsområde, fliken Icke-funktionella krav.

6.1 Införandeprojekt

Leverans av Avropad Tjänst ska genomföras inom ramen för ett Införandeprojekt. Leverantören har ett helhetsansvar för planering, koordinering och genomförande av de aktiviteter som krävs för införandet av Tjänsten i enlighet med tecknat Avropsavtal. Leverantören har en utsedd projektledare för Införandeprojekt.

Införandeprojektet omfattar installation, validering och utbildning. Följande punkter ingår i Leverantörens ansvar:

- Projektledning
- Initial kartläggning
- Systemuppsättning och parametersättning
- Teknisk installation (gäller endast Anbudsområde B)
- Kontroll och validering inför leverans
- Utbildning av Fullanvändare (som sedan i sin tur utbildar övriga användare hos myndigheten)
- Tester, leveransprov och leveransgodkännande
- Framtagning av kundunika rapporter
- Stöd vid konvertering och migrering av data/historik
- Avtalade integrationer
- Stöd vid driftstart
- Kundunika anpassningar (om Avropsavtal innefattar sådana)

Ovanstående beskrivning av Införandeprojekt omfattar alla typer av Avropade myndigheter.

Införandeprojekt vid Avrop av Statens servicecenter respektive Kundmyndighet omfattar samma ansvar och aktiviteter, men med följande skillnader avseende införandeprojekts upplägg och omfång.

- Införandeprojekt för Statens servicecenter avser projekt för initial grunduppsättning av Tjänsten vid Statens servicecenter, tillsammans med ett första införande av en eller flera Kundmyndigheter. Grunduppsättningen avser att möjliggöra och underlätta framtida anslutning av ytterligare Kundmyndigheter.
- Införandeprojekt för Kundmyndighet avser projekt för anslutning av Kundmyndigheter till en befintlig grunduppsättning av Tjänsten vid Statens servicecenter.

6.2 Migrering av data

Med begreppet migrering avses här processen att extrahera information (och beskrivande tekniska data) ur ett system och sedan ladda in/importera informationen i ett nytt system. I processen förekommer ofta att transformering/anpassning görs av informationens struktur för att överbrygga olikheter i systemen.

Myndigheten kan komma att genomgå flera migreringsprocesser under avtalstiden. Initialt behöver tjänsten laddas med information från myndighetens nuvarande lösningar. Vid avtalets slut kommer myndigheten behöva extrahera information för att kunna migrera till en ny lösning. Under avtalstiden kan det även förekomma att myndigheten behöver göra extraheringar av information av andra orsaker, exempelvis om verksamheter slås samman eller delas.

6.2.1 Import av information

Import av information till Leverantörens Tjänst görs efter en plan som beskriver de tekniska förutsättningar som gäller inklusive vilket sätt data ska vara strukturerat för import genom att specificera tillgängliga fält, fältlängder och formateringskrav. Leverantören är ansvarig för att ta fram förslag på plan.

Laddning/import till Tjänsten kan behöva göras vid flera tillfällen för att myndigheten ska kunna kvalitetssäkra och verifiera riktigheten i migreringen.

6.2.2 Export av information

Inför avveckling samråder myndigheten och Leverantören om hur och när avvecklingen ska genomföras. Avvecklingen genomförs sedan enligt en plan som parterna kommer överens om. I planen för avveckling framgår tider, aktiviteter, resurser, ansvarsfördelning och viktiga milstolpar.

Leverantören samverkar med myndigheten och eventuell ny tjänsteleverantör i arbetet.

Export av information och inläsning i ny tjänst/system behöver testas och kvalitetssäkras. Därför kan myndigheten behöva begära ut export av information vid fler än ett tillfälle under en migreringsfas.

6.3 Integration mellan myndighetens system

Integration mellan myndighetens egna system och tjänster görs på flera sätt. I vissa fall kan traditionell filöverföring med SFTP användas, i andra fall kan systemen kommunicera direkt med webtjänster eller motsvarande API. Både XML-baserade och sekventiella filer kan användas för att importera och exportera information.

Integration med systemstöd för e-arkiv kan på sikt underlättas genom att de system och tjänster som upphandlas här framöver stödjer specifikationer för e-arkiv som tas fram i Riksarkivets arbete med så kallade Förvaltningsgemensamma specifikationer. Även andra informationsutbyten mellan myndigheters system kan komma att beskrivas i Förvaltningsgemensamma specifikationer.

För integrationer där Förvaltningsgemensamma specifikationer saknas gäller som huvudregel att mottagande/inläsande system definierar det format som ska användas.

6.4 Informationssäkerhet

Informationssäkerhet är en avgörande faktor för att kunderna ska kunna upprätthålla de processer som de aktuella tjänsterna eller programvaran stödjer. Kunderna har också starka externa krav, bland annat från lagstiftning och på säkerhet i sin egen verksamhet. Dessa krav behöver tillgodoses även i de tjänster som upphandlas.

Leverantören behöver ha ett riskbaserat informationssäkerhetsarbete som både omfattar den interna organisationen och de produkter och tjänster som levereras. Leverantören förväntas även ha ett aktivt säkerhetsarbete så att nuvarande säkerhetsnivå upprätthålls, samt utveckla nya säkerhetslösningar vid förändringar avseende hot och risker. Nya organisatoriska och tekniska möjligheter behöver också tillvaratas i säkerhetsarbetet.

6.4.1 Generella regler och riktlinjer

Leverantören måste vara förtrogen med de regelverk som kunderna har att följa när det gäller informationssäkerhet. Med detta avses bland annat personuppgiftslagen (PUL) och den kommande dataskyddsförordningen (EU 2016/679). Det är nödvändigt att leverantören är insatt i kraven i Myndigheten för samhällsskydd och beredskaps (MSB:s) föreskrifter rörande systematisk informationssäkerhet (MSBFS 2016:1), rörande obligatoriskt it-incidentrapportering (MSBFS 2016:2) och rörande risk- och sårbarhetsanalyser (MSBFS 2015:3).

För att leverantören ska kunna ha en god samsyn med kunderna om inriktningen på informationssäkerhetsarbetet bör Leverantören använda MSB:s vägledningar om processorienterad informationskartläggning, om informationssäkerhet i upphandling och fysisk informationssäkerhet i it-utrymmen.

6.4.2 Fysiskt skydd [endast för molntjänst och vid driftservice]

Leverantören ansvarar för att driftmiljön är omgärdad av relevant skalskydd inklusive tillträdesskydd för att säkerställa att endast behörig personal har fysiskt tillträde. Utöver tillträdesskydd behöver Leverantören även vidta andra lämpliga åtgärder för att skydda driftmiljön och därmed reducera risker för bristande tillgänglighet och andra säkerhetsproblem i leveransen. Leverantören kan lämpligen utgå från MSB:s Vägledning för fysisk informationssäkerhet i it-utrymmen för att beskriva hur man arbetar med fysisk säkerhet.

6.4.3 Krav på informationssäkerhet i Tjänsten

För att kunna tillgodose kraven på informationssäkerhet är det en förutsättning att Leverantören har en dokumenterad säkerhetsorganisation, med som lägst följande komponenter.

Område	Beskrivning
Ledningssystem	Leverantören förutsätts bedriva ett strukturerat arbete för att upprätthålla en god informationssäkerhet i de levererade tjänsterna. Som en del i detta måste leverantören ha ett ledningssystem för informationssäkerhet utvecklat enligt ISO/IEC 27002 eller motsvarande. Leverantören förväntas kunna redovisa hur man arbetar med informationssäkerhet antingen genom intyg från en utomstående revision eller genom en redovisning med bilagda exempel på styrande dokument.
Säkerhetsorganisation	Leverantören förutsätts ha en säkerhetsorganisation som fastställer olika roller med ansvar för informationssäkerhet i verksamhet och tjänster.
Leverantörens kompetens	Det behöver finnas en ansvarig för området informationssäkerhet hos leverantören. Den informationssäkerhetsansvariga ska dels ha en generellt god kompetens inom området och dels ha möjlighet att tillägna sig de krav på, samt förutsättningar för, säkerhet som finns hos kunderna. Leverantören förväntas genomföra regelbunden utbildning om ledningssystemet samt aktuella risker inom informationssäkerhetsområdet för de medarbetare som har arbetsuppgifter relaterade till de tjänster som hanterar kundernas information.
Riskhantering	Leverantören behöver bedriva ett aktivt arbete för att identifiera risker för informationshantering i verksamhet och i tjänster. Riskanalyser ska ske efter fastställd metod och genomföras regelbundet. Leverantören måste ha metod och rutiner för att hantera och följa upp identifierade risker. I leverantörens riskhantering behöver hänsyn tas till risker för kunderna.
Regler för upphandling och utveckling	Leverantören behöver ha riktlinjer för hur informationssäkerhetsaspekter ska integreras vid utveckling och upphandling av produkter och tjänster som används för informationshantering.

6.4.4 Kontinuitetshantering

Kontinuitetshantering beskriver de åtgärder som krävs för att säkra att Tjänsten görs tillgänglig efter att en allvarlig driftsstörning har inträffat. Leverantören

behöver ha en dokumenterad plan för kontinuitetshantering som omfattar bland annat

- Kontinuerlig riskanalys
- Eskalering
- Prioritering
- Beroendeförhållanden
- Rapportering
- Dedikerade resurser
- Åtgärder för att undvika informationsförluster

I detta ingår även att beskriva åtgärder vidtagna för att skapa redundans. Åtgärder som kan vara aktuella för att reducera risken för informationsförluster inkluderar (men är inte begränsade till):

- Upprättande av en krisorganisation som har ansvar för att hantera störningar och säkerställa kontinuerlig drift
- Upprättande av reservkapacitet genom sekundärplats för säkerställande av drift
- Tillgång till alternativa överföringskanaler för kommunikation

Leverantören behöver genomföra egna övningar av planerad kontinuitetshantering samt vid behov kunna delta i kundens övningar av kontinuitetshantering.

Leverantören förutsätts kunna genomföra egen utvärdering efter störningar, utvärdera sitt eget arbete samt informera myndigheten om de erfarenheter som gjorts och eventuella åtgärder för att reducera risken för ytterligare störningar.

6.4.5 Efterlevnadskontroll

Kontroll av efterlevnad är nödvändig för att ett systematiskt informations-säkerhetsarbete ska fungera och brister kunna åtgärdas. Leverantören förväntas ha dokumenterade rutiner för uppföljning av informationssäkerhet. Uppföljningen består av kontroll av efterlevnaden av de regler som gäller för den egna verksamheten och av efterlevnaden av de regler och villkor som gäller för de system och tjänster som levereras. Uppföljning förväntas ske minst en gång årligen. Den interna uppföljningen bör kompletteras med regelbundna externa revisioner.

Leverantören behöver ta fram prioriterade åtgärdsplaner för att åtgärda de brister som framkommit vid uppföljningarna. Kunderna bör få en möjlighet att påverka Leverantörens prioritering av åtgärd utifrån den riskbedömning för egna verksamheten som kunden gör.

6.4.6 Arkivering

Arkivlagen gäller för myndigheten och skall tillämpas när det gäller hantering av information inklusive räkenskapsinformation. Den information som hanteras i tjänsten ska skyddas, vara sökbara, kunna gallras och kunna lämnas ut enligt myndighetens regler. Av särskild betydelse är att beakta att delar av räkenskapsinformationen ska vara tillgängliga för insyn på kort och lång sikt och att Riksarkivet ska ha en möjlighet att uppfylla sin skyldighet att inspektera informationen.

Gallring av allmänna handlingar får endast ske efter ett gallringsbeslut. Ett gallringsbeslut ger inte bara möjlighet att destruera handlingen utan betyder att destruktionen skall genomföras. Liksom för övriga allmänna handlingar är det att betrakta som gallring om den ursprungliga handlingen överförs till annat medium och originalet förstörs. I detta sammanhang skall fakturor bevaras i pappersform även om de skannats in. En faktura som inkommer i elektronisk form behöver kunna bevaras i detta format.

Det ska vara möjligt att kunna gallra information enligt vad som anges av Riksarkivet i form av RA-FS (generella föreskrifter) och RA-MS (myndighetsspecifika beslut).