Förstudierapport
Kort för identifiering och behörighet, KIB

KAMMARKOLLEGIET

Innehåll

1 Sammanfattning

Det har hänt väldigt mycket inom området sedan föregående förstudie för sju år sedan. Projektgruppen kan konstatera att det fortfarande finns ett stort behov av kort och andra bärare för inpassering samt för dator och it-system. Området för identifiering har utvecklats och även e-legitimation är i fokus, det vill säga identifiering via någon form av elektronisk legitimation på en bärare exempelvis placerad i mobiltelefon eller kort.

Vidare har området utökats med ett antal andra typer av bärare så som armband och ringar för in- och utpassering i lokaler, appar till mobiltelefoner, USB-stickor. Det är viktigt att ett kommande ramavtal inkluderar alla nya typer av bärare.

Gällande utbudet av tjänster kan ett nytt ramavtalsområde med fördel utökas med möjlighet till att tillhandahålla produkter som tjänst, det vill säga att avropande organisation inte själv äger någon utrustning utan köper tjänsten.

Området ska bibehållas i sin helhet men behöver utökas med ovan nämnda produkter och tjänster. Det är viktigt för digitaliseringsarbetet att ramavtalet mordaniseras enligt ovan. En e-tjänstelegitimation som används i tjänsten ska bereda möjlighet för olika användningsområden som främjar digitaliseringen exempelvis genom elektroniska underskrifter. Genom föreslagna ramavtal framskrider digitaliseringsarbetet så att statliga myndigheter, kommuner och regioner kan genomföra samtida anskaffningar på ett effektivt och kostnadsbesparande sätt.

Förstudierapporten framtagen av:

Renée Skiver, projektledare

Bidragande till informationsinsamling:

Jan Lundh, ramavtalsförvaltare

Petra Herdegen, biträdande ramavtalsförvaltare

2 Inledning

2.1 Bakgrund till förstudien

Förstudien är genomförd av Kammarkollegiet och omfattar området inom kort och andra bärare för identifiering och behörighet och inkluderar såväl produkter som tjänster.

Kammarkollegiet har ansvaret för upphandlingsverksamheten inom den statliga inköpssamordningen. Detta innebär att myndigheten har som uppdrag att ingå ramavtal för varor och tjänster som är avsedda för andra statliga myndigheter.

Enligt förordning (1998:796) om statlig inköpssamordning ska det finnas ramavtal eller andra gemensamma avtal som effektiviserar upphandlingarna för varor och tjänster som myndigheterna upphandlar ofta, i stor omfattning eller som uppgår till stora värden. Ramavtalsupphandling kan även motiveras med att det uppfylls en viss samhällsnytta med att ingå ramavtal för området.

2.2 Mål med förstudien

Syftet med förstudien är att samla information och kunskap om pågående utveckling kring ramavtalsområdet, samt om vilka behov offentlig sektor har. Förstudien ska även belysa hur upphandlingen kan genomföras och därmed ge underlag till såväl upphandlingsstrategin som kommande upphandlingsdokument. I sammanhanget ska särskilt beaktas att ramavtalen ska vara lätta att avropa från, i vilken utsträckning det kommer krävas stöd från ramavtalsförvaltningen samt eventuellt samspel med leverantörsmarknaden gällande förändringar i upplägg, kravställning med mera.

Samtliga rekommendationer som lämnas i samband med denna förstudie kan komma att prövas på nytt, ändras och anpassas i en kommande upphandling då ny information kan tillkomma och förutsättningar kan ändras med tiden.

2.3 Omfattning och avgränsningar i förstudien

Syftet med förstudierapporten har inte varit att ta fram en kravspecifikation till en kommande upphandling, och således är eventuella krav som kan ställas endast beskrivna på en övergripande nivå. Förstudierapporten beskriver nuläge och erfarenheter av användningen av ramavtalen inom området. Den innehåller avropande myndigheters och leverantörers synpunkter på det nuvarande ramavtalet samt deras förslag rörande upplägg av en eventuellt kommande upphandling. Därtill innefattar förstudierapporten en analys av myndigheters behov och marknadens utbud.

Ramavtalen inom detta område kan i dag användas av statliga myndigheter samt stiftelser och andra organisationer med anknytning till staten.

Ramavtalen omfattar även kommuner, regioner och andra offentligt styrda organisationer som har lämnat bekräftelse.

2.4 Målgrupp

Förstudien riktar sig i första hand till följande målgrupper.

- Berörda personer inom Kammarkollegiet.
- Beställare, upphandlare, inköpare och övriga anställda eller verksamma i statliga myndigheter offentlig sektor som använder våra ramavtal, samt de som inte gör det idag.
- Kommuner, regioner och andra upphandlande myndigheter.
- Leverantörer – nuvarande och potentiella ramavtalsleverantörer till Kammarkollegiet.

2.5 Metod för förstudien

Förstudiearbetet har utförts i enlighet med Kammarkollegiets projektstyrningsmetodik. Den innefattar:

- initiering av projektet med definition av projektets huvudsakliga mål i form av ett projektdirektiv,
- detaljerad planering, dvs. en projektbeskrivning och planering av projektets aktiviteter,
- genomförande som omfattat informationsinsamling, analys och författande av förstudierapporten,
- leverans av förstudien med föregående kvalitetssäkring.

Informationsinsamlingen till förstudien har skett genom möten med avropande myndigheter och organisationer och därtill har en referensgrupp med deltagare från olika avropande organisationer deltagit i förstudien och bidragit med värdefull information och synpunkter.

Vidare har projektgruppen haft möten med leverantörer och branschorganisationer för att få deras syn på såväl det nuvarande ramavtalet som branschen och dess utveckling.

Under hela arbetet har ansvarig ramavtalsförvaltare från Kammarkollegiet varit med.

Det kommer att göras en samlad bedömning av all information som inkommer i förstudien för att på så sätt undersöka hur en upphandling ska utformas på bästa sätt. Det kan innebära att förslag från enskilda intressenter inte alltid kan beaktas vid utformningen av en eventuellt kommande upphandling.

3 Föregående upphandling

3.1 Upphandlingsform och tidpunkter för anbudsgivning och tilldelning

Den föregående upphandlingen genomfördes enligt ett selektivt förfarande enligt lag (2011:1029) om Upphandling på försvars- och säkerhetsområdet (LUFS) och som tilldelningsgrund användes ekonomiskt mest fördelaktiga anbud. Ansökningsinbjudan publicerades under september 2013 och anbudsinbjudan publicerades i november 2013. Ramavtalet började gälla från och med den 27:e januari 2014. Det skedde ingen överprövning av tilldelningsbeslutet.

Sex ansökningar hade inkommit vid ansökningstidens utgång den 28 oktober 2013 och vid anbudstidens utgång den 3 januari 2014 hade dessa sex leverantörer inkommit med anbud enligt nedan.

- Cygate AB
- Gemalto AB
- Oberthur Technologies Sweden AB
- PartnerSec AB
- Technology Nexus Secured Business Soloutions AB
- EVRY Card Service AB

Evry Card Service AB hade uppgett för ”Krav på prestanda på chippet” att kravet inte uppfylldes och därmed hade bolaget inte full poäng i kravuppfyllnad, vilket övriga anbudsgivare hade.

Eftersom maximalt fem anbudsgivare skulle erhålla ramavtal, tilldelades de fem anbudsgivare som hade maximalt antal poäng i kvalificeringen

3.2 Upphandlingens omfattning

Upphandlingen omfattade både produkter i form av kort, korthållare, fotostationer, programvaror, med mera samt tjänster knutna till produkterna. Produkter och tjänster beskrivs nedan.

Blanka opersonaliserade smartkort utan foto för elektronisk identifiering eller behörighetskontroll. Exempel på denna typ av kort är ett kort utan tryck/märkning eller fotografi men med en elektronisk del. Ett smartkort definierades i upphandlingen som ett kort som kan lagra och/eller processa information. Dessa kan till exempel användas för att logga in i datasystem och datornät, användas för elektronisk identifiering och underskrift och/eller för inpassering i lokal. Smartkortets elektroniska del kan till exempel vara chip,

beröringsfri teknik och/eller magnetremsa och med möjlighet till installerade certifikat och konfigurering av PIN-kod.

Personaliserade kort för fysikidentifiering och/eller behörighetskontroll. Dessa typer av kort avser fysiska egenskaper och användning. Exempel på denna typ av kort är identitetskort, SIS-märkta identitetskort (SS 614314) och tjänstekort för anställda i offentlig sektor. Upphandlingen omfattade också kort som är en kombination av ovanstående korttyper det vill säga kort som kan användas för både fysisk och elektronisk identifiering och behörighetskontroll.

De tjänster som ingick i upphandlingen är följande:

- Tjänst för kontroll av korts giltighet,
- Tjänst för att spärra kort,
- Tjänst avseende kodning av kortens elektroniska del samt säkerhetslösning,
- Tjänster avseende kodning av andra bärare än kort ingick också i upphandlingen.

Upphandlingen omfattade även beställningsstationer. Detta är en lösning bestående av både hård- och programvara för att inhämta och spara personuppgifter till kort samt även att beställa kort, det vill säga en beställningsstation. Med hjälp av en sådan beställningsstation ska avropande kund kunna inhämta en persons namnteckning, fotografera, registrera personuppgifter, spara foto och personuppgifter samt överföra beställning och uppgifter till leverantör på elektronisk väg. Installation, konfiguration och underhåll av den hård- och programvara som beställningsstation består av ingår också.

Upphandlingen omfattade även olika tillbehör till exempel kortläsare och korthållare.

3.3 Synpunkter och erfarenheter från föregående upphandling

Föregående upphandling är gjord med stöd av Lag (2011:1029) om upphandling på försvars- och säkerhetsområdet, (LUFS), med ett selektivt förfarande. Det ansågs viktigt ur flera säkerhetsaspekter, bland annat för att personaliseringen av korten måste kunna ske i Sverige.

Eftersom leverantörerna var få till antalet gick det inte att dela in upphandlingen i områden på något sätt. Också baserat på antalet få leverantörer var det egentligen onödigt med en selektiv upphandling, men då LUFS inte medgav en öppen upphandlingsform, fanns inget bättre alternativ än selektiv form. LUFS medger inte heller idag öppen form.

4 Nuvarande ramavtal

4.1 Avtalens löptid

Ramavtalen började gälla den 27:e januari 2014 och gäller till och med de 31:a januari 2021.

4.2 Antagna ramavtalsleverantörer

Följande ramavtalsleverantörer antogs:

- Cygate AB
- Gemalto AB
- Idemia Sweden AB
- PartnerSec AB
- Technology Nexus Secured Business Solutions AB

Gemalto AB har köpts upp av Thales Sverige AB. Oberthur Technologies Sweden AB har bytt namn till Idemia Sweden AB.

4.3 Total omsättning på ramavtalet

Nedan redovisas omsättningsstatistik avseende hela ramavtalet hittills varande datum. Statistiken baseras på uppgifter redovisade av de fem ramavtalsleverantörerna.

Den totala omsättningen på ramavtalet uppgår i december 2019 till cirka 60 miljoner.

Den störa delen av försäljning står Gemalto AB för. Därefter kommer Idemia Sweden AB De tre övriga ramavtalsleverantörerna har en jämn omsättning men betydligt lägre än de två först nämnda leverantörerna.

Fördelningen mellan statliga myndigheter, kommuner och regioner är denna:

Stat:	82%
Kommun:	14%
Region:	4%

4.4 Ramavtalsanvändare

Flera avrop har genomförts, både större avrop och mindre avrop. De större statliga myndigheterna är dominerande men även ett antal mindre myndigheter har avropat. Åtta universitet har avropat och även en region.

4.5 Avstegsanmälan

Inga myndigheter, kommuner eller regioner har anmält avsteg till Kammarkollegiet.

4.6 Förvaltning av ramavtalet

Ramavtalet förvaltas av enheten för ramavtalsförvaltning vid Kammarkollegiet.

Ansvarig förvaltare har förvaltat och förvaltar ramavtalsområdet enligt framtagna rutiner för ramavtalsförvaltning framtagna av Kammarkollegiet. Inga avvikelser har rapporterats.

4.7 Information om ramavtalet

Information om ramavtalen förmedlas på www.avropa.se. Där publiceras bland annat listor över ramavtalsleverantörer och avropsberättigade myndigheter, avtalsdokument, avropsmallar, samt vägledningar med stöd för avropsberättigande myndigheter vid avrop.

Kammarkollegiet genomför också regelbundet olika typer av seminarier kopplat till respektive ramavtalsområde, två så kallade Avropadagar riktade till myndigheter och tre leverantörsdagar fördelat på leverantörer inom IT-och telekom, resebranschen samt övriga varor och tjänster. Därutöver ges vägledning och stöd i samband med bland annat avrop från ramavtalen via såväl e-post som telefon samt personliga besök.

5 Omvärldsanalys

På grund av en förändring i behovet av identifiering har förstudien fokuserat mycket på att kartlägga e-legitimation. Det finns flera olika beslut och uppdrag gällande e-legitimation och förstudien har försökt att fokusera på de delar som på något sätt kan ha bäring på kommande ramavtalsområde.

Det har även förekommit viss produktutveckling inom området för bärare. En bärare kan exempelvis vara ett kort, en mobiltelefon eller en USB-sticka.

5.1 E-legitimation

En e-legitimation är en elektronisk identitetshandling som kan användas för att identifiera innehavaren på elektronisk väg. Med hjälp av en e-legitimation kan innehavaren identifiera sig och myndigheter eller andra aktörer som har e-tjänster få en bekräftelse på vem personen är.

En e-legitimation innehåller, liksom en fysisk identitetshandling, uppgifter som uppenbart kan kopplas till en viss person. Den innehåller alltså endast identitetsuppgifter och inte uppgifter om vilken behörighet personen har. Uppgifter om personens behörighet finns i stället i e-tjänsten eftersom det är innehavaren av e-tjänsten som avgör vilken behörighet användaren ska ha.

En e-legitimation kan finnas på olika former av bärare, som en applikation i en mobiltelefon eller surfplatta eller som en fil på en dator eller annan lagringsmedia. Den kan också finnas på ett kort som innehåller ett chip där informationen lagras.

5.2 Gällande rätt

Inom EU gäller Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen). Syftet med förordningen är att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för e-legitimationer och betrodda tjänster. I förordningen fastställs därför de villkor som ska gälla för att en medlemsstat ska erkänna en annan medlemsstats e-legitimationer. Vidare fastställs i förordningen regler för betrodda tjänster och en rättslig ram för elektroniska underskrifter, elektroniska stämplar, elektronisk tidsstämpling, elektroniska dokument, elektroniska tjänster för rekommenderade leveranser och certifikattjänster för autentisering av webbplatser. I lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering finns bestämmelser som kompletterar eIDAS-förordningen. Kompletterande bestämmelser finns också i

förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering (ELOV) innehåller bestämmelser om valfrihetssystem när det gäller tjänster för elektronisk identifiering. Lagen tillämpas i stället för lagen (2016:1145) om offentlig upphandling (LOU) när en myndighet har beslutat att tillämpa valfrihetssystem i fråga om tjänster för elektronisk identifiering av enskilda i myndighetens elektroniska tjänster, har anslutit sig till ett system för säker elektronisk identifiering som tillhandahålls av Myndigheten för digital förvaltning och uppdragit åt Myndigheten för digital förvaltning att i myndighetens namn administrera valfrihetssystemet. Lagen innehåller endast allmänna bestämmelser om annonsering, upphandlingsdokument, ansökan, godkännande av sökande och ingående av kontrakt med mera. Regleringen av de krav som ställs på e-legitimationerna och på hur den elektroniska identifieringen ska gå till finns alltså inte i lagen utan framgår av det upphandlingsdokument som Myndigheten för digital förvaltning tar fram.

5.3 Tillitsnivåer

Enligt internationell standard, som även Myndigheten för digital förvaltning tillämpar, finns det fyra tillitsnivåer för elektronisk identifiering med olika grader av säkerhet. Ju högre tillitsnivå en e-legitimation har, desto säkrare är den, både vad gäller teknik och identifiering. I det tillitsramverk för Svensk e-legitimation och den tillhörande vägledningen som Myndigheten för digital förvaltning ansvarar för beskrivs vilka krav som gäller för tillitsnivå 2, 3 och 4. Tillitsnivå 1 kan vara ett användarkonto som någon själv registrerar på internet utan att styrka sin identitet. Den nivån omfattas inte av tillitsramverket. För nivå 2, 3 och 4 krävs så kallad flerfaktorsautentisering. Det finns tre huvudkategorier av autentiseringsfaktorer; ”något man vet” (koder), ”något man är” (biometriska egenskaper) eller ”något man har” (exempelvis en dator, koddosa, mobiltelefon eller aktivt kort). Med koder avses lösenord, lösenfraser, sifferkombinationer eller liknande. Utgångspunkten enligt tillitsramverket är att koder kombineras med innehav av en lagrad datastruktur. En e-legitimation på tillitsnivå 2 och 3 ska utformas enligt en sådan tvåfaktorsprincip som består dels av elektroniskt lagrad information som användaren ska inneha, dels av något som användaren ska bruka för att aktivera e-legitimationen. Det kan till exempel vara en e-legitimation i mobiltelefonen som aktiveras genom en pinkod. E-legitimationer på dessa nivåer kan utfärdas efter identifiering av sökanden på distans i enlighet med de närmare bestämmelser som föreskrivs i tillitsramverket.

E-legitimation på tillitsnivå 4 ska utformas enligt en sådan tvåfaktorsprincip som består dels av en personlig säkerhetsmodul som användaren ska inneha, dels av något som användaren ska bruka för att aktivera säkerhetsmodulen. En sådan enhet skyddar de uppgifter som är lagrade i e-legitimationen från att någon annan kommer åt dem. Vanligen är det fråga om ett så kallat aktivt kort. Aktivering sker med hjälp av någon form av kod. För att en e-legitimation på tillitsnivå 4 ska utfärdas krävs som regel att utfärdaren har identifierat sökanden vid ett personligt besök. Enligt eIDAS-förordningen finns det tre olika tillitsnivåer; låg, väsentlig och hög. Tillitsnivåerna i eIDAS-förordningen och det svenska tillitsramverket bygger på samma internationella standard. Enligt den bedömning som gjorts av Myndigheten för digital förvaltning motsvarar eIDAS-förordningens tillitsnivåer i stort sett de svenska. Tillitsnivå låg ställer dock lägre krav än tillitsnivå 2 enligt tillitsramverket. Nivån väsentlig motsvarar tillitsnivå 3. Nivån hög motsvarar den

svenska tillitsnivån 4, med undantag för att ett personligt besök krävs vid förnyelse av en e-legitimation på den svenska tillitsnivån 4.

Det är innehavaren av en e-tjänst som måste göra en bedömning av vilken tillitsnivå som ska krävas för identifiering i tjänsten. Vilken nivå som är lämplig beror på hur känslig informationen i e-tjänsten är och vilka konsekvenser det får om någon obehörig får del av den.

5.4 Dagens e-legitimationer och utfärdare

BankID utfärdas av bankerna och är den e-legitimation som dominerar på den svenska marknaden. BankID utvecklas av Finansiell ID-teknik BID AB som ägs av sju banker. Antalet innehavare av BankID är, enligt statistik från Finansiell ID-teknik BID AB, cirka 7,9 miljoner och antalet användningstillfällen var under år 2018 cirka 3,3 miljarder. Det finns tre olika varianter av BankID. Merparten av användarna (cirka 7 miljoner) har mobilt BankID. Mobilt BankID innebär att användaren har sin e-legitimation i en mobiltelefon eller surfplatta. För att kunna hämta och använda mobilt BankID krävs att användaren har installerat en app i mobiltelefonen eller på surfplattan. BankID på kort är en e-legitimation som är lagrad på ett så kallat smartkort. Förutom kortet och BankID-programmet krävs även att man har en kortläsare. BankID på fil är en e-legitimation i en dator. För att kunna hämta och använda BankID på fil krävs att användaren har installerat ett särskilt program på datorn. BankID på fil är den minst vanligt förekommande varianten av BankID. Det finns cirka tio banker som utfärdar BankID. BankID är inte granskad av Myndigheten för digital förvaltning men anses enligt uppgift på myndighetens webbsida motsvara tillitsnivå 3 enligt tillitsramverket.

AB Svenska Pass utfärdar den e-legitimation som sedan september 2017 finns på identitetskort för folkbokförda i Sverige som utfärdas av Skatteverket. Av den information som finns på Skatteverkets webbsida framgår att det behövs en kortläsare och ett särskilt program som installeras på datorn för att kunna använda e-legitimationen. AB Svenska Pass e-legitimation är godkänd enligt tillitsramverket för Svensk e-legitimation och uppfyller kraven för tillitsnivå 4.

Även Telia utfärdar en e-legitimation. Den finns på identitetskort för folkbokförda i Sverige som utfärdats före september 2017. Även denna e-legitimation kräver enligt Skatteverket en kortläsare och ett särskilt program som installeras på datorn. Telias e-legitimation är inte granskad men anses enligt uppgift på webbsidan för Myndigheten för digital förvaltning motsvara tillitsnivå 3.

Företaget Verisec utfärdar en e-legitimation som kallas Freja eID+. Den e-legitimationen finns i mobiltelefonen. För att kunna använda den behöver användaren, enligt uppgift på webbsidan, ladda ner en app i mobiltelefonen. Freja eID+ är godkänd på tillitsnivå 3. Förutom de e-legitimationer som utfärdas till enskilda förekommer det också e-legitimationer som arbetsgivare tillhandahåller sina anställda. Syftet med dessa är att de ska användas i tjänsten. Exempelvis utvecklar Huddinge kommun, Försäkringskassan och Inera sådana e-legitimationer för användning inom den offentliga sektorn.

5.5 Användning av e-legitimation

E-legitimation används framför allt vid identifiering i samband med att en person vill använda en e-tjänst, antingen i datorn eller i en app i mobiltelefonen. E-legitimation kan också användas vid telefonkontakt med kundtjänst till exempel i samband med bostadslån. Även vid identifiering i samband med ett personligt besök kan elektronisk identifiering vara aktuell, till exempel när en person har behov av hjälp till självservice med stöd av e-tjänster på ett servicekontor.

Av statistik från Finansiell ID-teknik BID AB framgår att det under år 2017 genomfördes cirka 3,3 miljarder transaktioner med BankID vilket motsvarar cirka 100 transaktioner per sekund. Av dessa stod internet- och mobilbankstjänster, betaltjänster och finansiella tjänster i övrigt för cirka 84 procent. En stor del av användningen sker enligt uppgift från dåvarande E-legitimationsnämnden i internetbanker och betaltjänsten Swish. Användningen inom den offentliga sektorn utgjorde cirka 7 procent av BankID-transaktionerna under år 2018. En stor del av användningen skedde i Skatteverkets och Försäkringskassans e-tjänster. Under år 2016 utgjorde användningen i dessa båda myndigheters tjänster totalt 62 procent av användningen av e-legitimation inom den offentliga sektorn. Tillsammans stod dessa myndigheter för över 75 miljoner användningar. Andra stora aktörer var 1177.se, Arbetsförmedlingen, Centrala studiestödsnämnden, Stockholms stad, Pensionsmyndigheten och Bolagsverket. Användningen i övriga myndigheters e-tjänster utgjorde tillsammans 2 procent. Enligt de enkätundersökningar E-legitimationsnämnden genomförde har många kommuner, alla regioner, alla länsstyrelser och ett 40-tal statliga myndigheter behov av att användare ska kunna identifiera sig elektroniskt. Behovet förväntades enligt E-legitimationsnämnden öka i takt med den kommande digitaliseringen.

5.6 Elektronisk underskrift

Som beskrivits ovan är e-legitimationens huvudsakliga syfte att identifiera användaren på elektronisk väg. Som regel kan emellertid e-legitimationer även användas för att framställa en elektronisk underskrift (e-underskrift). En mycket stor del av de förlitande aktörerna i såväl offentlig som privat sektor använder sig av denna funktion för att möjliggöra underskrift av exempelvis ansökningar, blanketter och olika former av ekonomiska och rättsliga transaktioner. Med e-underskrift menas uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form för att säkerställa de senares ursprung och dataintegritet. Handlingar skrivs under elektroniskt för att ge skydd mot förfalskning och förnekande på motsvarande sätt som när handlingar undertecknas på papper. E-underskriftens funktion är framför allt säkerhetsrelaterad och syftar till att ge underlag för bland annat äkthetsprövning, bevissäkring och säkerställande av originalkvalitet. Den fyller även andra viktiga skyddsfunktioner såsom att markera att ett visst innehåll är fullständigt och förenligt med avsikten hos användaren samt att säkerställa att användaren tänker sig för och förstår åtgärdens innebörd. E-underskriften kan antingen skapas direkt med användarens e-legitimation, eller indirekt genom användning av e-legitimationen i kombination med en fristående underskriftstjänst. Det förstnämnda fallet kräver att e-legitimationen har ett särskilt underskriftscertifikat. I det indirekta förfarandet behöver inte e-legitimationen ha några särskilda sådana egenskaper och blir således mer teknikoberoende. Det indirekta förfarandet kräver dock att den förlitande aktören har tillgång till en särskild underskriftstjänst som kan skapa den

elektroniska underskriften med stöd av e-legitimationen. Direkt e-underskrift är vanligast förekommande i dagsläget, men det finns även möjlighet att avropa en fristående underskriftstjänst på Kammarkollegiets ramavtal. Hanteringen av e-underskrift av utländska användare i svenska e-tjänster underlättas om ett indirekt förfarande används.

E-underskrift är en så kallad betrodd tjänst som regleras i eIDAS-förordningen. E-underskrift hanteras där helt frikopplat från frågan om elektronisk identifiering. I eIDAS-förordningen görs en uppdelning i avancerade elektroniska underskrifter och kvalificerade elektroniska underskrifter. En avancerad elektronisk underskrift ska enligt artikel 26 i eIDAS-förordningen uppfylla följande krav.

- Den ska vara unikt knuten till undertecknaren.
- Undertecknaren ska kunna identifieras genom den.
- Den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll.
- Den ska slutligen vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

En kvalificerad elektronisk underskrift ska, utöver kraven för avancerade elektroniska underskrifter, vara baserad på ett kvalificerat certifikat för elektroniska underskrifter och skapas med en särskild anordning för skapande av kvalificerade elektroniska underskrifter. En kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift och ska erkännas som en kvalificerad elektronisk underskrift i alla andra medlemsstater. En utländsk avancerad eller kvalificerad elektronisk underskrift ska även accepteras i medlemsstaternas offentliga e-tjänster om e-tjänsten kräver en avancerad elektronisk underskrift nationellt. De svenska e-legitimationerna, såsom BankID, bedöms generellt uppfylla kraven på avancerade elektroniska underskrifter enligt eIDAS-förordningen. I de svenska författningsreglerade formkrav som finns avseende elektronisk underskrift ställs inte krav på kvalificerade elektroniska underskrifter, utan enbart på avancerade elektroniska underskrifter eller mer allmänt på elektronisk underskrift utan specificering av vilken nivå den ska vara på.

5.7 Digitaliseringen och behovet av e-legitimation

Regeringens mål för digitaliseringen av den offentliga förvaltningen är en enklare vardag för medborgarna, en öppnare förvaltning som stödjer innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten. Regeringen har gjort bedömningen att digitala tjänster ska vara förstahandsval i den offentliga förvaltningens verksamhet och i kontakter med privatpersoner och företag. Det innebär att den offentliga förvaltningen, när det är lämpligt, ska välja digitala lösningar vid utformningen av sin verksamhet. Samtidigt ska säkerheten och skyddet för den personliga integriteten säkerställas. I regeringens digitaliseringsstrategi, som anger inriktningen för regeringens digitaliseringspolitik, betonas att en förutsättning för fortsatt utveckling av digital service till privatpersoner och företag är att medborgarna har en digital identitet. Att kunna styrka sin identitet digitalt på ett enkelt och säkert sätt är avgörande för möjligheten att kunna ta del av digitala tjänster inom såväl den privata som den offentliga sektorn. Identitetskapningar och bedrägerier på internet är ett stort samhällsproblem som får stora konsekvenser både för

den enskilde och för samhällsekonomin. En grundläggande förutsättning för att kunna uppfylla regeringens mål är att det är möjligt att säkerställa att den person som får tillgång till en e-tjänst hos exempelvis en myndighet också är den som han eller hon utger sig för att vara. En väl fungerande och säker elektronisk identifiering är alltså en förutsättning för en väl fungerande digital förvaltning. En stor andel av Sveriges befolkning har redan i dag tillgång till en e-legitimation. BankID är den e-legitimation som dominerar på den svenska marknaden.

Staten har hittills inte tagit ansvar för att medborgarna ska ha tillgång till en statligt utfärdad säker e-legitimation. I regeringsuppdraget till Skatteverket att ta fram ett identitetskort för folkbokförda i Sverige angavs att kortet skulle vara förberett för att kunna bära e-legitimationer och därför borde innehålla ett chip motsvarande det som finns på det nationella identitetskortet. Skatteverket har därefter på eget initiativ sett till att det finns en e-legitimation på id-kortet. Den e-legitimation som finns på id-kortet utfärdas dock inte av Skatteverket utan av AB Svenska Pass. Bolaget har avtal med Skatteverket om att förse det fysiska id-kortet med en e-legitimation. Det innebär att det är AB Svenska Pass och inte Skatteverket som har det juridiska ansvaret gentemot både innehavaren av e-legitimationen och de förlitande aktörer som ingått avtal med AB Svenska Pass.
I regeringsuppdraget till dåvarande Rikspolisstyrelsen att ta fram ett nationellt identitetskort angavs endast att kortet skulle innehålla en funktion för lagring av elektronisk information som i framtiden skulle kunna användas för att lagra till exempel elektroniska signaturer. Det finns i dagsläget således inte någon e-legitimation som utfärdas av en statlig myndighet och som är tillgänglig för alla.

5.8 En statlig e-legitimation

I och med den ökade digitaliseringen är det allt svårare att klara sig i samhället utan tillgång till en e-legitimation. Det anses vara av stor vikt att alla invånare har möjlighet att skaffa en säker e-legitimation som ger tillgång till samhällsfunktionerna. Den betydelse som en säker e-legitimering har för samhällsfunktionerna och brottsbekämpningen gör att det bör övervägas om inte staten bör ta ett större ansvar för att tillförsäkra alla invånare en sådan identitetshandling. I utredningen SOU 2019:14 framgår ett resonemang som pekar på att en myndighet kommer få i uppgift att genomföra detta. Det innebär att den myndigheten behöver upphandla statlig e-legitimation för samtliga medborgare. Nedan följer utdrag från utredningen om varför ett statlig e-legitimation bör tas fram.

Många personer i Sverige har som framgått redan en e-legitimation. Att endast privata aktörer utfärdar e-legitimation medför att staten inte kontrollerar villkoren för e-legitimationerna. Staten har därmed också begränsade möjligheter till insyn och påverkan.

Kravet i Tillitsramverket för Svensk e-legitimation, på fysisk identitetskontroll innebär att utfärdaren måste finnas på många ställen i landet och ha personal som kan utföra en identitetskontroll på ett tillförlitligt sätt. Om utfärdare i stället kan förlita sig på identifiering som görs av en statlig myndighet i samband med utfärdande av den statliga e-legitimationen underlättar det vid nyutgivning av innovativa och säkra e-legitimationer.

En annan viktig aspekt är att bankerna som regel utfärdar BankID endast till sina kunder. De har inte någon skyldighet att utfärda en e-legitimation till alla som vill ha en sådan.

Det finns därför personer som inte kan få BankID. Med en statligt utfärdad e-legitimation kan fler tillförsäkras tillgång till en sådan handling.

Det finns redan i dag en e-legitimation på identitetskort för folkbokförda i Sverige. E-legitimationen utfärdas inte av Skatteverket utan av företaget AB Svenska Pass. Det är dock Skatteverket som utför den identifiering av sökanden som föregår utfärdandet. AB Svenska Pass har som utfärdare det juridiska ansvaret gentemot innehavaren och de förlitande aktörerna. Detta anses inte tillräckligt för att staten ska få den kontroll som krävs för att kunna säkerställa att invånarna har tillgång till en säker e-legitimation. En e-legitimation på tillitsnivå 4 måste finnas på en personlig säkerhetsmodul som skyddar uppgifterna från obehörig åtkomst, vanligen ett kort. För att e-legitimationen ska vara enkel att bära med sig är det naturligt att placera den på en fysisk identitetshandling.

Det underlättar för den enskilde som endast behöver ha en handling med sig. Det är också mer effektivt att utfärda den fysiska identitetshandlingen och e-legitimationen samordnat eftersom samma process kan användas. E-legitimationer på fysiska kort är visserligen i dag ofta krångligare för användaren än mobila lösningar eftersom det krävs någon form av tekniskt hjälpmedel för att använda dem. Man kan därför ställa sig frågan om en statlig e-legitimation som finns på en fysisk identitetshandling kommer att användas i någon större utsträckning. En statlig e-legitimation på ett fysiskt kort som komplement till mobila varianter bidrar dock till att systemet som helhet blir mer stabilt eftersom det finns en alternativ lösning på en stabil bärare. Att endast ha en mobil e-legitimation är en sårbar lösning. Om mobiltelefonen exempelvis blir stulen eller slutar fungera krävs en reservlösning för att den enskilde inte ska stå utan e-legitimation under den tid det tar till dess att en ny finns tillgänglig.

För att kunna använda en e-legitimation som finns på ett id-kort behövs någon form av kortläsare. Kortläsare finns inbyggd i många datorer. Det finns också fristående kortläsare som kan kopplas till en dator. I dag finns det dessutom tekniska lösningar som skulle kunna användas som alternativ till en traditionell kortläsare. Ett alternativ kan vara en applikation i mobiltelefonen som läser av informationen på kortets chip. Genom att läsa av kortet i en sådan applikation kan användaren, precis som vid användning av en mobil e-legitimation, identifiera sig i en e-tjänst.

6 Offentlig sektors behov

6.1 Inledning

För att kartlägga behovet inom offentlig sektor gällande det aktuella ramavtalsområdet samt fånga in och analysera synpunkter för det befintliga ramavtalet har det i förstudien genomförts dels möten med flera olika myndigheter dels via ett referensgruppsmöte med deltagare från myndigheter.

6.2 Myndighetsmöten

Ett flertal individuella möten med myndigheter har genomförts. Kunderna anser att befintligt ramavtal fungerar bra och ställer sig positiva till en förändring gällande avropssätt. De ser gärna att kommande ramavtal erbjuder ett så kallat kombinationsavtal inom området samt en utökning av nuvarande utbud.

Dessa frågor ställdes till myndigheterna vid mötena. En sammanställning av svaren presenteras under frågan.

Hur många ramavtalsleverantörer är lagom att ha på ett kommande ramavtal?

Det är bra med konkurrens men att det inte får vara för många anbud att utvärdera. Mellan sex till åtta ramavtalsleverantörer är bra inom detta område då alla ramavtalsleverantörer inte alltid kan svara på en viss avropsförfrågan.

Behöver det kompletteras med fler produkter och/eller tjänster?

Ja, det saknas möjlighet att avropa e-legitimation. Det saknas även nya typer av bärare så som armband, ringar, USB-stickor och appar. Det är också bra om man samtidigt kan avropa signering eller underskrift på ett och samma ramavtal. Det är bra om man kan köpa en hel lösning som tjänst.

Borde man ändra i avropsordning, exempelvis ett kombinationsavtal?

Ja, det vore bra. Det är inte bra att behöva göra en förnyad konkurrensutsättning om man vill ha något tillbehör eller standardprodukt eftersom det är tidkrävande. Det är också till fördel för mindre avropande organisationer eftersom mindre avropade organisationer har färre antal resurser för att genomföra avrop. Det är viktigt att förnyad konkurrensutsättning finns kvar eftersom många av anskaffningar avser mer avancerade tekniska lösningar som kräver att myndigheten kan ställa egna krav genom den så kallade Kravkatalogen.

Är det något speciellt som ni önskar att vi kravställer kring?

Ja, det vore önskvärt att se över de allmänna villkoren så att det blir lättare att följa dem vid problem med reklamationer samt även vid teknikutveckling detta så att kund inte behöver stanna i äldre teknik i förhållande till vad som finns på marknaden.

Det vore bra om det kravställdes på FIPS-nivåer (Federal Information Processing Standard).

Fakturorna behöver specificeras bättre. Om fakturorna inte blir specificerade enligt krav i avropet borde det finnas någon form av sanktion gentemot ramavtalsleverantören.

Bättre garanti på nya kort.

Utbildning borde tas med som en tjänst för till exempel utbildning via telefoni och Skype.

Finns det något specifikt som behöver förbättras?

Korten borde delas in i olika grupper, exempelvis:

- Passagekort
- ID06
- Smartkort för inloggning, autentisering, signering, serveraccess, identifiering

Övrigt som kom upp vid dessa möten:

Det är viktigt att få in svar från samtliga ramavtalsleverantörer, även om svaret är ”nej”.

Vissa ramavtalsleverantörer är inriktade på en viss typ av affär och vissa andra ramavtalsleverantörer är inriktade på en annan typ av affär. Det är inte negativt, bara en upplysning och hur avropen fungerar. Därför fungerar det att utöka antalet ramavtalsleverantörer inom området.

Vissa avropande organisationer har hög och bred kunskap och hanterar mycket själva medan andra är beroende av att få hjälp med mycket. Ramavtalet måste täcka in behovet för alla olika varianter.

6.3 Referensgruppsmöte med myndigheter

De myndigheter som anmält intresse att medverka i referensgruppen bjöds in till ett möte på Kammarkollegiet.

Sammanlagt bjöds tolv avropsberättigade myndigheter in till referensgruppsmöte. 15 personer från totalt åtta myndigheter deltog.

Syftet med referensgruppsmötena var att, som ett komplement till möten med kunder, på ett fördjupat plan ge myndigheterna möjlighet att dela med sig av sina erfarenheter rörande det befintliga ramavtalet och ge generella synpunkter avseende en eventuellt kommande upphandling av ett statligt ramavtal.

Referensgruppen bidrog till att ta fram upphandlingsföremålet genom en mindre workshop i ämnet ”vad ska ingå i upphandlingen”. Vid mötet framfördes även förslag till kravställning och behov av förändringar i avtalstexter.

Därefter ställdes ett antal frågor som redovisas nedan.

- Finns det dominerande aktörer inom ramavtalet och marknaden i övrigt?

  Ja, det finns det, men de flesta myndigheter ser det som naturligt och att det inte är något problem.

- Finns det lokala marknader och hur fördelas de geografiskt?

  De flesta företagen finns i Stockholmsområdet vilket innebär att en geografisk indelning inte är lämplig. Alla leveranser sker med bud på något sätt och leverantören behöver i princip aldrig vara på plats hos kund.

- Är det svårigheter för små myndigheter att få avropssvar?

  Eftersom det för närvarande finns två större leverantörer på marknaden som tar de mer avancerade affärerna och med tanke på att det är ett antal leverantörer som hanterar de mindre respektive mindre avancerade affärerna, ska det inte vara några problem för de mindre myndigheterna att få avropssvar. Det finns en större konkurrens inom segmentet för mindre affärer.

- Är ramavtalsleverantörerna inriktade på större myndigheter?

  Ja, två av ramavtalsleverantörerna är det eftersom de större myndigheterna ofta är i behov av tjänstekort eller SIS-kort och det är ju endast två av ramavtalsleverantörerna som kan erbjuda det.

- Kan ett ramavtal som är rangordnat eller ett kombiramavtal underlätta för små myndigheter att erhålla avropssvar?

  Ja, ett kombinationsavtal skulle vara bra för både mindre myndigheter och för kompletteringsavrop.

- Hur komplexa och avancerade är ramavtalen för en mindre myndighet?

  Oavsett om myndigheten är liten eller stor kan det vara komplicerat med en förnyad konkurrensutsättning. Dock så måste den förnyade konkurrensutsättningen finnas kvar eftersom det är det avropssättet som mest detaljerat kan ringa in behovet genom att kunna ställa egna krav utifrån en så kallad kravkatalog. Kravkatalogen innehåller områden inom vilka avropande myndighet själva kan lägga till krav inom.

- Finns det anledning att utveckla ett särskilt ramavtal för små myndigheter?

  Nej, inte ett helt eget ramavtal däremot om det finns ett kombinationsavtal med fördelningsnyckel och med förnyad konkurrensutsättning som avropssätt i samma avtal, kommer det att underlätta för mindre myndigheter.

  Om man i ett kommande ramavtal skulle öka antalet ramavtalsplatser är sannolikheten den att det blir fler leverantörer som kan svara på mindre avrop.

6.4 Sammanfattning av referensgruppsmöte

I huvudsak är myndigheterna nöjda med ramavtalsområdet. Det finns behov av att köpa produkter som idag inte finns med på ramavtalet men sannolikt kommer framtida ramavtalsområde även inkludera dessa. Anledningen till att dessa produkter inte finns att köpa på befintligt ramavtal är att det har skett en teknikutveckling under åren som gått och dessa produkter inte fanns som produkt vid tiden för tidigare upphandling.

De synpunkter som var mest framträdande är bland annat svårigheten att reklamera kort som kvalitetsmässigt inte upprätthöll krav från både upphandling och avrop. Det är även svårt att hantera vite för sen leverans eftersom det är små belopp det rör sig om.

Styrkan i befintligt ramavtal är den att ramavtalet är flexibelt vid avrop. Man kan enkelt kravställa utifrån det egna behovet.

Befintligt ramavtal tillgodoser i huvudsak behovet hos avropande myndigheter och organisationer och behovet kan tillgodoses genom ett rikstäckande ramavtal. Det finns inget behov av geografisk närhet för leverantörer inom ramavtalet i förhållande till kund.

Det finns önskemål om att förbättra avtalsskrivningar gällande vite och reklamationer samt även försöka hantera frågan gällande leverans av kort och koder till kort. Dessa delar är kostnadsdrivande eftersom rekommenderad försändelse används vid varje enskilt tillfälle. Det är önskvärt att fundera över detta i kommande upphandling så att dessa kostnader kan minimeras för avropande myndigheter.

Myndigheter och organisationer ser gärna att ramavtalsområdet utökas med ett antal produkter samt även med e-legitimation.

6.5 Möte med andra myndigheter

Projektet har träffat Myndigheten för digital förvaltning, DIGG.

DIGGs uppdrag är bland annat att tillhandahålla och tillse att det finns ramverk för e-underskrifter, e-legitimationer och de förvaltar Tillitsramverket och EIDAS-noden. EIDAS-noden sammanbinder andra länder med deras e-legitimationer.

En sökande kan hos DIGG ansöka om att få möjlighet till att utfärda e-legitimation.

DIGG ser gärna att Kammarkollegiet upphandlar detta område på nytt och att Kammarkollegiet då även inkluderar e-legitimation och signering. DIGG hänvisar gärna till Kammarkollegiets ramavtal.

DIGG ser gärna att ett samarbete vid ramavtalsupphandlingen genomförs eftersom kraven i ramavtalsupphandlingen kan bygga på det ramverk som DIGG tar fram. Det blir då enklare för sökande att uppfylla ramverket om de redan är ramavtalsleverantör eller underleverantör på Kammarkollegiets ramavtal. Till exempel kan ett förslag till krav i ramavtalsupphandlingen vara att anbudsgivare ska kunna påvisa att de har levererat till EIDAS.

6.6 Möte med kundorganisationer

6.6.1 Möte med Inera AB

Inera AB ägs av SKL Företag, Regioner och Kommuner. Inera AB koordinerar och utvecklar gemensamma digitala lösningar till nytta för invånare, medarbetare och beslutsfattare.

Anledningen till att projektet träffade Inera AB är att de hanterar en digital lösning för korthantering åt regioner och kommuner. Inera AB ansvarar för upphandling av deras tekniska plattform och att anslutna regioner och kommuner samt driftansvaret för den tekniska plattformen.

Inera AB ser att framtiden för bärare inte enbart är kort utan även andra typer av bärare.

Dagens distribution av kort är dyr eftersom varje kort skickas med rekommenderad post, REK. Det skulle vara önskvärt om det gick att samdistribuera till en adress på något sätt för att få ner kostnaderna.

Det vore även bra om pin/puk/säkerhetskoder kunder skickas till en elektronisk brevlåda som man kan logga in i via exempelvis mobilt BankID istället för som idag via REK.

Utbudet inom kommande ramavtalsområde bör vara kort, fotostationer eller liknande, portallösning, programvara till exempelvis datorn, tilläggsutrustning mot ett öppet API samt tillbehör.

Gällande den administrativa portalen är det viktigt att kunna kravställa exempelvis kring flöden både avseende beställning men även aktivering, ekonomisk historik, tjänstekortsaktivering, ta fram GDPR-uppgifter i en standardrapport och kunna skapa egna rapporter.

6.6.2 Möte med SKR, Sveriges Kommuner och Regioner, tidigare SKL

SKR ser sig positiva till att en ny ramavtalsupphandling inom området genomförs. Det är viktigt att alla kommuner och regioner ansluter sig som avropsberättigade till ett kommande ramavtal.

SKR ser gärna att ett nytt ramavtal inkluderar e-legitimation och även gärna signering samt kanske även att kunna köpa korthantering som tjänst.

SKR redogjorde för hur de har kartlagt behovet av en e-legitimation i tjänsten. En kort summering av deras enkät menar att:

- Många kommuner och regioner använder sig av identifiering av den som loggar in på tjänsten via e-legitimation och då används i de flesta fall BankID.
- Kommuner och regioner har många tjänster som kräver elektronisk underskrift
- Anskaffning av e-legitimation sker via ramavtal
- Det är ungefär hälften som är anslutna via eIDAS
- Leverantörer som används för eIDAS är exempelvis Svensk eID, CGI, Visma och Nexus.
- Behovet för e-legitimation i tjänst är främst för autentisering mot egna it-system, autentisering mot andra organisationers it-system, e-underskrifter och kryptering av e-post samt elektroniska underskrifter.

6.6.3 Status eIDAS augusti 2019

Anslutna länder med tillåtna e-legitimationer i svenska offentliga e-tjänster:

- Estland
- Italien
- Kroatien
- Spanien
- Tyskland

Anslutna svenska e-legitimationer som kan användas inom EU:

- Inga

Antal anslutna till eIDAS i Sverige:

- 22 myndigheter
- 89 kommuner (30 procent)

Antal e-tjänster där andra länders e-legitimation kan användas:

- Inga (det fungerar bara med personnummer)

7 Marknadsundersökning

7.1 Inledning

För att kartlägga marknadens utbud inom det aktuella ramavtalsområdet och fånga in och analysera synpunkter på det befintliga ramavtalet har det i förstudien genomförts dels en enkätundersökning riktad till befintliga ramavtalsleverantörer dels möten med nuvarande ramavtalsleverantörer samt därutöver ett antal potentiella leverantörer.

7.2 Marknaden

Det finns maximalt ungefär tio leverantörer på marknaden. Fem av dessa är i dag ramavtalsleverantör på befintligt ramavtal. De befintliga ramavtalsleverantörerna finns i Stockholmsområdet. Några befintliga ramavtalsleverantörer har bäst kompetens för mer komplicerade lösningar för korthantering medan några andra tar de lite enklare affärerna. På så sätt kompletterar de varandra väl och täcker tillsammans behovet för större avropande myndigheter såväl som för mindre. Eftersom det finns flera leverantörer på marknaden mot dagens antal ramavtalsplatser och mot bakgrund av att det skulle kunna bli en bättre konkurrenssituation om det var fler ramavtalsleverantörer, innebär det att antalet tilldelade leverantörer skulle kunna ökas i en upphandling. Från dagens fem ramavtalsleverantörer till fler, förslagsvis mellan sex till åtta ramavtalsleverantörer.

Utöver det som ingick sedan föregående upphandling har marknaden utvidgats med e-legitimation och funktioner som man kan använda sin e-legitimation till exempelvis underskrift.

Det är inte lika stor efterfrågan på fotostationer nu som det var vid föregående upphandling eftersom tekniken gällande att ta foton har blivit lättare att hantera med annan typ av utrustning. Men behovet finns fortfarande och fotostationer bör fortsättningsvis vara en del av ett kommande ramavtal.

Det finns både stora företag inom branschen samt även mindre. De mindre kan inkomma med egna anbud men de skulle även kunna vara underleverantörer. I första hand vill de själva vara ramavtalsleverantörer.

Om ramavtalsleverantörsutbudet ska vara på det sätt som det är idag, det vill säga en blandning med små och stora företag, är det fördelaktigt att alla krav inte ställs som obligatoriska eftersom det skulle utarma antalet anbud. Mycket få eller knappt någon leverantör kan leverera samtliga typer av kort, andra produkter och tjänster som offentlig sektor sammantaget har behov av.

Produkterna och tjänsterna säljs direkt av ramavtalsleverantörerna och i vissa fall tas underleverantörer till hjälp. Inga återförsäljare är aktuella.

De leverantörer som projektet har träffat har inga problem att hantera personuppgifter och/eller vara personuppgiftsansvariga.

Konsulttjänster betalas vanligen efter utfört arbete. Produkter betalas vid köptillfället. Konsulttjänster kan betalas per timme eller per uppdrag.

Det finns intresse hos offentlig sektor att kunna ställa säkerhetskrav på leverantörerna vid avrop och de leverantörer som projektet har träffat har inga problem med att möta säkerhetskrav.

Det finns även intresse hos offentlig sektor av att kunna ställa miljö- och hållbarhetskrav gällande produkter och tjänster, utöver de som ställs i ramavtalsupphandlingen. Leverantörerna har inga problem med att sådana krav kan ställas vid avrop.

Leverantörerna har heller inga problem med att krav gällande tillgänglighet och användbarhet ställs i både ramavtalsupphandling och vid avrop.

En av de befintliga ramavtalsleverantörerna, Gemalto AB, har blivit uppköpta av annat bolag som heter Thales AB. Gemalto AB kvarstår som ramavtalsleverantör, i denna förstudie träffade vi representanter från Thales AB.

En annan ramavtalsleverantör har bytt namn och heter numera Idemia Sweden AB istället för Oberthur Technologies AB.

7.3 Möte med leverantörer

7.3.1 Om leverantörsmöten

Projektet har träffat sju olika leverantörer inom området. Fem av dem är befintliga ramavtalsleverantörer. Agendan för dessa möten var ett antal frågor samt en övrigpunkt.

7.3.2 Redovisning av leverantörsmöten

Leverantörerna ser gärna att antalet ramavtalsplatser är ungefär så många som det finns idag, men det spelar inte så stor roll ifall antalet ramavtalsplatser ökar till cirka sju.

Leverantörerna tycker att det är en mycket bra idé att göra ett kombinationsavtal där en del är för avrop med förnyad konkurrensutsättning samt en del med en fördelningsnyckel som baserar sig på ett antal i förväg bestämda och specificerade produkter. Detta på grund av att leverantörerna har uppfattat att kunderna antingen inte känner till ramavtalsområdet och därmed missar att avropa från det och istället direktupphandlar eller att de tycker att en förnyad konkurrensutsättning är allt för krävande för en enklare anskaffning. Vidare anser leverantörerna att det skulle förenkla även för dem om en

fördelningsnyckel införs, eftersom de inte behöver lägga ner massa tid på att svara på enklare avropsförfrågningar med ett större avropssvar via förnyad konkurrensutsättning.

Två av sju leverantörer har kollektivavtal inom området.

Leverantörerna är till största del inte certifierade för något miljöledningssystem eller kvalitetsledningssystem. Några leverantörer är certifierade för informationssäkerhetssystem, men inte alla leverantörer.

De flesta leverantörer har rutiner för hur man bistår personal med specialbehov så att tillgängligheten för all personal tillgodoses.

Alla leverantörer anser att ramavtalsområdet borde inkludera e-legitimation.

Merparten av befintliga ramavtalsleverantörer tycker att ramavtalsområdet har fungerat bra, vissa tycker dock att omsättningen har varit oväntat låg.

Det är inget problem för leverantörerna att hantera fakturor i Peppolformat. De flesta leverantörer kan ordna en kundunik webbsida.

De trender som leverantörerna ser inom detta område är:

- e-legitimation
- köpa kortportalen som tjänst
- andra typer av bärare än enbart kort, så som mobil, USB, appar (walletlösningar)

För mer information kring Idemia Sweden AB och Världsbanken hänvisar vi till uppdaterad information på Avropa.

8 Relevant lagstiftning, föreskrifter och allmänna råd

8.1 Lagar och föreskrifter

Följande lagar och föreskrifter kan komma att behöva beaktas i en kommande upphandling

- Säkerhetsskyddslag (2018:585) gällande hanteringen av identitetskort
- Offentlighets- och sekretesslag (2009:400) gällande bestämmelser om sekretess i en myndighets personaladministrativa verksamhet.
- Polisens FAP för Tjänstekort
- Andra interna regler för Tjänstekort
- Svenska institutet för standarder gällande identitetskort
- Myndigheten för digitalisering gällande tillitsnivåer
- Lag (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering
- Europaparlamentet och rådets förordning 910/2014 om elektronisk identifiering och betrodda tjänster före elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG
- Lag (2016:561) med kompletterade bestämmelser till EU:s förordning om elektronisk identifiering
- Förordning (2016:576) med kompletterade bestämmelser till EU:s förordning om elektronisk identifiering

8.2 Val av upphandlingslag

Tidigare ramavtalsupphandling genomfördes med stöd av lag (2011:1029) om offentlig upphandling på försvars- och säkerhetsområdet, (LUFS).

Eventuellt kommande ramavtalsupphandling bör också upphandlas enligt LUFS eftersom personaliseringen av kort kan behöva ske i Sverige och innehåller uppgifter av känslig karaktär.

Utrustning av känslig karaktär definieras i 2 kap. 29 § LUFS. ”Med utrustning av känslig karaktär, byggentreprenad av känslig karaktär och tjänster av känslig karaktär avses utrustning, byggentreprenad och tjänster som har ett säkerhetssyfte och som inbegriper, kräver eller innehåller säkerhetsskyddsklassificerade uppgifter.”

9 Hållbarhet

9.1 Inledning

Med hållbar offentlig upphandling menas att offentlig sektor tillgodoser sitt behov av varor och tjänster på ett sätt som säkerställer den goda affären sett till hela livscykeln. Hänsyn

ska inte bara tas till de fördelar som uppstår för organisationen utan även till samhället i sin helhet, samtidigt som anskaffningen görs på ett sätt som minimerar skador på miljön.

Kammarkollegiets målsättning är att inom ramen för verksamhetens uppdrag, offentlig sektors behov och lagstiftningens möjligheter, på ett ansvarfullt sätt ska beakta miljö och sociala hänsyn vid upphandling och förvaltning av de statliga ramavtalen. De statliga ramavtalen ska bidra till att offentlig sektor kan möta de mål som satts i den nationella upphandlingsstrategin, Agenda 2030 och de nationella miljömålen.

Förutsättningarna för hållbarhetskrav varierar dock mellan de olika ramavtalsområdena och branscherna. I förstudiearbetet utreds därför vilket behov av hänsyn till de olika hållbarhetsdimensionerna som behöver tas för att möta olika strategiska mål men även de risker som finns inom det specifika ramavtalsområdet.

Av 4 kap. 3 § LOU framgår att en upphandlande myndighet bör beakta miljöhänsyn, social och arbetsrättsliga hänsyn vid offentlig upphandling om upphandlingens art motiverar detta. Hållbarhetshänsyn kan tas i alla delar av en upphandling, det vill säga som kvalificeringskrav (till exempel krav på miljöledningssystem), som tekniska krav (till exempel krav på viss märkning eller certifiering), eller som kontraktsvillkor (till exempel arbetsrättsliga villkor).

Av 17 kap. 4 § LOU framgår vilka skyldigheter en upphandlande myndighet har att kräva att leverantören fullgör kontraktet i enlighet med ILO:s kärnkonventioner. Detta gäller i de fall svensk arbetsrätt inte är tillämplig.

Nedan redovisas vilka analyser gällande hållbarhetshänsyn (miljö och sociala krav) som genomförts för det aktuella ramavtalsområdet.

9.2 Miljökrav

Det finns i princip inga miljömärkningar för produkter inom området. Området är smalt och det är en begränsad efterfrågan inom området.

Man skulle kunna tänka sig att ställa krav på miljövänligt lim när kortens skikt limmas, men risken finns att ett miljömärkt lim är av sämre kvalitet och då går kortens skikt upp och kan inte användas. Det i sin tur påverkar miljön dåligt eftersom ett nytt kort måste tillverkas.

Möjligtvis kan man ta fram alternativa miljövänliga produkter som ett alternativ, om det finns sådana produkter. De produkter som i så fall kan bli aktuella är korthållare av återvunnen plast till exempel. I övrigt gäller standarder och riktlinjer elektronikprodukter.

Leverantörerna kan redovisa bakåt i leverantörs- och tillverkningskedjan gällande var komponenterna kommer ifrån.

9.3 Sociala krav

Med sociala krav avses villkor om lön, semester och arbetstid vilka de arbetstagare som utför uppdraget minst ska tillförsäkras Beslut om och i så fall vilka sociala krav ska ställas i en upphandling ska förgås av en så kallad behövlighetsbedömning. I denna görs analys av risken för oskäliga arbetsvillkor i den aktuella upphandlingen, samt i förlängningen risken för att konkurrensen snedvrids. Villkoren ska ha en anknytning till det som upphandlas, och vara proportionerliga. Kraven gäller även underleverantörer som direkt medverkar till att fullgöra kontraktet.

Projektet anser att det finns behov av att ställa villkor i enlighet med ILO:s kärnkonventioner eftersom delar av tillverkningen av komponenter till bland annat korten sker i länder där då svensk lag inte är tillämplig. Det kan finnas en risk att arbetsrättigheter inte respekteras gällande tillverkning utanför Sverige.

Vad gäller transporttjänster som anlitas i ramavtalet, är Kammarkollegiets bedömning att de är att anse som mindre delar av kontraktet samt att vi inte köper tillräckligt stor del av transporterna.

Majoriteten av de leverantörer som vi har träffat använder inget kollektivavtal inom området. Två av de leverantörer som vi träffade använder sig av kollektivavtal och det är ett IT-avtal respektive Unionens kollektivavtal.

Leverantörerna använder sig av egna avtal med goda avtalsvillkor. Projektet har inte funnit några risker med dessa avtal och branschen uppfattas inte som någon riskbransch med oskäliga villkor för de anställda.

Projektgruppen bedömer att det inte behöver ställas särskilda arbetsrättsliga villkor i en eventuellt kommande upphandling.

10 Säkerhet och SUA

Verksamhet som omfattas av säkerhetsskyddslagen (2018:585) ska ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Ansvaret för säkerhetsskyddet ligger hos den som är verksamhetsansvarig. När det i utförandet av en tjänst förekommer uppgifter som med hänsyn till Sveriges säkerhet omfattas av sekretess (hemliga uppgifter) har staten, kommunerna och regionerna ansvaret för att det finns ett fullgott säkerhetsskydd hos leverantören.

För att tillgodose kravet på säkerhetsskydd när sådan verksamhet utförs på uppdrag av en myndighet, ska den uppdragsgivande myndigheten träffa ett skriftligt avtal – säkerhetsskyddsavtal – med ramavtalsleverantören om det säkerhetsskydd som behövs i det enskilda fallet. Vid de ramavtal där behov av säkerhetsavtal föreligger bör en sådan möjlighet anges i ramavtalet.

11 Dataskyddsförordningen

Inom ramen för förstudiens rekommendation kommer ramavtalsleverantörerna inte enbart behandla personuppgifter såsom personuppgiftsansvariga. Detta innebär att ett personuppgiftsbiträdesavtal kan komma att behöva tecknas vid anskaffning från ramavtal enligt föreslagen indelning. Detta innebär att personuppgiftsbiträdesavtal samt även kravställning enligt dataskyddsförordning ska beaktas i ramavtalsupphandlingen.

12 E-handel

Med elektronisk handel (e-handel) menas ett sätt att skapa en effektiv inköpsprocess med IT som stöd. Elektronisk affärskommunikation ersätter den pappersbaserade kommunikationen. Avtal, leverantörer, priser med mera blir lättillgängliga för de som ska beställa varor och tjänster, därför att avrop/beställningar och fakturahanteringen kan ske elektroniskt. E-handel enligt denna definition förutsätter att köparen hanterar sin elektroniska affärskommunikation via sitt e-handelssystem. Att en enskild handläggare inom köparens organisation gör inköp i en leverantörs webbshop via ett individuellt inloggningskonto betraktas inte som e-handel.

Målsättningen är att de leverantörer som tecknar statliga ramavtal med Kammarkollegiet ska medverka till att avropande myndigheter kan tillämpa e-handel och därmed leva upp till strategi, förordning och lagstiftning.

Kammarkollegiet ställer krav på e-handel i alla upphandlingar. Förutsättningarna för att tillämpa e-handel varierar dock mycket mellan olika ramavtalsområden och branscher. I förstudiearbetet utreds därför förutsättningarna för e-handel för det aktuella ramavtalsområdet. Kammarkollegiet följer SFTI:s rekommendationer om hur man kravställer på e-handel vid upphandling av varor och tjänster.

Leverantörerna inom detta område har olika möjlighet till e-handelslösningar. Vissa leverantörer kan erbjuda olika typer av e-handelslösningar medan andra leverantörer endast kan erbjuda enklare varianter av e-handelslösningar.

Produkterna och tjänsterna som området inkluderar lämpar sig inte speciellt väl för avancerade e-handelslösningar eftersom det i många fall är specialanpassade produkter för kund. Det kan säkert vara genomförbart för vissa kunder, förutsatt att leverantörerna klara av att genomföra efterfrågad e-handelslösning. Det finns vissa produkter inom området som en e-handelslösning fungerar väldigt enkelt för, till exempel korthållare och andra lite enklare produkter.

Den 1 april 2019 blir det lag på att alla inköp i offentlig sektor ska faktureras med e-faktura. Kammarkollegiet ställer alltid krav på e-faktura. Samtliga leverantörer som förstudieprojektet har talat med kan hantera Peppol-format gällande e-faktura.

13 Andra upphandlingar inom området

Kammarkollegiet har upphandlat inom ett ramavtalsområde som heter Säkerhetsteknik som bland annat omfattar inpasseringslösningar till byggnader. Ramavtalsområdet är helt begränsat till inpassering i byggnader.

Det finns även ramavtal inom området för programvaror och tjänster som inkluderar e-underskrifter. Dessa ramavtal tillhör också Kammarkollegiets ramavtal.

.

14 Utvecklingsområden och förändringsbehov i en kommande upphandling

Kommande upphandling behöver utöka sortimentet i ramavtalet med e-legitimation som möjliggör exempelvis e-underskrift i tjänsten. Vidare bör ramavtalsområdet tydligt kompletteras med legitimation för byggnadsbranschen, så kallat ID06. Idag kan ID06 avropas med det är inte helt tydligt att dessa kort ingår i nuvarande ramavtal. Tjänster kopplade till samtliga produkter är också nödvändigt för att ramavtalsområdet ska upplevas som komplett vid avrop. Vidare behöver området även omfatta möjlighet att köpa vissa produkter som tjänst. Området behöver även utökas med fler olika typer av bärare, utöver kort, så som armband, ringar, USB-stickor med flera.

15 Slutsatser

Projektgruppen förordar att en upphandling inom området för identifiering och behörighet genomförs. Området behöver utökas med e-legitimation eftersom både efterfrågan från myndigheterna och utbudet på marknaden pekar mot en sådan lösning. Även om omsättningen för nuvarande ramavtalsområde har varit låg, så bedömer projektet att det är viktigt att en ny upphandling genomförs därför att en statlig ramavtalsupphandling gynnar samhället utveckling med ytterligare användning av e-legitimation i samband med digitaliseringen. Kammarkollegiet kan också samarbeta med flera myndigheter vid genomförande av en nationell ramavtalsupphandling, vilket anses vara av särskild betydelse för en förvaltningsgemensam utveckling och effektivisering inom området.

Eventuellt kommande upphandling bör omfatta produkter och tjänster kopplade till lösningar för identifiering och behörighet i enlighet med föregående upphandling med en utökning inom området med vissa produkter och tjänster så som e-legitimation, fler typer av olika bärare samt även möjlighet att kunna köpa aktuella produkter som tjänst.

Avrop bör ske genom ett kombinationsavtal, dels via en förnyad konkurrensutsättning och att vissa delar av produktsortimentet kan avropas via ett enklare avropssätt med så kallad fördelningsnyckel.

Antalet ramavtalsplatser kan utökas till omkring sju eller åtta stycken.

Upphandlingen bör fortsättningsvis även upphandlas genom lag (2011:1029) om offentlig upphandling på försvars- och säkerhetsområdet, LUFS.

16 Källförteckning

16.1 Möten med myndigheter

Arbetsförmedlingen

Myndigheten för digital förvaltning

Inera AB som representerar kommuner och regioner inom detta område

Försvarsmakten

Försäkringskassan

Migrationsverket

Polisen

Skatteverket

Statens fastighetsverk

Sveriges Kommuner och Regioner, SKR

16.2 Möten med leverantörer

Cards and more Sverige AB

Idemia Sweden AB (Tidigare Oberthur Technologies AB)

PartnerSec AB

Seriline AB

Technology Nexus Secured Business Solutions AB

Telia Sverige AB (Cygate AB är ramavtalsleverantör)

Thales Sverige AB (Gemalto AB är ramavtalsleverantör)

16.3 Referenslitteratur och andra källor

Betänkandet av 2017 års ID-kortutredning ”Ett säkert statligt ID-kort – med e-legitimation”, Statliga offentliga utredningar, SOU 2019:14.

www.inera.se

www.digg.se