# Redovisning av krav och villkor avseende informationssäkerhet i ramavtalsupphandling av Identifiering och behörighet

Box 2218, 103 15 Stockholm
Birger Jarlsgatan 16, Stockholm

www.kammarkollegiet.se
registratur@kammarkollegiet.se

Telefon 08-700 08 00
Telefax 08-700 09 98

Organisationsnummer 202100-0829

# 1 Inledning

Detta dokument redovisar krav och villkor avseende informationssäkerhet som använts i ramavtalsupphandlingen av Identifiering och behörighet. Det innehåller även krav som kan ställas vid avrop. Dokumentet är avsett att ge en bild av hur informationssäkerhetsfrågor hanterats i den aktuella ramavtalsupphandlingen.

Krav och villkor är hämtade från upphandlingsunderlag och ramavtal. För de fullständiga dokumenten hänvisas till information på avropa.se.

Kraven och villkoren är här indelade på följande sätt:

**Kravkatalog**

Kravkatalogen innehåller informationssäkerhetskrav och villkor som kan ligga till grund för kompletteringar och preciseringar vid avrop. Den avropsberättigade kan välja ut och formulera lämpliga krav.

**Kvalificeringskrav**

Kvalificeringskrav är obligatoriska krav på leverantören som ska vara uppfyllda redan när anbud lämnas in.

**Tekniska krav**

Tekniska krav avser obligatoriska krav på upphandlingsföremålet, produkten och eller tjänsten ställda i ramavtalsupphandlingen. Dessa krav kan vara uttryckta som ”ska-krav”.

**Tilldelningskriterier**

Tilldelningskriterier avser krav på egenskaper hos upphandlingsförmålet, produkten och eller tjänsten, som gett ett mervärde i ramavtalsupphandlingen, exempelvis poäng, påslag eller avdrag. Dessa krav kan vara uttryckta som ”bör-krav”.

**Särskilda kontraktsvillkor**

Särskilda kontraktsvillkor är krav och villkor som leverantör och upphandlingsförmål ska uppfylla vid ramavtalets fullgörande. Dessa villkor finns i ramavtalets Huvuddokument och i Allmänna villkor samt i Kravkatalog. Även andra benämningar förekommer.

# 2 Kravkatalog

I det fall ett rangordnat ramavtal upphandlas utgår avsnitt 2. Följande krav från kravkatalogen kan ett avrop kompletteras med. Rubriksättningen hänvisar till kravkatalogen, vilken kan ses i sin helhet under Gemensamma dokument.

**5.1.3 Certifiering**

Vid Avrop kan krav komma att ställas på certifiering av exempelvis viss hårdvara, Programvara, Tjänster eller Konsulttjänster.

**5.1.6 Drift**

Vid Avrop kan krav komma att ställas på förutsättningarna för drift av aktuella tjänster.

**5.1.7 E-legitimationer**

Vid Avrop kan krav komma att ställas på e-legitimation. Kraven kan exempelvis avse tillitsnivåer enligt DIGG:s tillitsramverk eller kvalitetsmärkningen Svensk e-legitimation.

**5.1.9 Funktionalitet**

Vid Avrop kan krav komma att ställas på funktionalitet. Kraven kan även avse hur funktionaliteten uppfylls och förändras under Kontraktets giltighetstid.

**5.1.10 Fysiska egenskaper**

Vid Avrop kan krav komma att ställas på olika fysiska egenskaper hos olika bärare, funktionella tjänster eller andra Produkter. Dessa krav kan bland annat omfatta hela eller delar av ISO/IEC 7810:2019.

**5.1.11 Hårdvara**

Vid Avrop kan krav komma att ställas på hårdvara exempelvis storlek, bestyckning, komponenter och kompatibilitet. Krav kan även ställas på hårdvarans funktionalitet.

### 5.1.12 Informationssäkerhet

Vid Avrop kan krav komma att ställas på informationssäkerhet till exempel krav på identifiering, möjlighet att sätta rättigheter och behörigheter samt loggning. Krav även komma att ställas på olika standarder så som Common Criteria.

### 5.1.13 Integration

Vid Avrop kan krav komma att ställas på att det som avropas är möjligt att integrera med Avropsberättigads befintliga miljö.

### 5.1.14 Installation

Vid Avrop kan krav komma att ställas på installation. Med installation avses hjälp och stöd med att installera hårdvara eller Programvara i Avropsberättigads lokaler.

### 5.1.15 Konfiguration

Vid Avrop kan krav komma att ställas på konfiguration. Med konfiguration avses hjälp med att kundanpassa parametrar för Avropsberättigads behov.

### 5.1.16 Konsultkompetens

Vid Avrop kan krav komma att ställas på exempelvis Konsults erfarenhet, kunskaper och kompetensnivå. Krav kan även ställas på leveranskompetens.

### 5.1.17 Kortets egenskaper och funktioner

Vid Avrop kan krav komma att ställas på korts olika egenskaper och funktioner exempelvis på kort där det i anslutning till bilden ska finnas möjlighet att ange olika typer av information så som personnummer.

### 5.1.21 Migrering

Vid Avrop kan krav komma att ställas på migrering. Med migrering avses planering för och flytt av data och funktionalitet.

### 5.1.28 Säkerhet

Vid Avrop kan krav komma att ställas på säkerhet exempelvis fysisk säkerhet, informationssäkerhet, signalskydd och IT-säkerhet samt även pseudonymisering och tillitsnivåer.

#### 5.1.29 Säkerhetsskyddsavtal

Vid Avrop kan krav komma att ställas på att Ramavtalsleverantör och Underleverantör ingår Säkerhetsskyddsavtal med Avropsberättigad.

#### 5.1.30 Tekniska egenskaper

Vid Avrop kan krav komma att ställas på olika tekniska egenskaper exempelvis längd på krypteringsnycklar, chipets tekniska egenskaper, överföringsprotokoll, lasergravyr, konturlinjer och olika typer av information till bilden.

#### 5.1.31 Tekniska förutsättningar

Vid Avrop kan krav komma att ställas på olika avropsobjektets interoperabilitet och kompatibilitet med den Avropsberättigades tekniska miljö.

#### 5.1.32 Test

Vid Avrop kan krav komma att ställas på tester av olika slag. Med test avses exempelvis planering för och test av installation och funktionalitet, konfiguration, migrering, systemutveckling, integration och avveckling.

# 3 Kvalificeringskrav

## Krav på ramavtalsleverantörens informationssäkerhetsarbete

#### 4.5.6 Säkerhet

#### 4.5.6.1 Ledningssystem för informationssäkerhet

Sökande ska ha ett strukturerat och dokumenterat ledningssystem för informationssäkerhet.

Ledningssystemet för informationssäkerhet ska omfatta samtliga delar av Sökandes verksamhet som medverkar i fullgörandet av Ramavtalet. Ledningssystemet för informationssäkerhet ska minst innehålla nedan punkter, A-H.

Som alternativ till redovisning av ledningssystem för informationssäkerhet godtas redovisning av att ett gällande certifikat som minst uppfyller nedan punkter, A-H. Certifikatet som redovisas ska vara utställt av ett ackrediterat certifieringsorgan

som är medlem eller ansluten till någon av de internationella organisationerna för ackrediteringsorgan enligt nedan.

- EA (European co-operation for Accreditation),
- IAF (International Accreditation Forum), eller
- ILAC (International Laboratory Accreditation Cooperation).

Ledningssystemet för informationssäkerhet ska minst innehålla:

**A. Process för bedömning av informationssäkerhetsrisker**
Ledningssystemet för informationssäkerhet ska innehålla rutiner för fastställande och tillämpning av en process för bedömning av informationssäkerhetsrisker som upprättar och underhåller kriterier för riskacceptans och kriterier för bedömningar av informationssäkerhetsrisker. Processen ska säkerställa att upprepade bedömningar av informationssäkerhetsrisker genererar konsistenta, korrekta och jämförbara resultat.

Processen ska omfatta att informationssäkerhetsriskerna identifieras genom tillämpning av processen för bedömning av informationssäkerhetsrisker för att identifiera risker förknippade med förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen för ledningssystem för informationssäkerhet. Processen ska omfatta att informationssäkerhetsriskerna analyseras genom att bedöma de potentiella konsekvenser som skulle uppstå om riskerna som identifieras realiseras.

Vidare ska den realistiska sannolikheten för förekomsten av de risker som identifieras bedömas och risknivåer fastställas. Informationssäkerhetsriskerna ska utvärderas och resultaten av riskanalyser jämföras med de fastställda riskkriterierna.

De analyserade riskerna ska prioriteras för riskbehandling. Bedömningar av informationssäkerhetsrisker ska genomföras med planerade intervall eller när betydande förändringar föreslås eller uppstår, med hänsyn till de kriterier som fastställs.

**B. Process för behandling av informationssäkerhetsrisker**
Ledningssystemet för informationssäkerhet ska innehålla rutiner för fastställande och tillämpning av en process för behandling av informationssäkerhetsrisker för att välja ut lämpliga alternativ för behandling av informationssäkerhetsrisker, med hänsyn tagen till resultaten av riskbedömningen samt fastställande av alla säkerhetsåtgärder som är nödvändiga för att införa valda alternativ för behandling av informationssäkerhetsrisker.

Processen ska omfatta verifikation av att inga nödvändiga säkerhetsåtgärder har utelämnats. Processen ska leda till skapandet av ett uttalande om tillämplighet som innehåller de nödvändiga säkerhetsåtgärderna och motivering för inkludering samt

om de är införda eller inte. Processen ska omfatta formulerandet av en plan för behandling av informationssäkerhetsrisker.

**C. Process för upprättande och dokumentation av informationssäkerhetsmål**
Ledningssystemet för informationssäkerhet ska innehålla rutiner för fastställande och tillämpning av en process för upprättande och dokumentation av informationssäkerhetsmål för relevanta funktioner och nivåer.

Informationssäkerhetsmålen ska vara mätbara (om det är praktiskt möjligt), beakta tillämpliga informationssäkerhetskrav och resultat från riskbedömning och riskbehandling, kommuniceras samt uppdateras vid behov.

**D. Process för lämpligheten, tillräckligheten och verkan av ledningssystem**
Ledningssystemet för informationssäkerhet ska innehålla rutiner för fastställande och tillämpning av en process för att lämpligheten, tillräckligheten och verkan av ledningssystem för informationssäkerhet ständigt förbättras. Processen ska innefatta fastställande av vilka resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra ledningssystem för informationssäkerhet samt säkerställande av att resurserna tillhandahålls.

**E. Roller, ansvar och befogenheter**
Högsta ledningen ska säkerställa att roller, ansvar och befogenheter är identifierade och kommunicerade inom organisationen.

**F. Kompetens och utbildning**
Ledningssystemet för informationssäkerhet ska säkerställa att varje person som är anställd inom organisationen och som utför uppgifter som kan orsaka sådan påverkan som organisationen identifierat som betydande, har kompetens grundad på lämplig teoretisk och praktisk utbildning eller erfarenhet. Det gäller personer som i rollen som anställd eller på organisationens uppdrag utför uppgifter åt organisationen.

**G. Lagkrav**
Ledningssystemet för informationssäkerhet ska säkerställa organisationens åtagande om att följa lagkrav inom området.

**H. Genomförande av interna revisioner**
Ledningssystemet för informationssäkerhet ska innehålla rutiner för genomförande av interna revisioner med planerade intervall för att få information om huruvida ledningssystem för informationssäkerhet överensstämmer med kraven på ledningssystem för informationssäkerhet samt att ledningssystem för informationssäkerhet har införts och underhållits på ett ändamålsenligt sätt.

#### 4.5.6.2 Kontinuitetsplan och skydd mot obehöriga

Sökande ska ha en kontinuitetsplan för sin verksamhet och it-system. Kontinuitetsplanen ska testas regelbundet. Sökande ska skydda Avropsberättigads information som hanteras och förvaras i Ramavtalsleverantörens lokaler från obehöriga samt ha rutiner för hur denna information skyddas från obehöriga.

Sökande ska ha rutiner för hur information som är säkerhetsskyddsklassificerad förvaras i sökandes lokaler så den skyddas fråntillträde av obehöriga.

Den lokal där sökande personaliserar kort ska uppfylla skyddsklass 2 enligt SSF 200, låsklass 3 enligt SS 3522 samt brandklass enligt SS/EN 1047-2, om inte annat anges i Avrop.

#### 4.5.6.3 Personalisering av kort

Sökande ska ha en organisation som kan hantera att personalisering av kort ska ske i Sverige när kortens uppgifter är säkerhetsskyddsklassificerade eller av annan orsak ska personaliseras i Sverige.

#### 4.5.6.4 Säkerhetsskyddsansvarig

Sökande ska ha en säkerhetsskyddsansvarig som ansvarar för säkerheten i Sökandes verksamhet och IT-miljö. Denne ska tillsammans med Avropsberättigad ta fram säkerhetsskyddsinstruktioner i samband med att säkerhetsskyddsavtal skrivs.

#### 4.5.6.5 Kryptering

Sökande ska ha omhändertagande rutiner och en lösning för att kravet om att fast och löstagbar lagringsmedia som lagrar uppgifter som är säkerhetsskyddsklassificerade hos Sökande ska vara krypterade.

Uppgifter som är säkerhetsskyddsklassificerade, vilka överförs via datorkommunikation utanför lokaler som kontrolleras av Sökande ska också skyddas med kryptering.

#### 4.5.6.6 Säkerhetskopiering

Sökande ska regelbundet överföra säkerhetsskyddsklassificerade uppgifter till krypterade säkerhetskopior. Säkerhetskopiorna ska förvaras avskilt och väl skyddade så att de kan återskapas efter ett fel. Sökande ska ha en rutin för test av återläsning.

#### 4.5.6.7 Behörighetskontroll

Sökandes IT-system ska ha en behörighetskontroll som styr åtkomsten till de skyddsvärda uppgifterna. Behörigheten ska begränsas till de hos Sökande som behöver uppgifterna för sitt arbete. Sökande ska ha rutiner för tilldelning och borttagande av behörigheter.

#### 4.5.6.8 Tvåfaktorsautentisering

Sökande ska kunna skydda personuppgifter med skyddad identitet, hemliga personuppgifter eller andra typer av skyddsvärda uppgifter som lagras i Sökandes IT-system mot obehörig åtkomst, med minst tvåfaktorsautentisering.

#### 4.5.6.9 Radering av information

Sökanden ska ha rutiner för att all information avseende Avropsberättigad ska kunna raderas vid avtalsslut och underlag som bekräftar detta ska återrapporteras till Avropsberättigad .

#### 4.5.6.10 Export av data i strukturerat format

Sökande ska kunna exportera all data i strukturerad form så att denna är maskinläsbar samt ändringsbar.

### 4.6.6 Personalisering av kort

Sökande ska ha en organisation som kan ta emot personuppgifter med eller utan foto för personalisering av kort från Avropsberättigad på minst följande sätt:

- skriftligen på papper via postgång eller
- personligt överlämnande på krypterat, digitalt media till exempel USB
- elektroniskt till exempel via fast, krypterad förbindelse mellan avropsberättigad och sökande

### 4.6.9 Säkerhetskoder

Sökande ska ha en organisation som kan leverera olika typer av säkerhetskoder så som PIN- och PUK-koder på ett säkert sätt via postgång och/eller med en krypterad elektronisk metod.

Samsändning av säkerhetskoder ska ske om Avropsberättigad så begär det. Sökande ska kunna ändra texten i säkerhetsbrevet i enlighet med Avropsberättigads instruktioner. Sökande ska kunna leverera upplåsningskod/PUK på begäran av Avropsberättigad.

# 4 Tekniska krav

## Informationssäkerhetskrav på upphandlingsföremålet

Inga.

# 5 Tilldelningskriterier

## Tilldelningskriterier avseende informationssäkerhet

**3.5 Tilldelningskriterier**

**3.5.1 Säkerhetsmönster i flera färger**

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

# 6 Särskilda kontraktsvillkor

## Villkor för informationssäkerhet vid fullgörande av ramavtalet

**6.1.11.5 Informationssäkerhet**
Ramavtalsleverantören ska bedriva ett systematiskt informationssäkerhetsarbete gällande den egna verksamheten som minst omfattar kraven i kvalificeringsfasen.

Ramavtalsleverantören ska på begäran av Kammarkollegiet inkomma med beskrivning som ska vara så utförlig att det tydligt framgår att punkterna i kvalificeringsfasen är uppfyllda.