





## Upphandlande organisation

Statens inköpscentral vid Kammarkollegiet

Ylva Lovén Anderson





### Symbolförklaring:

-  Texten ingår i annonsen
-  Texten/frågan innehåller krav som måste uppfyllas
-  Texten kommer att ingå i avtalet
-  Texten ingår i kvalificeringen

## Upphandling

Kort för identifiering och behörighetskontroll

96-22-2013

-  Texten kommer att publiceras i avtalskatalogen
-  Texten innehåller sekretessbelagd information
-  Frågan är viktad och ingår i delen av upphandlingen
-  Frågan besvaras av köparen

# 1. Inbjudan att inkomma med anbud

## 1.1. Inbjudan

### 1.1.1. Innehållsförteckning

Denna anbudsinvitan består av följande kapitel och bilagor.

Kapitel:

1. Inbjudan att inkomma med anbud
2. Administrativa bestämmelser
3. Kravspecifikation

Bilagor:

- Bilaga Avropsberättigade
- Bilaga Undertecknande och sanningsförsäkran
- Bilaga Huvudtext
- Bilaga Allmänna villkor
- Bilaga Säkerhetsskyddsavtal
- Bilaga Personuppgiftsbiträdesavtal
- Bilaga Kravkatalog

Bilaga Kravkatalog innehåller krav som kan komma att ställas vid avrop från det kommande ramavtalet.

### 1.1.2. Inledning

Statens inköpscentral vid Kammarkollegiet, i fortsättningen kallad Statens inköpscentral, inbjuder selekterade företag, i fortsättningen kallad anbudsgivare, att inkomma med anbud avseende ramavtalsupphandling av kort för både fysisk och elektronisk identifiering och behörighetskontroll. Upphandlingen är benämnd *Kort för identifiering och behörighetskontroll* och avser hela den offentliga förvaltningen i Sverige.

Statens inköpscentral ansvarar bland annat för att samordna upphandling inom IT-området för offentlig förvaltning. Statens inköpscentral verkar för att bästa möjliga villkor skapas för

anskaffning och användning av informationsteknik inom den offentliga sektorn, samt att offentlig förvaltning använder gemensamma funktioner och lösningar.

Syftet med de statliga ramavtalen är;

- att kostnadseffektivisera avropande kunders inköpsverksamhet och därigenom hushålla med offentliga medel.
- att tillgodose avropande kunders behov inom efterfrågat område.
- att skapa fördelaktiga ramavtalsvillkor inom ramen för upphandlingsområdet.
- att verka för att minska den tid det tar för avropande kunder att införskaffa varor och tjänster.

För mer information om Statens inköpscentral, se

[www.kammarkollegiet.se/statensinkopscentral](http://www.kammarkollegiet.se/statensinkopscentral)

För ytterligare information om Statens inköpscentrals andra upphandlingar, samordnade ramavtal och praktisk vägledning, se [www.avropa.se](http://www.avropa.se)

Statens inköpscentral tar, enligt regeringens beslut och efter samråd med Ekonomistyrningsverket (ESV), ut en administrationsavgift av ramavtalsleverantörer avseende all försäljning under respektive ramavtal för att täcka verksamhetens samtliga kostnader. Ramavtalsleverantörer erlägger för närvarande en avgift om 0,7 procent av fakturerat nettobelopp, det vill säga fakturavärdet exklusive mervärdesskatt.

### 1.1.3. Bakgrund

Ett av de områden som Statens inköpscentrals ramavtal täcker är tjänstekort och andra id-handlingar (identifieringshandlingar) samt tjänster kopplade till korten. Detta ramavtalsområde, som benämndes "Tjänstekort och andra id-handlingar", gick efter maximal förlängning ut den 31 augusti 2013. Då behov av ett dylikt ramavtalsområde föreligger avser Statens inköpscentral härmed att upphandla och teckna nya ramavtal.

Syftet med denna upphandling är att, med utgångspunkt från offentlig förvaltnings behov och marknadens utbud, underlätta och skapa bästa möjliga villkor för anskaffning av kort för identifiering och behörighetskontroll inom upphandlingsområdet. En förstudie är genomförd för att undersöka omfattning, inriktning och upplägg av upphandlingen. Förstudiens förslag är vägledande för upphandlingens innehåll, syfte och kravställning. Förstudien benämning är Tjänstekort och andra ID-handlingar, dnr 96-63-2012.

### 1.1.4. Avropsberättigade

Ramavtalen kommer att kunna användas för avrop av statliga myndigheter under regeringen samt andra statliga upphandlande myndigheter, landsting och kommuner som lämnat fullmakt. Dessa framgår av bilagan *Avropsberättigade*.

Myndigheter under regeringen deltar med stöd av förordning (1998:796) om statlig inköpsamordning. Myndigheter under riksdagen och andra statliga offentligt styrda organ deltar med stöd av att de lämnat fullmakt till Statens inköpscentral att upphandla ramavtal för deras räkning.

Kommuner och landsting kommer vid tiden för tilldelningsbeslutet själva att fatta ett tilldelningsbeslut baserat på Statens inköpscentrals tilldelningsbeslut. I det fall en kommun eller ett landsting inte godtar utvärderingsresultatet måste detta meddelas till Statens inköpscentral. Den aktuella kommunen eller landstinget som lämnat fullmakt kommer då att tas bort från bilagan *Avropsberättigade*. Detta innebär att bilagan *Avropsberättigade* kan komma att förändras inför ramavtalstecknandet.

### 1.1.5. Upphandlingsföremålet

Upphandlingen Kort för identifiering och behörighetskontroll omfattar följande varor och tjänster:

- 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 elektroniska del. Ett smartkort definieras i denna upphandling som ett kort som kan lagra och/eller processa information. Dessa kan t ex 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 t ex vara chip, beröringsfri teknik och/eller magnetremsa och med möjlighet till installerade certifikat och konfigurering av PIN-kod.

- Personaliserade kort för fysisk identifiering och/eller behörighetskontroll

Med detta avses primärt kort vars fysiska egenskaper och användning är det viktiga.

Exempel på denna typ av kort är identitetskort, SIS-märkta identitetskort (SS 61 43 14) och tjänstekort för anställda i offentlig sektor.

- Upphandlingen omfattar 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 kopplade till korten som omfattas av 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 ingår också i upphandlingen.

- Beställningsstation

Upphandlingen omfattar en lösning, bestående av både hård- och programvara, för att inhämta och spara personuppgifter till kort samt även att beställa kort, dvs 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.

-Tillbehör

Upphandlingen omfattar även olika tillbehör t.ex. kortläsare och korthållare.

### 1.1.6. Avropsordning

Avrop från detta ramavtal sker genom en förnyad konkurrensutsättning, enligt lag (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS) 5 kap. 7 § och ska föregås av en skriftlig avropsförfrågan som avropsberättigad gör för att värdera vilken ramavtalsleverantör som ska tilldelas kontrakt.

1. Avropsberättigad ska upprätta en avropsförfrågan för att inbjuda samtliga ramavtalsleverantörer att lämna avropssvar i enlighet med de villkor som avropsberättigad anger.

Avropsberättigad kan utöver de krav som ställts i upphandlingen uppställa krav i enlighet med **bilaga Kravkatalog** och vid behov precisera avtalsvillkoren och komplettera med

andra krav och villkor som angetts i upphandlingen.

2. Avropsberättigad ska ange de kriterier som kommer att ligga till grund för tilldelning av kontraktet. Dessa kriterier ska omfattas av de kriterier som har angivits i upphandlingens förfrågningsunderlag.

Avropsberättigad avgör vilka av dessa kriterier som är relevanta för det specifika avropstillfället.

3. Avropsberättigad ska ange en skälig tidsfrist för att lämna avropssvar. Tidsfristen ska fastställas med hänsyn till avropsföremålets komplexitet och omfattning samt den tid som behövs för att lämna avropssvar. Ramavtalsleverantör som vid avropstillfället inte kan leverera efterfrågad varor och/eller tjänster är ändå skyldig att svara på avropet och ange skäl till varför Ramavtalsleverantör inte kan leverera. I det fall Ramavtalsleverantören inte kan leverera ska Ramavtalsleverantören även meddela detta till ramavtalets kontaktpersoner.

4. Avropssvaren ska vara skriftliga. Avropsberättigad får ta del av avropssvaret först när angiven svarstid har löpt ut.

5. Kontraktet ska tilldelas den ramavtalsleverantör som lämnat det för avropsberättigad bästa avropssvaret på grundval av de kriterier och villkor som angetts i avropsförfrågan.

6. Avropsberättigad ska snarast möjligt skriftligen meddela de ramavtalsleverantörer som deltagit i den förnyade konkurrensutsättningen om beslut om tilldelning av kontrakt och redovisa skälen för beslutet.

Vid avrop från ramavtal börjar ingen automatisk avtalsspärr att löpa. Avropsberättigad kan dock frivilligt iaktta en avtalsspärr för att undvika att ett ingånget kontrakt ska kunna ogiltigförklaras i ett senare skede. I det fall avropsberättigad väljer att beakta den frivilliga avtalsspärren ska detta framgå i tilldelningsbeslutet.

Observera att om avropet i sig innehåller säkerhetsskyddsklassificerade uppgifter måste säkerhetsskyddsavtal tecknas med de ramavtalsleverantörer som vill ta del av avropet innan avropets ingående handlingar kan lämnas ut.

Avropande kund ska träffa personuppgiftsbiträdesavtal och eventuellt säkerhetsskyddsavtal med såväl ramavtalsleverantör som eventuella underleverantörer. En ramavtalsleverantör kan aldrig gentemot avropande kund ansvara för bearbetning av personuppgifter eller säkerhetsskyddet hos en underleverantör.

Avropande kunder ska kunna få sin försörjning inom området tillgodosedd genom att sluta långa leveransavtal. Enstaka anskaffningar ska också vara möjliga.

#### **1.1.7. Ramavtalets ikraftträdande och giltighetstid**

Ramavtalet träder i kraft efter att det signerats av båda parter.

Ramavtalet är giltigt i 24 månader från och med ramavtalets signering.

Ramavtalet upphör att gälla utan uppsägning den sista dagen i den månad som infaller 24 månader från signering.

Eventuell förlängning av ramavtalet sker på initiativ av Statens inköpscentral. Förlängning av ramavtalets avtalsperiod kan uppgå till högst 60 månader. Förlängning kan ske i etapper.

#### **1.1.8. Uppllysning om lagstiftning**

Statens inköpscentral vill uppmärksamma anbudsgivare om att avrop från de ramavtal som blir resultatet av denna upphandling och genomförande av kontrakt, regleras bland annat av följande lagar och förordningar.

\* För hantering och bearbetning av personuppgifter vid personalisering av korten gäller

*personuppgiftslagen (1998:204)*. Ett personuppgiftsbiträdesavtal som ska användas vid kontrakt medföljer därför denna upphandling

\* Vissa avrop kommer att avse kort med sekretessbelagda personuppgifter vilket regleras bland annat i *offentlighets- och sekretesslag (2009:400) 22 kap.*

\* Vissa avrop kommer att avse kort med personuppgifter som är säkerhetsskyddsklassificerade. Dessa säkerhetsskyddsklassificerade uppgifter regleras i *säkerhetsskyddslag (1996:627)* och *säkerhetsskyddsförordningen SFS 1996:633* som ger bestämmelser till *säkerhetsskyddslagen*. Vid avrop som bl a innefattar hantering av säkerhetsklassificerade uppgifter ska säkerhetsskyddsavtal tecknas mellan avropande kund och ramavtalsleverantörer samt även mellan avropande kund och eventuella underleverantörer till ramavtalsleverantören.

\* Vissa avrop kan komma att avse kort som är tjänstekort. Tjänstekort regleras av *förordning om tjänstekort SFS 1958:272* som bl a innehåller bestämmelser om vem som får utfärda tjänstekort och för vem samt vad korten ska innehålla för uppgifter.

\* Vissa avrop kan komma att avse identitetskort. För t.ex. identitetskort för folkbokförda i Sverige gäller *förordning (2009:284) om identitetskort för folkbokförda i Sverige*.

## 2. Administrativa bestämmelser

### 2.1. Administrativa bestämmelser

#### 2.1.1. Allmänt

Anbudsgivare ska i sin anbud visa att de krav som ställs i förfrågningsunderlaget uppfylls. Om anbudsgivare inte visar att de ställda kraven uppfylls eller inte svarar på frågorna, kommer detta att tolkas som att kraven inte kan uppfyllas eller att kravet inte kan accepteras.

Anbudsgivare uppmanas att följa anvisningarna i detta förfrågningsunderlag. Det är av yttersta vikt att anbud innehåller samtliga efterfrågade uppgifter, särskilt då möjligheten att efter anbudstidens utgång inhämta eller inkomma med förtydliganden eller kompletterande uppgifter är begränsad.

Anbudsgivare uppmanas att noggrant gå igenom sitt anbud innan det lämnas in för att kontrollera att den efterfrågade informationen verkligen finns med i anbudet samt kontrollera att samtliga bilagor bifogats. Observera att ställda krav ska vara uppfyllda senast sista dag för anbud, såvida inte annat uttryckligen anges i anslutning till kravet i förfrågningsunderlaget.

#### 2.1.2. Upphandlingsförfarande

Upphandlingen genomförs med selektivt förfarande enligt lag (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFSS), 4 kap 1§.

Detta innebär i korthet följande stegvisa förfarande:

1. Annonsering av upphandlingen
2. Anbudsansökan inkommer till Statens inköpscentral från företag som önskar delta i anbudsgivningen.
3. Statens inköpscentral gör en selektering och ett eventuellt urval av vilka anbudssökande som inbjuds att lämna anbud baserat på kvalificeringskraven och ansökningarna.
4. Selekterad anbudssökande inbjuds att lämna anbud och dessa utvalda anbudssökande erhåller förfrågningsunderlaget.
5. Anbud inkommer från utvalda företag.
6. Prövning om anbuden uppfyller ställda ska-krav.
7. Utvärdering av prövade anbud.
8. Beslut om ramavtalsleverantörer.
9. Utskick av tilldelningsbeslut.
10. Ramavtalstecknande.

Statens inköpscentral har annonserat denna upphandling i Europeiska unionens tidning (EUT). Annonser är avsedda via TendSign.

#### 2.1.3. Alternativa anbud

Alternativa anbud accepteras inte. I de fall en anbudsgivare inkommer med fler anbud kommer Statens inköpscentral anse det senast inkomna som det giltiga anbudet.

#### 2.1.4. Anbudets språk



Anbudet som lämnas i TendSign ska vara skrivet på svenska. Svenska språket tillämpas vid all kommunikation rörande denna upphandling, med undantag för intyg, certifikat och bevis som kan vara på engelska.

#### 2.1.5. Utvärdering och urval

Utvärdering och urval av anbud kommer att genomföras i tre (3) steg.

1. I det första steget provas om anbudet uppfyller de obligatoriska krav (ska-krav) som ställs. De anbud som inte uppfyller de obligatoriska kraven kommer att uteslutas från vidare utvärdering.

2. I steg två görs en utvärdering av svar på ställda utvärderingskriterier (bör-krav) för de kvarvarande anbudena. Anbudsgivarens svar kommer att bedömas och tilldelas poäng i enlighet med respektive utvärderingskriterium.

3. Om två eller flera anbud efter utvärdering av bör-krav behöver särskiljas för att avgöra vem som erbjuds teckna ramavtal kommer priset angivet i krav Urval på pris användas. Lägsta pris kommer att få företräde.

Om två eller flera anbud efter utvärdering och urval i steg 3 behöver särskiljas, kommer lottning att genomföras för att slutligen särskilja anbudena. Lottningen kommer att genomföras med minst tre (3) personer, från Statens inköpscentral, samt med Notarius Publicis närvarande för att säkerställa förfarandets opartiskhet.

#### **2.1.6. Högst antal ramavtal**

Statens inköpscentral har för avsikt att teckna högst fem (5) ramavtal.

#### **2.1.7. Inlämning av anbud**



Statens inköpscentral använder sig av det webbaserade upphandlingsverktyget Tendsign för upphandling samt hantering av ansökan och anbud. Tendsign ägs av Visma Opic AB.

Anbud lämnas elektroniskt via Tendsign, vilket innebär att anbud inte kan lämnas i pappersformat eller via fax eller e-post.

Företrädare för anbudsgivare ansluter sig personligen till tjänsten Tendsign genom att registrera ett användarkonto på Tendsigns hemsida, [www.tendsign.com](http://www.tendsign.com)

Anbudsgivare bör registrera användarkontot i god tid innan inlämning.

Anbudsgivare uppmanas använda följande förfarande: Logga in, gå in under "Annonser", "Aktuella annonser", välj upphandlande myndighet "Statens inköpscentral vid Kammarkollegiet" och aktuell upphandling och diarienummer.

För supportfrågor gällande hanteringen av systemet kan Tendsigns support kontaktas på telefon 013-474 75 20.

Det är även möjligt att komma i kontakt med Tendsign via deras hemsida. Då Tendsigns support inte har öppet dygnet runt är det viktigt att ta kontakt i god tid innan sista anbudsdag för att på så sätt garanteras teknisk support.

Den e-postadress som anbudsgivare använt för sin inloggning i systemet, är den som gäller för all vidare kommunikation i upphandlingen både från och till Statens inköpscentral.

#### **2.1.8. Anbudets giltighetstid**



Anbudsgivaren är bunden av sitt anbud åtta (8) månader efter sista anbudsdag. Vid en eventuell överprövning kan giltighetstiden för anbudena komma att förlängas. Statens inköpscentral kommer i sådana fall att begära bekräftelse hos anbudsgivaren att denne godkänner förlängningen.

#### **2.1.9. Kostnader i samband med anbud**

Anbudsgivare äger inte rätt till ersättning för anbud eller för kostnader som uppstår i

samband med anbud.

#### **2.1.10. Sista dag för inkommande med anbud**



Anbud ska ha inkommit senast 2013-12-19. För sent inkommet anbud behandlas inte.

#### **2.1.11. Frågor om förfrågningsunderlaget**

Alla frågor om förfrågningsunderlaget ställs till Statens inköpscentral via upphandlingsverktyget Tendsign. Den e-postadress som anbudsgivare använt för sin inloggning i systemet, är den som gäller för all vidare kommunikation i upphandlingen mellan Statens inköpscentral och anbudsgivare.

Förfrågningsunderlaget ska på ett tydligt och transparent sätt beskriva vad som ska upphandlas. Skälen till att upphandlingen görs och orsaken till att den genomförs på ett visst sätt eller att vissa krav ställs ligger däremot, enligt Statens inköpscentral, utanför ramen för upphandlingen. Av den anledningen besvaras endast frågor som är relevanta för själva upphandlingen.

Frågor om varför ett visst krav ställts kommer inte att besvaras. För att samtliga anbudsgivare ska behandlas lika, kommer frågor att besvaras och förmedlas till samtliga anbudsgivare via Tendsign. Alla frågor och svar som publiceras är avidentifierade.

Frågor och svar utgör en del av förfrågningsunderlaget. Om förfrågningsunderlaget behöver kompletteras med anledning av frågor från anbudsgivare, eller av någon annan anledning, kommer kompletteringen att finnas i Tendsigns frågor-och-svarsfunktion samt sändas, via den e-postadress som anbudsgivare använt för sin inloggning i systemet, till alla som via Tendsign hämtat förfrågningsunderlaget.

De av Statens inköpscentral lämnade svaren avseende förfrågningsunderlaget är endast bindande om svaren lämnats via Tendsign. Anbudsgivare är själv skyldig att hålla sig uppdaterad och ta del av den information som publiceras under anbudstiden. Om anbudsgivare inte registrerar sig på [www.tendsign.com](http://www.tendsign.com) utan hämtar förfrågningsunderlaget på annat sätt, kan Statens inköpscentral inte garantera att all information, som frågor och svar, under anbudstiden kommer anbudsgivaren tillhanda. Anbudsgivaren ansvarar i så fall själv för att kontrollera och hämta eventuell tillkomna upplysningar.

Sista dag för att ställa frågor är 2013-12-11. Frågor ställda senare kommer inte att besvaras.

Sista dag för att besvara frågor är 2013-12-16.

#### **2.1.12. Rättelse av fel och kompletteringar**

Anbudsgivare kan inte på eget initiativ vidta ändringar i eller kompletteringar till anbudet efter sista anbudsdag. Däremot kan anbudsgivare, på begäran av Statens inköpscentral, få rätta uppenbara felskrivningar eller felräkningar eller annat uppenbart fel. Statens inköpscentral får också begära att anbud förtydligas eller kompletteras efter sista dag för anbud, om det inte finns risk för särbehandling eller konkurrensbegränsning. Anbudsgivande har ingen motsvarande rätt att få ett förtydligande eller komplettering till stånd.

#### **2.1.13. Öppning av anbud**

Öppning av inkomna anbud äger rum så snart som möjligt efter sista dag för inlämning av anbud i närvaro av minst två personer från Statens inköpscentral.



#### 2.1.14. Tilldelningsbeslut

Tilldelningsbeslut kommer att fattas så snart som möjligt efter att anbudet inkommit.

#### 2.1.15. Sekretess

Uppgifter i ett upphandlingsärende omfattas av absolut sekretess enligt offentlighets- och sekretesslagen (2009:400) till dess upphandlingen offentliggjorts, beslut fattats eller upphandlingen på annat sätt avslutats. Därefter blir ansökan och anbudet enligt huvudprincipen i 2 kap. tryckfrihetsförordningen (1949:105) offentliga allmänna handlingar. Delar av ansökan och anbudet kan dock omfattas av kommersiell sekretess.

För kommersiell sekretess till skydd för en anbudsgivares uppgifter krävs att uppgifterna avser affärs- eller driftförhållanden för anbudsgivare samt att det av särskild anledning kan antas att anbudsgivare lider skada om uppgifterna röjs. För det fall anbudsgivare anser att de uppgifter som lämnats i upphandlingsärendet uppfyller vad som krävs för kommersiell sekretess, kan anbudsgivare skriftligen inkomma med begäran om att uppgifter i anbudet ska sekretessbeläggas. Sådan begäran ska innehålla precisering av vilka uppgifter som avses samt vilken skada som skulle uppkomma om anbudsgivares uppgifter röjs.

Observera dock att uppgifter som rör utvärderingen endast undantagsvis är av sådan karaktär att de kan sekretessbeläggas av kommersiella skäl.

Statens inköpscentral kommer inte på förhand att ge besked om en viss uppgift kommer att omfattas av sekretess utan sekretessprövning sker först i samband med att en uppgift begärs ut. Slutlig prövning kan komma att ske i domstol.

*Begärs sekretess? Ange namn på bilaga om sådan bifogas.  
(Fritextsvar)*

#### 2.1.16. E-signering av ramavtal



Statens inköpscentral tillämpar e-signering av ramavtal. Detta ställer krav enligt nedan på blivande ramavtalsleverantörer.

För att kunna utföra e-signering i Statens inköpscentrals upphandlingsverktyg Tendsign ska ramavtalsleverantör ha en e-legitimation hos utfärdare av e-legitimationer samt konto hos Chambersign för tjänsten CSign och signering. Konto och signering av Statens inköpscentrals ramavtal via CSign är kostnadsfri för ramavtalsleverantör.

CSign stöder ett flertal e-legitimationer. Läs mer på CSign.se för beställning av e-legitimation samt för anslutning till CSign och konto för e-signeringstjänst.

## 3. Kravspecifikation

### 3.1. Krav på kort

#### 3.1.1. Verifiering av krav på kort

##### 3.1.1.1. Verifiering av krav på kort

Statens inköpscentral kan komma att verifiera ställda krav på kort genom att begära in exempel på av anbudsgivaren eller av dess underleverantör tillverkade kort som uppfyller kraven. Anbudsgivare ska kunna leverera kort inom fyra veckor från Statens inköpscentral begäran.

#### 3.1.2. Typkort: blankt opersonaliserat smartkort utan foto

##### 3.1.2.1. Typkort: blankt opersonaliserat smartkort utan foto



Anbudsgivaren ska kunna leverera blanka, opersonaliserade smartkort utan foto enligt följande specifikation:

##### Krav på kortets fysiska egenskaper:

Kortet ska vara tillverkat av Polycarbonat och följa standarden ISO/IEC 7810:2003 eller likvärdig.

##### Krav på chip:

Kortet ska ha chip med processor samt övriga mekanismer för att chip ska kunna utföra signering och kryptering med RSA-nycklar.

Chip ska uppfylla Evaluation Assurance Level 4+ (EAL 4+) eller högre och kraven för Common Criteria Protection Profile Secure Signature Creation Device (SSCD).

Chip ska följa Global Platform Specifikation 2.1.1 eller senare och förses med en applet för standard ISO/IEC 7816-15:2004 eller likvärdig.

Chip ska kunna hantera kontrollsummaberäkningar med SHA-1

Chip ska kunna hantera kontrollsummaberäkningar med SHA-256

##### Följande krav ställs på chip om RSA används:

Chip ska levereras med minst två förgenererade RSA-nyckelpar med minst 2048-bitar nyckellängd.

Kunden ska ha möjlighet att själv skapa minst ytterligare tre nyckelpar med 1024-bitars (för att kunna stödja legacy system) eller 2048-bitars RSA nyckellängd som genereras intern i chip.

Kunden ska ha möjlighet att själv importera RSA-nyckelpar.

-Prestandan ska vara följande:

- privat 2048-bit nyckeloperation med algoritmen RSAES-OAEP (dekryptering) ska utföras på < 500ms

- privat 2048-bit nyckeloperation med algoritmen RSASSA-PSS (signering) ska utföras på < 500ms

##### Följande krav gäller kortets profil:

Profilen på kortet ska ha minst två PIN-koder.

Chip ska uppfylla standard ISO/IEC 7816-15:2004 eller likvärdig.

Chip ska ha stöd för omformatering av standard ISO/IEC 7816-15:2004-strukturen eller likvärdig och samtliga nyckelpar, men inte möjlighet att sätta egen PIN- och PUK-kod.

PIN2 som används för oavvislighetscertifikatet, ska uppfylla standard ISO/IEC 7816-15:2004 eller likvärdig definition på userConsent med värde 1.  
PIN1 som används för autentiseringcertifikatet, ska inte uppfylla standard ISO/IEC 7816-15:2004 definition på userConsent. Den ska tillåta flera RSA-operationer i följd för att kunna hantera PIN-pad.  
Storleken på chip ska vara minst 64 kB

Det ska finnas plats för minst 20 certifikat pekare.  
Det ska finnas minst 25kB ledigt utrymme för certifikatdata.  
PIN- och PUK-kod ska vara möjliga att byta.

Följande krav ställs på kortdrivrutin:

Kortdrivrutin ska ha stöd för följande operativsystem:  
- Windows 7 eller senare mot CryptoAPI och PKCS#11  
- MacOS X 10.6 eller senare mot PKCS#11  
- Linux SLED 11.0 eller senare mot PKCS#11

Övriga krav: \_\_\_\_\_

Korten ska vara försedda med beröringsfri teknik enligt ISO/IEC 14443-4:2008 eller likvärdig som t ex kan användas för inpassering.  
Korten ska ha magnetremsa som medger att korten kan användas för t ex inpasseringssystem.  
Korten med magnetremsa ska följa standard ISO/IEC 7811:1995 eller likvärdig.

Uppfylls kravet? (Ja/Nej svar)

Kravgräns

Ja

Nej



### **3.1.3. Typkort: personaliserat smartkort för elektronisk identifiering och/eller behörighetskontroll med foto**

#### **3.1.3.1. Personaliserat smartkort för elektronisk identifiering och/eller behörighetskontroll med foto**



Anbudsgivaren ska kunna leverera personaliserade smartkort för elektronisk identifiering och/eller behörighetskontroll med foto och namn enligt följande specifikation:

Krav på kortets fysiska egenskaper:

Kortet ska vara tillverkat av Polycarbonat och följa standarden ISO/IEC 7810:2003 eller likvärdig.

Krav på chip:

Kortet ska ha chip med processor samt övriga mekanismer för att chip ska kunna utföra signering och kryptering med RSA- nycklar på kortet.  
Chip ska uppfylla Evaluation Assurance Level 4+ (EAL 4+) eller senare och kraven för Common Criteria Protection Profile Secure Signature Creation Device (SSCD).  
Chip ska följa Global Platform Specifikation 2.1.1 eller senare samt förses med en applet för standard ISO/IEC 7816-15:2004 eller likvärdig.  
Chip ska kunna hantera kontrollsummaberäkningar med SHA-1  
Chip ska kunna hantera kontrollsummaberäkningar med SHA-256

#### Följande krav ställs på chippet om RSA används:

Chip ska levereras med minst två förgenererade RSA-nyckelpar med minst 2048-bitar nyckellängd.

Kunden ska ha möjlighet att själv skapa minst tre ytterligare nyckelpar med 1024-bitars (för att kunna stödja legacy system) eller 2048-bitars RSA nyckellängd som genereras intern i chip.

Kunden ska ha möjlighet att själv importera RSA-nyckelpar.

Krav på prestandan:

- privat 2048-bit nyckeloperation med algoritmen RSAES-OAEP (dekryptering) ska utföras på < 500ms
- privat 2048-bit nyckeloperation med algoritmen RSASSA-PSS (signering) ska utföras på < 500ms

#### Följande krav gäller kortets profil:

Profilen på kortet ska ha minst två PIN-koder.

Chip ska uppfylla standard ISO/IEC 7816-15:2004 eller likvärdig.

Chip ska ha stöd för omformatering av standard ISO/IEC 7816-15:2004-strukturen eller likvärdig och samtliga nyckelpar, men inte möjlighet att sätta egen PIN- och PUK-kod.

PIN2 som används för oavvislighetscertifikatet, ska uppfylla standard ISO/IEC 7816-15:2004 definition eller likvärdig på userConsent med värde 1.

PIN1 som används för autentiseringcertifikatet, ska inte uppfylla standard ISO/IEC 7816-15:2004 definition på userConsent. Den ska tillåta flera RSA-operationer i följd för att kunna hantera PIN-pad.

Storleken på chip ska vara minst 64 kB

Det ska finnas plats för minst 20 certifikat pekare.

Det ska finnas minst 25kB ledigt utrymme för certifikatdata.

Chip ska levereras med antingen transportcertifikat eller personlig e-legitimation.

Processen för nedskrivning av den personliga e-legitimationen på chip ska uppfylla aktuell e-legitimationsutfärdares regelverk (CP/CPS)

PIN- och PUK-kod ska vara möjliga att byta.

#### Följande krav ställs på kortdrivrutin:

Kortdrivrutin ska ha stöd för följande operativsystem:

- Windows 7 eller senare mot CryptoAPI och PKCS#11
- MacOS X 10.6 eller senare mot PKCS#11
- Linux SLED 11.0 mot PKCS#11

#### Övriga krav:

Korten ska vara försedda med beröringsfri teknik enligt ISO/IEC 14443-4:2008 eller likvärdig som t ex kan användas för inpassering.

Korten ska ha magnetremsa som medger att korten kan användas t ex för inpasseringssystem.

Korten med magnetremsa ska följa standard ISO/IEC 7811:1995 eller likvärdig.

Uppfylls kravet? (Ja/Nej svar)

Kravgräns

Ja

Nej



### **3.1.4. Utvärderingskrav**

#### **3.1.4.1. Säkerhetsmönster i flera färger**

Anbudsgivaren bör kunna leverera kort som förses med synliga tryckta säkerhetsmönster i mer än en färg.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.2. Säkerhetstryck

Anbudsgivaren bör kunna leverera kort där delar av det synliga säkerhetstrycket kan gå in över kortinnehavarens bild.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.3. Information

Anbudsgivaren bör kunna leverera kort där någon del av kortets information utförs i tydlig upphöjd (taktill) lasergravyr.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.4. Information i anslutning till bild

Anbudsgivaren bör kunna leverera kort där det i anslutning till bilden bör finnas möjlighet att ange olika typer av information, t.ex. personnummer.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.5. Konturlinjer

Anbudsgivaren bör kunna leverera kort där innehavarens bild inte har ram eller konturlinjer.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.6. Lasergraverad namnteckning

Anbudsgivaren bör kunna leverera kort med lasergraverad namnteckning som bör kunna återges i i olika storlek.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.7. Optically Variable Device

Anbudsgivaren bör kunna leverera kort som förses med Optically Variable Device, i detta fall en form av säkerhetsdetalj som visar olika information, beroende på betraktnings- och/eller belysningsförhållanden.

Korten bör innehålla tydligt urskiljbara motiv.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.8. Utformning av fönster

Anbudsgivaren bör kunna leverera kort med unikt utformade fönster med en oregelbunden form.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.9. Krav på prestanda på chippet

Anbudsgivaren bör kunna leverera kort med följande prestanda.

- privat 2048-bit nyckeloperation med algoritmen RSAES-OAEP (dekryptering) bör utföras på < 250ms
- privat 2048-bit nyckeloperation med algoritmen RSASSA-PSS (signering) bör utföras på < 250ms

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.10. Omformatering av kort

Anbudsgivaren bör ha möjlighet till omformatering av kortets chip via en av kortleverantör levererad PKCS#11.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.11. Eliptic Curve Cryptography-nycklar

Anbudsgivaren bör kunna leverera kort med Eliptic Curve Cryptography-nycklar (ECC-nycklar).

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.12. ECC med minst 224-bitars nycklar

Anbudsgivaren bör kunna leverera kort med chip som hanterar ECC med minst 224-bitars nycklar.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.13. ECC - förgenererade nyckelpar

Anbudsgivaren bör kunna leverera kort med chip med två förgenererade ECC-nyckelpar med minst 224-bitars nyckellängd.

Uppfylls kravet? (Ja/Nej svar)

% 7,14 🗳️

100 Ja  
0 Nej

#### 3.1.4.14. Import av ECC-nyckelpar

Kunden bör själv kunna importera ECC-nyckelpar vid avrop av kort med ECC-nycklar.

100 Ja

0 Nej

### 3.1.5. Urval baserat på pris

#### 3.1.5.1. Urval på pris

Anbudsgivaren ska ange pris för blanka, opersonaliserade smartkort utan foto enligt följande specifikation.

Styckpris per kort ska anges i SEK. Priset är ett takpris och ska upprätthållas under tolv månader från dagen för avtalstecknande.

##### Krav på kortets fysiska egenskaper:

Kortet ska vara av Polycarbonat och följa standarden ISO/IEC 7810:2003 eller likvärdig.

##### Krav på chip:

Kortet ska ha chip med processor samt övriga mekanismer för att chip ska kunna utföra signering och kryptering med RSA-nycklar.

Chip ska uppfylla Evaluation Assurance Level 4+ (EAL 4+) och kraven för Common Criteria Protection Profile Secure Signature Creation Device (SSCD).

Chip ska följa Global Platform Specifikation 2.1.1 och förses med en applet för standard ISO/IEC 7816-15:2004 eller likvärdig.

Chip ska kunna hantera kontrollsummaberäkningar med SHA-1

Chip ska kunna hantera kontrollsummaberäkningar med SHA-256

##### Följande krav ställs på RSA :

Chip ska levereras med två förgenererade RSA-nyckelpar med 2048-bitars nyckellängd.

Kunden ska ha möjlighet att själv skapa ytterligare tre nyckelpar med 1024-bitars (för att kunna stödja legacy system) eller 2048-bitars RSA nyckellängd som genereras intern i chip.

Kunden ska ha möjlighet att själv importera RSA-nyckelpar.

-Prestandan ska vara följande:

- privat 2048-bit nyckeloperation med algoritmen RSAES-OAEP (dekryptering) ska utföras på < 500ms

- privat 2048-bit nyckeloperation med algoritmen RSASSA-PSS (signering) ska utföras på < 500ms

##### Följande krav gäller kortets profil:

Profilen på kortet ska ha två PIN-koder.

Chip ska uppfylla standard ISO/IEC 7816-15:2004 eller likvärdig.

Chip ska ha stöd för omformatering av standard ISO/IEC 7816-15:2004-strukturen eller likvärdig och samtliga nyckelpar, men inte möjlighet att sätta egen PIN- och PUK-kod.

PIN2 som används för oavvislighetscertifikatet, ska uppfylla standard ISO/IEC 7816-15:2004 eller likvärdig definition på userConsent med värde 1.

PIN1 som används för autentiseringcertifikatet, ska inte uppfylla standard ISO/IEC 7816-15:2004 definition på userConsent. Den ska tillåta flera RSA-operationer i följd för att kunna hantera PIN-pad.

Storleken på chip ska vara 64 kB

Det ska finnas plats för 20 certifikat pekare.

Det ska finnas 25kB ledigt utrymme för certifikatdata.  
PIN- och PUK-kod ska vara möjliga att byta.

Följande krav ställs på kortdrivrutin:

- Kortdrivrutin ska ha stöd för följande operativsystem:
- Windows 7 eller senare mot CryptoAPI och PKCS#11
  - MacOS X 10.6 eller senare mot PKCS#11
  - Linux SLED 11.0 eller senare mot PKCS#11

Övriga krav:

Korten ska vara försedda med beröringsfri teknik enligt ISO/IEC 14443-4:2008 eller likvärdig som t ex kan användas för inpassering.

Korten ska ha magnetremsa som medger att korten kan användas för t ex inpasseringssystem.

Korten med magnetremsa ska följa standard ISO/IEC 7811:1995 eller likvärdig.

Vänligen ange styckpris per kort i SEK. (Fritextsvar)

### 3.2. Krav på beställningsstation

#### 3.2.1. Beställningsstation

Anbudsgivaren ska beskriva vilka komponenter, dvs vilken hård- och programvara, som ingår i den beställningsstation som anbudsgivaren erbjuder.


Av beskrivningen ska Statens inköpscentral kunna följa hur komponenterna används för att inhämta persons namnteckning, fotografera, registrera personuppgifter, spara foto och personuppgifter samt överföra beställning och uppgifter till leverantör på elektronisk väg.

Beskrivning: (Fritextsvar)

### 3.3. Acceptans av avtal samt undertecknande och sanningsförsäkran

#### 3.3.1. Huvudtext

Anbudsgivaren ska acceptera villkoren i bilaga Huvudtext i dess helhet.

Accepteras villkoren i bilaga Huvudtext i dess helhet? (Ja/Nej svar) 


Kravgräns \_\_\_\_\_

Ja

Nej

#### 3.3.2. Allmänna villkor

Anbudsgivaren ska acceptera villkoren i bilaga Allmänna villkor i dess helhet.

Accepteras villkoren i bilaga Allmänna villkor i dess helhet. (Ja/Nej svar) 


Kravgräns \_\_\_\_\_

Ja

Nej

#### 3.3.3. Personuppgiftsbiträdesavtal

Anbudsgivaren ska acceptera villkoren i bilaga Personuppgiftsbiträdesavtal i dess helhet.

Accepteras villkoren i bilaga Personuppgiftsbiträdesavtal i dess helhet? (Ja/Nej svar) 

Kravgräns \_\_\_\_\_

Ja

Nej



### 3.3.4. Säkerhetsskyddsavtal



Anbudsgivaren ska acceptera villkoren i bilaga Säkerhetsskyddsavtal i dess helhet.

*Acceptera villkoren i bilaga Säkerhetsskyddsavtal i dess helhet.*



*(Ja/Nej svar)*

Kravgräns

Ja

Nej

### 3.3.5. Sanningsförsäkran



Anbudsgivaren ska på heder och samvete försäkra att lämnade uppgifter i anbudet är sanningsenliga och korrekta. Det elektroniska anbudet och samtliga villkor i upphandlingen godkännes genom att behörig företrädare för anbudsgivaren fyller i och undertecknar bilaga *Undertecknande och sanningsförsäkran*, skannar in den och bifogar den tillsammans med anbudet i PDF-format. I det fall anbudet undertecknas av person som är behörig att företräda anbudsgivaren utan att vara behörig firmatecknare kan dokumentet för styrkande av rätten att underteckna anbudsgivaren i efterhand komma att inhämtas.

*Bifoga undertecknad bilaga Undertecknande och sanningsförsäkran: (Bifogat dokument)*

