Vägledning

för avrop av tjänster för

elektronisk identifiering och elektronisk underskrift

från ramavtalsområden inom
Programvaror och Tjänster 2019

Version 2.0 publicerad 2020-04-08

KAMMARKOLLEGIET

Innehåll

Versioner	Publicerat datum	Uppdaterat avsnitt
1.0	2018-04-26	Första version
1.1	2019-02-13	Uppdaterat 2.4.1
2.0	2020-04-08	Referenser ändrade från ramavtalsområdet Informationsförsörjning till de tre nu aktuella ramavtalsområdena. Se avsnitt 1.1 Syfte och omfattning.

1 Vägledningen

1.1 Syfte och omfattning

Genom de ramavtalsupphandlingar som genomfördes under 2019 finns för närvarande möjlighet att avropa e-underskrifter och e-identifiering från tre ramavtalsområden som ingår i familjen av ramavtalsområden inom Programvaror och tjänster (PT19):

Programvarulösningar (PT19-PL)	giltigt som längst till 2023-02-28
Systemutveckling (PT19-SU)	giltigt som längst till 2023-05-31
Vård Skola Omsorg (PT19-VSO)	giltigt som längst till 2023-01-01

Alla ramavtalsleverantörer inom de tre ramavtalsområdena ska, själva och med hjälp av underleverantörer, tillhandahålla funktioner för e-identifiering och för e-underskrifter.

Godkännanden görs tillsammans av Myndigheten för digital förvaltning (DIGG) och Kammarkollegiet av tjänster för e-underskrifter. Godkännandena avser följsamhet mot DIGG:s specifikationer och villkoren i ramavtalen.

Vägledningen beskriver övergripande hur avrop av funktioner för e-identifiering och e-underskrift kan göras från nämnda ramavtalsområden inom familjen Programvaror och tjänster.

Vägledningen tar också upp viktiga saker att tänka på i de olika stegen Planering, Avrop, Införande, Användning och Avslut.

Själva genomförandet av avropet beskrivs endast övergripande. För detaljer kring avropsprocessen hänvisas till den allmänna vägledningen för familjen Programvaror och tjänster. Den återfinns bland stöddokumenten för respektive ramavtalsområde.

För den som använt eller läst dokumentation avseende tidigare generation ramavtal (PT14) är det viktigt att känna till att de nu aktuella ramavtalsområdena (PT19) har både likheter och skillnader i förhållande till de tidigare. Se Allmänna vägledningen avsnitt 1.2 Nyheter.

Juridiska aspekter vid användande av elektroniska legitimationer för identifiering och underskrift tas inte upp i vägledningen. För detta hänvisas till lagstiftning som eIDAS och annan relevant lagstiftning samt eSAM:s juridiska vägledning.

Centrala begrepp

Med **Kund** avses en avropsberättigad organisation som har tecknat Kontrakt.

Med **Avrop** avses anskaffning som Kund gör genom tilldelning av Kontrakt under Ramavtalet.

Med **elektronisk identifiering (e-identifiering)** avses i denna vägledning funktion som erbjuder identifiering med stöd av e-legitimationer. DIGG använder e-legitimering i samma betydelse som e-identifiering.

Med **elektronisk underskrift (e-underskrift)** avses i denna vägledning funktion som erbjuder underskrift med stöd av e-legitimationer i första hand i enlighet med DIGG:s Normativa specifikation för underskriftstjänst. DIGG använder fristående underskriftstjänst i samma bemärkelse som här använda e-underskrift.

eID-tjänster används som ett samlingsbegrepp för de två tjänsterna ovan.

DIGG:s Normativa specifikation för underskriftstjänst är en rekommenderad specifikation som leverantörer av underskrifttjänst kan följa.

1.2 Målgrupp

Vägledningen vänder sig i till strateger, arkitekter, verksamhetsutvecklare, projektledare och upphandlare som planerar för införande och anskaffning av tjänster för e-identifiering och/eller e-underskrift.

Läsaren bör ha en allmän kunskap om vad e-legitimationer är och hur dessa kan användas i tjänster för identifiering av användare och för att göra e-underskrifter. Läsaren bör också ha en allmän kunskap om ramavtal och avrop från ramavtal.

2 Programvaror och tjänster – en familj av ramavtalsområden

2.1 Några aktörers ansvar

Kort om ramavtalsleverantörens ansvar mot avropande organisation samt Kammarkollegiet och DIGG:s ansvar i sammanhanget.

Ramavtalsleverantören har ett helhetsansvar gentemot den avropande organisationen för att tjänsterna uppfyller de krav som ställs. Hantering av bolag som bidrar med ekonomisk eller teknisk kapacitet har ändrats i de nu gällande ramavtalen i förhållande till hur de tidigare hanterades. Se avsnitt 1.2.5 Åberopade företag och underleverantörer i den allmänna vägledningen.

Kammarkollegiet har bland annat till uppgift att effektivisera den offentliga förvaltningen genom att ingå ramavtal. Kammarkollegiet ansvarar för ramavtalen.

DIGG har till uppgift att stödja och samordna offentlig sektor i frågor som rör e-identifiering och e-underskrift. DIGG ansvarar bland annat för kravdokumenten tekniska ramverk samt den normativa specifikationen för underskriftstjänsten.

2.2 Ramavtalsområden i familjen Programvaror och tjänster

Övergripande om ramavtalen i de ramavtalsområden som ingår i familjen Programvaror och tjänster. och sådant som bedöms som intressanta i samband med avrop av tjänster för e-identifiering och e-underskrift.

Ramavtalen ger förutsättningar för de upphandlingsjuridiska frågorna och för ansvar i tillhandahållandet av tjänster, support och icke funktionella krav i de allmänna och specifika villkor som finns i ramavtalet. Det är dock väldigt viktigt att den avropande organisationen stämmer av de förutsättningar som ges i ramavtalet med de egna behoven och önskemålen. Den avropande organisationen måste också sätta sig in i vilka villkor i ramavtalen och dess bilagor som kan preciseras och förtydligas vid avrop och hur man avser att beskriva de egna kraven och villkoren.

Ramavtalen är kravställda på funktionell nivå och anger inte hur de specifika tjänsterna eller funktionerna ska fungera i detalj eller hur dessa ska tillhandahållas. Att ta fram krav och beskrivningar av efterfrågade tjänster är ett arbete som den avropande organisation måste göra själv, och/eller genom att i samverkan med andra organisationer ta fram gemensamma kravställningar. När det gäller en fristående e-underskriftstjänst tas specifikationer fram av DIGG.

2.2.1 Ramavtalens omfattning

Funktioner för e-identifiering och e-underskrifter kan avropas från nämnda ramavtalsområden som ingår i familjen Programvaror och tjänster. Dessa ramavtalsområden omfattar programvaror, publik molntjänst, privat molntjänst, konsulttjänster. https://www.avropa.se/ramavtal/ramavtalsomraden/it-och-telekom/Programvaror-och-tjanster/. De omfattar i vissa fall licenstjänster och i visst fall inte privata molntjänster. Se bilaga 1. För respektive ramavtalsområde finns en Kravkatalog.

- Konsulttjänsterna kan avropas som resurstjänst, teamtjänst eller uppdragstjänst.
- Programvaror kan ha proprietär karaktär eller utgöras av öppna programvaror.
- Tjänster kan avropas som publik molntjänst eller som privat molntjänst.
- Med publik molntjänst avses en standardiserad tjänst som tillhandahålls över internet, som inte är anpassad för specifik kund. Se Allmänna villkor avsnitt 2 Definitioner och Särskilda villkor för Publik molntjänst.
- Med privat molntjänst avses en it-miljö för kund med ingående konsult- och supporttjänst. Se Allmnna villkor avsnitt 2 Definitioner och Särskilda villkor för Privat molntjänst.
- Notera att Avrop av Privat molntjänst där annan än Ramavtalsleverantör eller dess Drifttjänstleverantör tillhandahåller Drifttjänst inte är möjligt i detta Ramavtal. Ramavtalsleverantör eller dess Konsulttjänstleverantör kan som en del av Konsulttjänsten systemförvaltning ansvara för applikationsdrift i Kunds lokal.

2.2.2 Viktiga delar i ramavtalet

Att köpa tjänst innebär att leverantören tillhandahåller en funktion till kunden. Leverantören äger och underhåller den bakomliggande tekniska plattformen samt levererar det stöd och support som behövs för att använda tjänsten.

De aktuella ramavtalen omfattar ett antal kravområden för att ge den avropande organisationen ett stöd vid avrop och användande av tjänst. Nedan en kort beskrivning av de viktigaste delarna.

Helhetsansvar

Ramavtalsleverantören ska ta ett helhetsansvar för det som avropas inklusive integration mellan samtliga ingående delar.

> Med avseende på eID-tjänsterna innebär detta att Kund i normal fallet endast behöver kravställa organisationens behov på en funktionell nivå.

Allmänna villkor

Allmänna villkor är en ramavtalsbilaga som alltid ingår i det kontrakt som tecknas vid avrop från ramavtalet oavsett om den hänvisas till eller ej. Av allmänna villkor framgår bland annat villkor för följande områden:

- Övergripande hur leverans ska gå till med delar som tidsperioder, tester, godkännande, avtalad och effektiv leveransdag.
- Försening, när det uppstår och ansvar i detta.
- Fel, åtgärdande av fel och support.
- Sekretess och säkerhet.
- Immateriella rättigheter och intrång.
- Behandling av personuppgifter och att separat personuppgiftsbiträdesavtal ska tecknas vid behov. I ramavtalet finns exempel på sådant avtal.
- Befrielsegrund, ansvarsbegränsning och försäkring.
- Villkor vid kontraktets upphörande. Vid behov bör parternas åtaganden vid kontraktets upphörande dokumenteras som en del av kontraktet.

Med avseende på eID tjänsterna innebär detta att viktiga villkor redan finns på plats, och oftast är hållna på en nivå som passar flertalet kunder. Där Kund har särskilda behov ger ramavtalet vissa möjligheter till anpassning eller precisering.
Se avsnitt 1 Inledning.

Särskilda villkor

Särskilda villkor kompletterar Allmänna villkor och utgör en del av kontraktet. Det finns särskilda villkor för respektive sätt tjänsten eller produkten ska levereras på. Fler särskilda villkor kan bli aktuella i samma kontrakt. Se respektive ramavtalsområdes sida:

https://www.avropa.se/ramavtal/ramavtalsomraden/it-och-telekom/Programvaror-och-tjanster/

Särskilda villkor kompletterar allmänna villkor i bland annat följande:

- Leverans och servicenivåer. Vid avrop av tjänst bör servicenivåer preciseras ytterligare i kontraktet genom ett särskilt servicenivåavtal (SLA).
- Säkerhet och behandling av kunds information,
- Kunds tillgång till sin egen information.

Med avseende på eID-tjänsterna innebär detta att Kund kan specificera krav och precisera villkoren vad gäller servicenivåer eller säkerhetsnivåer för att passa den egna organisationens behov

2.2.3 Avrop genom förnyad konkurrensutsättning

Vid avrop ska förnyad konkurrensutsättning tillämpas. Förnyad konkurrensutsättning sker genom att avropande organisation skickar en skriftlig avropsförfrågan samtidigt till samtliga ramavtalsleverantörer.

2.2.4 Prismodell

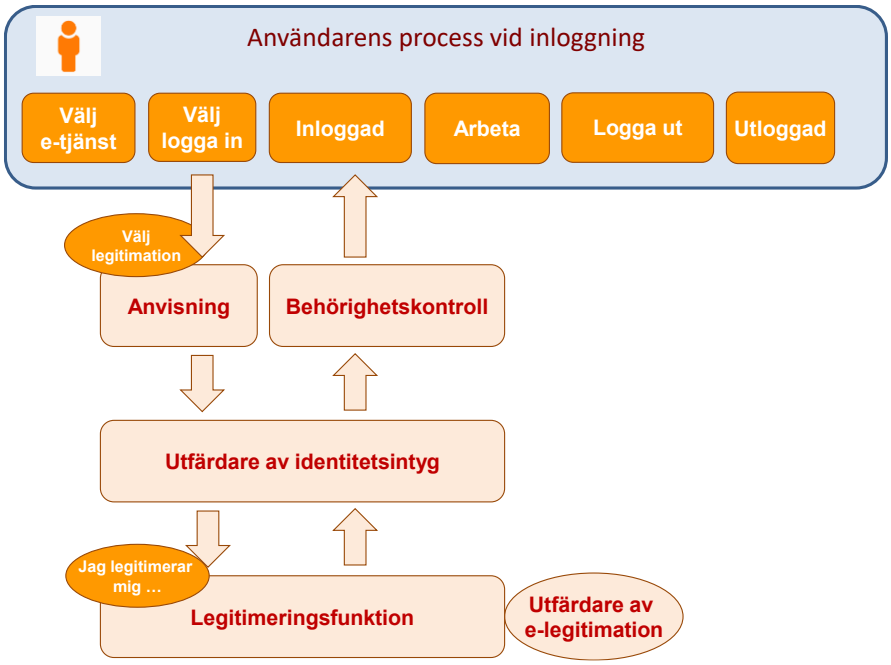
Vid avrop kan kund kravställa om en i sammanhanget passande prismodell.

Med avseende på eID-tjänsterna innebär detta att kund kan kvarställa om olika prismodeller beroende på kontraktföremålets art och omfattning. Exempel på prismodeller är engångslicensavgift, fastpris, rörligt pris med eller utan takpris samt periodisk avgift (abonnemangsavgift).

2.3 Elektronisk identifiering

Schematisk beskrivning av hur e-identifiering går till ur ett användarperspektiv.

Följande figur ger en schematisk bild över hur inloggning och identifiering fungerar ur ett användarperspektiv.



Figur 1 Användarens process vid inloggning och identifiering

Användaren väljer tjänst och att logg in i tjänsten.

- Användaren överförs till anvisningstjänsten.
- I anvisningstjänsten får användaren välja den e-legitimation som ska användas vid inloggningen. Anvisningstjänsten har uppgifter om tillgängliga legitimeringstjänster i något som ibland benämns metadata. Legitmeringstjänsten utförs oftast av utfärdaren av e-legitimationen och innebär en kontroll av att e-legitimationen är giltig.
- När användare har valt e-legitimation överförs användaren, via utfärdaren av identitetsintyg, till utfärdarens legitimeringsfunktion.
- I legitimeringsfunktionen legitimerar sig användaren till exempel genom att ange säkerhetskoden för e-legitimationen.
- Legitimeringsfunktionen autentiserar användaren och sänder resultatet till utfärdaren av identitetsintyg.
- Utfärdaren av identitetsintyg tar emot och kontrollerar uppgifter om legitimeringen.

- Utfärdaren av identitetsintyg ställer ut ett identitetsintyg och stämplar det för att möjliggöra kontroll av intygets äkthet. Identitetsintyget sänds tillbaka till e-tjänsten.
- E-tjänsten kontrollerar identitetsintyget och användarens behörighet i e-tjänsten.
- Användaren ges tillgång till tjänsten om denna är behörig.

I denna struktur är det som avropas från ramavtalet en funktion: e-identifiering. I tjänsten ingår normalt följande funktioner:

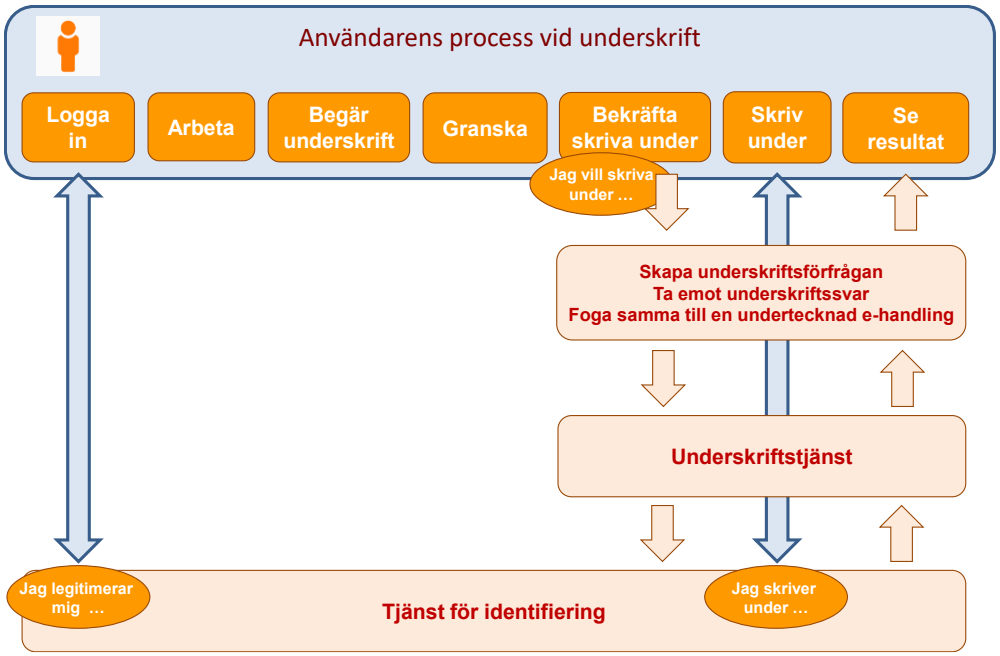
- Anvisning inklusive metadata
- Utfärdande av identitetsintyg
- Integration mot funktion för legitimering för respektive e-legitimation som ska kunna användas.
- Om utländska e-legitimationer används ska integration finnas mot den svenska eIDAS-noden som DIGG tillhandahåller. För mer information om användning av utländsk e-legitimation hänvisas till DIGG vägledningar och eIDAS.

En fördel med denna struktur är att kundens egen it-miljö endast behöver anpassas till ett tekniskt gränssnitt oavsett vilken e-legitimation som används.

2.4 Elektronisk underskrift

Schematisk beskrivning av hur e-underskrift går till ur ett användarperspektiv. Avsnittet tar också upp den provning av underskriftstjänst som genomförs inom ramen för ramavtalet.

Följande figur ger en schematisk bild över hur e-underskrift fungerar ur ett användarperspektiv.



Figur 2 Användarens process vid e-underskrift

När underskrift ska göras väljer användaren att begära underskrift av en handling.

- Handlingen visas för användaren som bekräftar att underskrift ska göras genom att välja "jag vill skriva under ...", eller motsvarande.
- En funktion paketerar den handling som ska skrivas under samt skapar ett kondensat av den elektroniska handlingen, en så kallad hashsumma. En begäran om underskrift (sign request) skapas och sänds till underskriftstjänsten. Även ett meddelande (sign message) sänds med som användaren ser när denna legitimerar sig i legitimeringstjänsten. Notera att det endast är kondensatet av den elektroniska handlingen som sänds till underskriftstjänsten, inte handlingen som sådan.
- Underskriftstjänsten tar emot begäran om underskrift och sänder användaren vidare till identifieringstjänsten.
- Användaren legitimerar sig genom att välja "jag skriver under ...", eller motsvarande, och ange sin säkerhetskod. Underskriftsmeddelandet (sign message) visas också för användaren för att tydliggöra i vilket sammanhang underskriften görs.
- Identifieringstjänsten kontrollerar legitimeringen och ställer ut ett identitetsintyg som sänds tillbaka till underskriftstjänsten.

- Underskriftstjänsten tar emot och kontrollerar identitetsintyget och skapar användarens elektroniska underskrift med tillhörande underskriftscertifikat. Underskriftstjänsten skapar ett underskriftssvar som sänds tillbaka till funktionen som tar emot underskriftssvaret.
- Underskriftssvaret tas emot och kontrolleras och underskriftssvaret fogar därefter samman med originalhandlingen till en undertecknad elektronisk handling.
- Resultatet visas för användaren.

Notera återigen att själva handlingen som undertecknas inte sänds till underskriftstjänsten. Detta innebära att tjänsten kan placeras hos leverantören även i de fall där de handlingar som ska skrivas under innehåller känsliga uppgifter.

Den funktion som skapar underskriftsförfrågan, tar emot underskriftssvar och fogar samman delarna till en undertecknad elektronisk handling benämner vi här **stödtjänst**.

Notera att stödtjänsten kan behöva avropas som en separat del om inte leverantören erbjuder stödtjänsten i samma paketering som underskriftstjänsten.

2.5 Godkända ramavtalsleverantörer för underskriftstjänster

Kammarkollegiet genomför i samverkan med DIGG, provning av underskriftstjänster för att säkerställa att tjänsterna är följsamma mot DIGG:s Normativa specifikation för underskriftstjänst.

Provningen omfattar kontroll av såväl funktionella som icke funktionella krav. De funktionella kraven är kontrollerade i testmiljöer som etablerats för provningen. Icke funktionella krav är avstämda i möten med leverantören.

Följande ramavtalsleverantörer med eventuella underleverantörer har per 2020-04-08 fått sina underskriftstjänster granskade och uppfyller kraven enligt DIGG:s Normativa specifikation för underskriftstjänst:

- CGI Sverige AB
- Chas Visual Management AB med Cybercom Sweden AB* som underleverantör
- Pulsen AB med Technology Nexus Secured Business Solution AB* som underleverantör

*) Cybercom Sweden AB och Technology Nexus Secured Business Solution AB levererar den kompletta tjänsten.

Detta innebär att avropare kan ställa krav på godkända underskriftstjänster i sin avropsförfrågan.

Prövningen ger dock bara en ögonblicksbild av hur leverantören lever upp till kraven just vid det provtillfället. Tänk därför på att kontrollera att detta godkännande av underskriftstjänsten fortfarande är aktuellt.

3 Tjänsteplanering

Planeringen bör omfatta tjänstens hela livscykel.

En bra planering är en framgångsfaktor och en viktig del i arbetet inför avrop, införande, användning och avslut av tjänst. En bra planering bidrar till att det fortsatta arbetet kan genomföras utan större störningar och förseningar. Planeringen bör ha föregåtts av ett grundläggande arbetet omfattande strategier samt analys av kostnad och nytta.

Under planeringen måste viktiga frågor rörande tjänsten och dess användning behandlas. I det följande ges exempel på saker som kan vara viktigt att hantera med avseende på eID-tjänster.

3.1 Behov

Utifrån den behovsbild och de förutsättningar som organisationen har behöver en struktur för eID-tjänster tas fram innan en upphandling genomförs. En optimal strukturering gör att organisationen kan växa i lösningen över tid och att inlåsningseffekter undviks.

En del organisationer organiserar sin IT-miljö och sina IT-tjänster i olika segment för att skapa en struktur där e-tjänster erbjuder extern åtkomst och kopplingar inåt mot befintliga verksamhetsperspektiv. Samtidigt läggs olika funktioner i separata block för att skapa flexibilitet.

I strukturen av eID-tjänsterna är det viktigt att definiera vilka funktioner som ska hanteras internt inom organisationen och vilka som lämpligen läggs ut på extern leverantör. Förutom säkerhet och lagkrav bör hänsyn tas till den egna organisationens förmåga att utveckla och förvalta tjänster, samt vad som är lämpligt att göra själv och vad som är lämpligt att extern leverantör gör.

3.2 Särskilda registerförfattningar

I den generella vägledningen för ramavtalsområdena i Programvaror och tjänster anges ett antal lagreglerade områden som behöver granskas inför avrop. Viktiga områden för eID-tjänster är hantering av information inklusive personuppgifter.

Hantering av information

Kartlägg var och hur den information som förekommer i tjänsterna får behandlas. Genomför en egen så kallad laglighetskontroll samt en risk- och sårbarhetsanalys. Även en gallringsutredning bör genomföras för att kartlägga vad som gäller för gallring och bevarande av informationen i tjänsterna. Gallringsutredning görs lämpligen i samband med införande av tjänsterna när det blir tydligt vilka informationsmängder som finns.

Hantering av personuppgifter

Klargör vad personuppgiftsansvaret omfattar samt vilka registerförfattningar som kan reglera behandlingen av personuppgifter. Personuppgiftsbiträdesavtal kan behöva tas fram och samtycke för behandling personuppgifter bör utredas. I detta arbete bör dataskyddslagstiftningens krav identifieras och följas.

Om leverantören tillhandahåller utkast på avtal bör det granskas i förhållande till de krav som finns i ramavtalet och det exempel på personuppgiftsbiträdesavtal som finns i ramavtalet innan det undertecknas. Leverantörens förslag på avtalstexter ska inte strida mot det som framgår av ramavtalet i övrigt.

Om leverantörer använder underleverantörer i olika delar eller om tjänsten i delar finns placerad i andra länder bör det i kontraktet också säkerställas att leverantören garanterar att personuppgiftslagen uppfylls i alla delar. Och om det skulle uppdagas att lagen inte uppfylls bör krav ställas på att leverantören på egen bekostnad vidtar de åtgärder som krävs för att uppfylla lagen.

3.3 Avropsteam

Vid avrop av eID-tjänster från ramavtal bör ett team med olika kompetenser sättas ihop. Förutom kunskap om upphandling och ramavtalet behövs juridisk kompetens inom områden som är relaterade till eID-tjänsterna. Det är delar som hantering av personuppgifter, eIDAS, gallring, offentlighet och sekretess med flera. Dessutom behövs kompetenser som projektledning, informationssäkerhet, användbarhet, IT-drift, tjänstehantering och leverantörsstyrning.

3.4 Tidplan

En tydlig och realistisk tidplan är alltid ett bra underlag för såväl planeringen som när avropsförfrågan och kontrakt ska tas fram. Tänk därför igenom när tjänsten ska vara på plats och i produktionsläge.

Planera också för inledande testverksamhet och ta fram en tänkt tidplan för hela tjänstens livscykel.

3.5 När kontraktet upphör

Även om det i denna planeringsfas känns avlägset är det viktigt att också planera för vad som ska hända när kontraktet löper ut. Ska tjänstens funktioner kunna överföras till ny leverantör och hur ska det då gå till?

Det är också viktigt att planera för de aktiviteter som organisationen själv behöver vidta inför avtalsslut så att det görs i tillräckligt god tid och på rätt sätt. Om tjänsten ska kunna överföras till ny leverantör ska det ske med så lite störningar som möjligt för användarna av tjänsten.

Allmänna villkor i ramavtalen reglerar vad som gäller vid kontraktets upphörande.
Se särskilt avsnitt 24 Konsekvenser av Kontrakts upphörande.

3.6 Informationsförfrågan (RFI)

En förfrågan om information eller request for information (RFI) kan ställas till leverantörerna under planeringsfasen, innan avropet formellt påbörjas.

Syftet med en RFI är att undersöka svaren på principiella frågor och för att säkra att god konkurrens kan uppnås vid kommande avrop.

De svar som leverantörerna ger på en informationsförfrågan ska inte på något sätt kunna påverka utfallet i avropet.

3.7 Punkter att beakta inför anskaffning

Som sammanfattning bör bland annat följande beaktas inför avrop av eID-tjänster inom ramen för Programvaror och tjänster.

Generella delar

- Skapa en struktur för tjänster och funktioner som passar den egna organisationen. Fundera speciellt på vad som bör finnas internt och vad som kan läggas ut externt samt att strukturen ger möjlighet till framtida utveckling och inte skapar inlåsning.
- Tydliggör vilka servicenivåer (SLA) som ska gälla för tjänsterna. Ett så kallat servicenivåavtal bör tas fram och ingå som en del av kontraktet.
- Tydliggör vad som ska loggas och rapporteras för att kunna säkerställa korrekt agerande i felsituationer och för uppföljning av tjänsternas funktion. Noteras bör att loggar normalt är allmänna handlingar. Hantering och rapportering av incidenter bör särskilt beaktas.
- Tydliggör hur personuppgifter ska hanteras i alla led av leveransen.
- Se till att information i tjänsterna hanteras korrekt samt gallras och bevaras enligt gällande regelverk.
- Klargör äganderätt till olika typer av information och handlingar/dokument.
- Prognosticera transaktionsvolymer avseende eID-tjänsterna. Ju bättre detta kan göras desto enklare för en leverantör att tillhandahålla rätt tjänster.
- Kartlägg risker och sårbarheter vid införande och användning av tjänsterna. Vidtag åtgärder för att minska riskerna till en acceptabel nivå.

E-identifiering

- Kartlägg vilka e-legitimationer e-tjänstens användargrupp har.
- Fastställ e-tjänsternas krav på tillitsnivåer för e-legitimationer.
- Identifiera om e-tjänsten ska erbjuda inloggning med utländsk e-legitimation enligt eIDAS.
  Klargör om det finns behov av att under kontraktstiden kunna lägga till och ta bort e-legitimationer, till exempel legitimationer med kvalitetsstämpeln Svensk e-legitimation.

E-underskrift

- Kartlägg behov gällande av DIGG och Kammarkollegiet godkänd underskriftstjänst.
- När avrop av tjänster för elektronisk underskrift ska göras, bör krav ställas på att tjänsten följer DIGG:s Normativa specifikation för underskriftstjänst.
- Bestäm tillitsnivåer för de e-legitimationer som ska användas för att göra elektroniska underskrifter.
- Säkerställ möjligheten att spåra gjorda transaktioner i alla led i tjänsten.

Informationssäkerhet

Lagstiftning som rör personuppgifter, offentlighet och sekretess, säkerhetsskydd, arkivering med flera gäller givetvis även för eID-tjänster. Det finns dessutom ett antal specifika juridiska frågor att beakta vid användning av just e-legitimationer och e-underskrifter. Dessa behandlas inte här. Dessa frågor belyses i den juridiska vägledningen från eSAM.

I ramavtalsupphandlingarna har krav ställts på att Ramavtalsleverantören ska ha ett strukturerat och dokumenterat ledningssystem för informationssäkerhet. Som alternativ till redovisning av ledningssystem för informationssäkerhet i sig godtas att ramavtalsleverantör redovisar gällande certifikat avseende ett ledningssystem för informationssäkerhet som minst motsvarar punkterna 1 - 5 nedan, samt kan redovisa kraven för certifiering till Statens inköpscentral.

1. Process för bedömning av informationssäkerhetsrisker
2. Process för behandling av informationssäkerhetsrisker
3. Process för upprättande och dokumentation av informationssäkerhetsmål
4. Process för lämpligheten, tillräckligheten och verkan av ledningssystem
5. Genomförande av interna revisioner

Vid avrop ska inte krav på leverantören som sådan ställas. Det är redan gjort i ramavtalsupphandlingen.

Möjlighet finns att vid avrop ställa krav på att leverantören ingår säkerhetsskyddsavtal i samband med avropet eller i samband med fullföljandet av kontraktet.

Leverantören ska också följa de säkerhetsföreskrifter som kunden ställer inom säkerhetsområdet.

4 Tjänsteavrop

Avropsfasen startar när planeringen är gjord i väsentliga delar och beslut har fattats om att genomföra avrop från ramavtalet. Avropsfasen är i stora delar formellt styrd av ramavtalet.

Avropsfasten består i grova drag av följande steg.

- Utformning av avropsförfrågan
- Utskick av avropsförfrågan
- Utvärdering av avropssvar
- Tilldelningsbeslut
- Tecknande av kontrakt

Det är viktigt att avropsförfrågan formuleras på ett bra sätt så att det tydligt framgår vad som efterfrågas, vilka krav som ska gälla samt hur värderingen av avropssvar kommer att ske. Det är också en fördel om ett kontraktsförslag följer med avropsförfrågan då det tydliggör för leverantören hur kontraktsförhållandet kommer att se ut.

Efterfrågade tjänster ska vara kravställda så att det är tydligt vad som ska gälla vid införande, under kontraktstiden och vid kontraktets upphörande. Krav på tjänster bör i huvudsak avse funktionella krav. Krav på tekniska detaljer bör undvikas så långt som möjligt, men kan också vara nödvändigt om tjänsten till exempel ska integreras med andra befintliga tjänster och system.

De svar och förtydliganden som avropande organisation lämnar är att betraktas som en del av avropsförfrågan.

Kontraktet ska ha tecknats inom ramavtalens giltighetstid, men fullgörandet kan ske även efter att ramavtalet har upphört.

För mer detaljerad beskrivning av avrop hänvisas till den generella vägledningen för Programvaror och tjänster.

5 Tjänsteinförande

Efter att kontraktet är tecknat ska tjänsterna införas enligt vad som överenskommits i kontraktet. Det bör finnas en tidplan för hela införandet som parterna har kommit överens om, eventuella detaljer och preciseringar i planen kan ha överenskommits om efter kontraktets tecknande.

Införandet avslutas med en leveranskontrollperiod där kunden ska kontrollera att tjänsterna uppfyller avtalad specifikation. Se Bilaga Allmänna villkor för aktuellt ramavtalsområde om leverans och leveranskontroll. Hur denna leveranskontroll ska gå till bestämmer kunden själv, men det bör planeras i samråd med leverantören.

Innan leveranskontrollperioden startar ska leverantören genom egna tester säkerställa att tjänsterna uppfyller avtalad specifikation. Den enklaste formen av leveranskontroll kan

vara att gå igenom leverantörens testprotokoll och godkänna leveransen om testprotokollet är till fyllest.

Den dag tjänsten godkänns är den effektiva leveransdagen. Om den effektiva leveransdagen inträffar efter den avtalade leveransdagen föreligger en försening.

Om leveransen har delats upp i delleveranser så bör en leveranskontroll göras för respektive leverans, men också en slutlig leveranskontroll för helheten för att säkerställa att alla delar i leveransen fungerar tillsammans som avsett.

I samband med införandet, eller strax efter, bör en kartläggning göras för att tydliggöra vilken information som hanteras i tjänsterna. Här bör också fastställas ägandeskap till de olika delarna av informationen. Även en gallringsutredning kan behöva genomföras för att kartlägga vad som gäller för gallring och bevarande av informationen i tjänsterna.

6 Tjänsteanvändning

Under användningen av tjänsterna bör leveransen av tjänsterna kontinuerligt följas upp.

Delar som bör följas upp är användning, priser, uppfyllelse av tjänstenivåer och övriga villkor som parterna kommit överens om och som framgår av kontraktet.

Avvikelser och brister kan vara både vites- och hävningsgrundande. Var noga med att bokföra och tidsange alla avvikelser och brister för att kunna påvisa för leverantören vid ett eventuellt tvisteförfarande.

Ramavtalen ger möjlighet för kund att begära att en samverkansorganisation ska upprättas för kontraktet. Hur tjänsterna uppfyller överenskomna tjänstenivåer ska rapporteras av leverantören.

Ändring av tjänsterna är något som löpande bör hanteras. Förutsättningarna för ändringar framgår av Allmänna villkor avsnitt 25 Ändring av Kontrakt eller Kontraktsföremål. Det är viktigt att kunden kan vara med och styra att ändringar görs på sådant sätt så att verksamhetens påverkas i så liten omfattning som möjligt och att ändringar som påverkar funktionen i tjänsten endast görs efter överenskommelse.

Hantering av incidenter är en viktig del i den löpande förvaltningen. Speciella krav bör finnas när det gäller hantering och rapportering av incidenter och säkerhetsincidenter som har stor påverkan på kundens verksamhet. Incidenter hanteras som fel i enlighet med Allmänna villkor avsnitt 8 Ansvar för Fel.

7 Tjänsteavslut

I god tid innan kontraktet löper ut måste planering göras för avslut av befintlig tjänst. Om tjänsten fortsättningsvis ska erhållas från en ny part, till exempel som följd av tecknande av nytt kontrakt, kommer avslut av befintlig tjänst att bli beroende av hur införandet av den nya tjänsten ska gå till.

Den befintliga leverantören ska ansvara för att upprätthålla befintlig tjänst så länge det är nödvändigt och för att bistå i överföring av tjänst till leverantören i det nya kontraktet

Den nya leverantören ansvarar för införande av tjänsten enligt det nya kontraktet.

Förutsättningarna för överföring anges i Allmänna villkor främst avsnitt 24 Konsekvenser av Kontrakts upphörande.

8 Referenser för eID-tjänster

Nedan anges ytterligare några specifika referenser för eID-tjänsterna som kan ha betydelse vid införande av eID-tjänster.

DIGG:s Tekniska ramverk

Det tekniska ramverket beskriver funktion och ställer krav på eID-tjänster med hänvisning till relaterade standarder inom området. Syftet med ramverket är att göra införandet av e-legitimering och e-underskrift säkert, enkelt och effektivt. Ramverket ska användas av svenska e-tjänster som kopplar upp sig mot den svenska eIDAS-landsnoden.

E-underskrift

De tjänster för e-underskrift som beskrivs i vägledningen följer DIGG:s Tekniska ramverk och Normativ specifikation för underskriftstjänst.

DIGG:s Normativa specifikation för underskriftstjänst

Specifikation består av följande dokument:

- Normativ specifikation
  Huvuddokumentet för specifikation av underskriftstjänsten.
- Policy för underskriftstjänst
  Specificerar värden för konfigurerbara parametrar som styr underskriftstjänstens funktion.
- Tjänstespecifikation Underskriftstjänst
  Specificerar underskriftstjänstens funktion.
- Icke funktionella krav
  Anger krav på tillgänglighet, kapacitet, säkerhet och motsvarande.

DIGG:s Tillitsramverk

Tillitsramverket syftar till att etablera gemensamma säkerhetskrav för utfärdare av Svensk e-legitimation. Kraven är fördelade på olika skyddsklasser - tillitsnivåer - som svarar mot olika grader av teknisk och operationell säkerhet hos utfärdaren och olika grader av kontroll av att en person som tilldelas en elektronisk identitet verkligen är den han eller hon utger sig för att vara.

Svensk e-legitimation

Svensk e-legitimation är statens kvalitetsmärke för e-legitimationer. Kvalitetsmärket visar att en e-legitimation är kontrollerad och godkänd av DIGG. Prövningen sker mot DIGG:s Tillitsramverk.

eIDAS

EU:s förordning nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden kallas i dagligt tal för ”eIDAS”. eIDAS och följdändringar i svensk författning trädde i kraft den 1 juli 2016.

Se DIGG:s hemsida.

9 Kontaktuppgifter

Information om e-identifiering, e-underskrift och ramavtal

På Statens inköpscentrals webbplats avropa.se för ramavtal finns information om funktionerna E-identifiering och E-underskrift i Programvaror och tjänster: https://www.avropa.se/ramavtal/ramavtalsomraden/it-och-telekom/Programvaror-och-tjanster/

Kontaktuppgifter

Frågor om E-identifiering och E-underskrift och anskaffning av dessa funktioner via ramavtal ställs till Kammarkollegiet:

E-post: jan.lundh@kammarkollegiet.se eller pedra.herdegen@kammarkollegiet.se.

Allmänna frågor om Statens inköpscentrals ramavtal ställs till Ramavtalsservice:

E-post: ramavtalsservice@kammarkollegiet.se

Frågor om elektronisk identifiering och elektroniska underskrifter, som inte har att göra med ramavtal eller avrop, ställs till DIGG:

Hemsida: https://www.digg.se/
E-post: info@digg.se

Bilaga 1 – Vad kan avropas på respektive ramavtalsområde

Leverans-form	**Programvaru-lösningar**	**Licens-försörjning**	**System-utveckling**	**Vård Skola Omsorg**
Programvara	x	x	x	x
Publik molntjänst	x	x	x	x
Privat molntjänst	x	-	x	x
Licenstjänster	x	x	-	-
Konsulttjänster	x	-	x	x

Konsulttjänster omfattar kompetenser som bemannar it och it-relaterade projekt eller aktiviteter under systems livscykel från behovsanalys till leverans och förvaltning inklusive migrering och avveckling.