Tullverket

Certifikatpolicy (CP) och utfärdardeklaration (CPS)

för

Tullverkets CA för informationsutbyte via EDI

Version 1.0

2011-05-10

Innehållsförteckning

1 Inledning
[Introduction]

1.1 Översikt
[Overview]

Dokumentet beskriver policy för *Tullverkets CA för informationsutbyte via EDI*[1] för utfärdande och hantering av signeringscertifikat. Signeringscertifikat krävs vid användning av *Tullverkets PKI-baserade säkerhetslösning*. Signeringscertifikaten, vilka inte innehåller personuppgifter, används för låsning av informationen och identifiering av avsändares organisationer vid informationsutbytet.

En certifikatpolicy (Certificate Policy, CP) innehåller krav på CA-verksamheten. För att ange hur dessa krav har tillgodoses av certifikatutfärdaren (CA) tar denne fram en utfärdardeklaration (Certification Practice Statement, CPS). Via certifikatpolicyn och utfärdardeklarationen förvissa sig de i en PKI ingående parterna om dess säkerhetsnivå.

Ofta görs implementationer av CA (Certificate Authority) av flera organisationer utifrån en och samma certifikatpolicy. Det finns då en enda certifikatpolicy men flera olika utfärdar-deklarationer. Tullverkets implementation av *Tullverkets CA för informationsutbyte via EDI* finns dock endast i en enda instans. På grund av detta har certifikatpolicy (CP) och utfärdardeklaration (CPS) kunnat slås samman till ett enda dokument.

Dokumentet är strukturerat enligt rekommendationen i IETF RFC 3647, ”Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. Rubrikerna i RFC 3647 har översatts, men finns i sin ursprungliga engelska lydelse inom parantes direkt därunder.

1.2 Dokumentnamn och identifierare
[Document name and identification]

Namn:	ca-policy-1
Version:	1.0
Datum:	2011-05-10
OID:	1.2.752.168.1.1.1

[1] EDI – Electronic Data Interchange

1.3 PKI-aktörer
[PKI participants]

1.3.1 Certifikatutfärdare
[Certification authorities (CA)]

Med certifikatutfärdare (CA) avses en av ingående parter betrodd instans som skapar, signerar och hanterar certifikat och tillhörande spärrlistor (CRL).

Certifikatutfärdare som avses i denna policy är Tullverkets CA för utgivning av signeringscertifikat för användning vid säkert informationsutbyte via EDI mellan företag och Tullverket.

1.3.2 RA (Behörig registreringsenhet)
[Registration authorities]

RA (Registration Authority) är en instans ansvarig för identifiering och autentisering av certifikatets subjekt (innehavare, ämne) på uppdrag av CA. Certifikatets subjekt anger ägaren (nyckelinnehavaren).

RA utgörs av intern grupp inom Tullverket. Denna RA mottar, identifierar och autentiserar CSR (Certificate Signing Request) från certifikatbeställande företag.

1.3.3 Nyckelinnehavare
[Subscribers]

Nyckelinnehavare kan vara Tullverket och de företag som har informationsutbyte via EDI med Tullverket. Nyckelinnehavare kan ej vara fysisk person.

1.3.4 Förlitande parter
[Relying parties]

Förlitande part kan endast vara Tullverket och de företag som har informationsutbyte via EDI med Tullverket.

1.3.5 Övriga parter
[Other participants]

Ej tillämpligt.

1.4 Certifikatanvändning
[Certificate usage]

1.4.1 Godkänd certifikatanvändning
[Appropriate certificate uses]

Certifikat utfärdade i enlighet med denna certifikatpolicy är avsedda att användas för att via den elektroniska signaturen identifiera avsändande organisation samt uppnå oavvislighet för sänd information vid informationsutbyte via EDI mellan företag och Tullverket.

1.5 Ej tillåten certifikatanvändning
[Prohibited certificate uses]

Utfärdade certifikat är endast avsedda för bruk enligt 1.4.1 ovan.

1.6 Administration av policydokument
[Policy administration]

1.6.1 Organisation som administrerar dokumentet
[Organization administering the document]

Tullverket är ansvarig för förvaltning och administration av denna certifikatpolicy.

Frågor rörande denna certifikatpolicy skickas skriftligen till:

Tullverkets IT-avdelning
EDI-certifikat
Aurorum 3
977 75 LULEÅ

1.6.2 Kontaktperson
[Contact person]

Ansvarig för CA-tjänsten kan kontaktas via ovanstående adress.

1.6.3 Person som avgör CPS lämplighet utifrån CP
[Person determining CPS suitability for the policy]

Säkerhetsansvarig för CA-tjänsten (se 5.2.1) är ansvarig för lämplighet och tillämplighet för denna CP/CPS.

1.6.4 Godkännandeprocedur för CPS

[CPS approval procedures]

Säkerhetsansvarig för CA-tjänsten ansvarar för godkännandeprocess för detta dokument.

1.7 Definitioner och förkortningar

[Definitions and acronyms]

Förkortningar

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
EORI	Economic Operator Registration and Identification
PKI	Public Key Infrastructure
RA	Registration Authority
HSM	Hardware Security Module

Definitioner

Ansökande	Den som ansöker om certifikat (och då blir nyckelinnehavare).
CA-nyckel	Nyckelpar där den privata nyckeln används av CA för att signera certifikat och där den publika nyckeln används för att verifiera samma certifikat.
CA-certifikat	Certifikat tillhörande CA. Utgörs av CA:s rotcertifikat samt certifikat tillhörande CA i certifikatkedja under rotcertifikatet. CA-certifikaten används för att signera andra certifikat.
Certification Authority (CA)	Betrodd organisation som har till uppgift att ge ut signerade certifikat. Certifikatutfärdare och utfärdare används i dokumentet som synonym till ”Certificate Authority”.
Certifikat	Med certifikatet avses här är ett elektroniskt signerat intyg att en specifik publik nyckel tillhör en specifik nyckelinnehavare. Certifikatet utformas enligt standarden X.509.
Certifikatpolicy (CP)	En namngiven uppsättning regler för framställning, utgivning och spärr av certifikat och som reglerar tillämpligheten av certifikaten inom ett specifikt användningsområde.
Certifikatutfärdare	Se Certificate Authority

Certifikatets ämnesfält	Fält i certifikatet som anger certifikatets ägare (subjekt)
Certification Practice Statement (CPS)	En dokumentation av hur en CA tillämpar en certifikatpolicy.
Förlitande part	Part som litar på uppgifter i ett certifikat för sina beslut efter att certifikatet har verifierats.
Nyckelinnehavare (eng. subscriber)	I detta sammanhang en organisation som innehar exklusiv kontroll av den privata nyckel vars publika motsvarighet certifieras i ett certifikat.
Privat nyckel	Den av nycklarna som ska skyddas i ett nyckelpar med privat och publik (öppen) krypteringsnyckel, baserad på asymmetrisk krypteringsmetod.
Publik nyckel	Den av nycklarna som ska publiceras (via ett certifikat) i ett nyckelpar med privat och publik (öppen) krypteringsnyckel, baserad på asymmetrisk krypteringsmetod.
Registration Authority (RA)	En part som av CA tilldelats uppgiften att identifiera och registrera nyckelinnehavare samt hantera olika decentraliserade procedurer relaterat till certifikatbeställning, spärr, nyckelgenerering mm.
Utfärdare	Se Certificate Authority
Utfärdarpolicy	Se Certifikatpolicy
Utfärdardeklaration	Se Certification Practice Statement (CPS)

2 Ansvar för publicering och lagring
[Publication and repository responsibilities]

2.1 Lagringsplatser
[Repositories]

Information relaterad till denna CA (Tullverkets CA för hantering av informationsutbyte via EDI) lagras internt hos Tullverket och publiceras på Tullverkets webbplats:
http://www.tullverket.se

2.2 Publicering av information relaterad till certifikat
[Publication of certification information]

Följande information relaterat till denna CA kan hämtas från Tullverkets webbplats:

- Utfärdade CA-certifikat, egensignerade rotcertifikat och eventuella korscertifikat för korscertifierade CA.
- Information om procedur för beställning av certifikat.
- Aktuell version av spärrlista (CRL).
- Aktuell och tidigare versioner av detta dokument (Certifieringspolicy (CP) inklusive utfärdardeklaration (CPS)).

2.3 Tidpunkt eller frekvens avseende publicering
[Time or frequency of publication]

Tidpunkt och frekvens avseende spärrlistor se avsnitt 4.8.7.

2.4 Behörighet för åtkomst till lagringsplatsen
[Access controls on repositories]

Ingen behörighet krävs för att hämta/läsa information enligt 2.2 ovan. Endast behörig har rätt att ändra och publicera informationen enligt 2.2.

3 Identifiering och autentisering
[Identification and authentication]

3.1 Namngivning
[Naming]

3.1.1 Typer av namn
[Types of names]

Certifikat för nyckelinnehavare

För nyckelinnehavares certifikat utgörs ämnesfält (subject) av:

countryName	Landskod	
organizationName	Organisationens namn	
organizationUnitName	Avdelning inom organisationen	*Frivilligt*
serialNumber	EORI-nummer	
commonName	Organisationens namn på kortare form	*Frivilligt*

CA-Certifikat (inklusive rotcertifikat)

För CA-certifikat utgörs ämnesfält (subject) och utgivarfält (issuer) av:

countryName	SE
organizationName	Tullverket
organizationUnitName	Kan innehålla flera OU-attribut för att närmare beskriva CA
serialNumber	EORI-nummer
commonName	Sammanfattande namn för aktuell CA (unikt inom Tullverkets CA)

3.1.2 Behov av meningsfulla namn
[Need for names to be meaningful]

Namnen i certifikatets ämnesfält (subject) skall vara meningsfull i den bemärkelse att certifikatutfärdaren kan härleda sambandet mellan dessa namn och nyckelinnehavaren.

3.1.3 Anonyma eller pseudonyma nyckelinnehavare
[Anonymity or pseudonymity of subscribers]

Signeringscertifikaten måste via korrekta namn identifiera nyckelinnehavaren, d v s anonymitet eller pseudonymer tillåts inte.

3.1.4 Regler för att tolka olika av namnformer
[Rules for interpreting various name forms]

Landskoder använda i certifikatet skall överensstämma med 2-teckens kod enligt ISO 3166-1.

3.1.5 Unika namn
[Uniqueness of names]

Möjlighet finns att samma nyckelinnehavare (organisation) kan ha flera certifikat med samma identitet i ämnesfältet (subjekt-fältet). Certifikaten kan då skiljas via certifikatserienumret (ej att förväxla med serienumret i ämnesfältet).

3.1.6 Igenkänning, autentisering och roll för varumärke
[Recognition, authentication, and role of trademarks]

Det är nyckelinnehavarens eget ansvar att se till att valet av namn i certifikatets ämnesfält (subject-fält) inte strider mot varumärke eller varumärkesrätt.

3.2 Inledande identifiering av identitet
[Initial identity validation]

3.2.1 Metod att bevisas innehavet av den privata nyckeln
[Method to prove possession of private key]

Nyckelinnehavaren genererar själv sitt nyckelpar och sänder över den publika nyckeln tillsammans med identitetsuppgifter i en CSR. Genom att CSR är signerad med nyckelinnehavarens privata nyckel kan certifikatutfärdaren vara säker på att certifikatbegäran kommer från innehavaren av den privata nyckeln.

3.2.2 Autentisering av organisationens identitet
[Authentication of organization identity]

Organisationens identitet i form av namnuppgifter i certifikatets subjekt-fält skall verifieras. Detta gäller fälten för organisationens unika namn (organizationName) och EORI-nummer (serialNumber).

Autentiseringen görs av inkommen CSR genom:

- Kontroll att CSR överensstämmer med mottagen och underskriven information på papper.

- Kontroll att organisationens namn (organizationName) i CSR stämmer med tidigare inkommen anmälan av kontaktperson (*Anmälan/avanmälan av kontaktperson för hantering av signeringscertifikat).*
- Kontroll att den kontaktperson som sänt CSR har rätt behörighet.
- Kontroll att angivet EORI-numret motsvarar angivet namn i CSR för organisationen.

3.2.3 Autentisering av individens identitet
[Authentication of individual identity]

Beställare av signeringscertifikat för organisationens (företagets) räkning skall autentiseras. Kontaktperson används här som benämningen på denna person.

I en tidigare dialog mellan företag och Tullverket har företaget gjort anmälan, underskriven av företagets firmatecknare, som pekar ut behöriga kontaktpersoner (beställare) med namn och e-postadresser.

Tullverkets RA-funktion mottar beställning av signeringscertifikat från kontaktperson i form av CSR tillsammans med på papper utskriven CSR med kontaktpersonens underskrift.

Autentisering av individens identitet vid mottagen beställning görs bland annat via:
- identifiering av kontaktpersonens identitet (beställare) via e-postadress och mottagen underskriven CSR
- autentisering av kontaktpersonens identitet via utbyte av e-post med användning av engångskoder.

3.2.4 Icke kontrollerade uppgifter om nyckelinnehavaren
[Non-verified subscriber information]

Ämnesfälten organizationUnitName (avdelning inom organisationen) och commonName (organisationens namn i kortare form) i mottagen CSR förutsätts vara korrekt och inte behöva ytterligare kontroll.

3.2.5 Validering av behörighet
[Validation of authority]

Beställare av organisations signeringscertifikat skall vara behörig.

Behörighet för kontaktperson som beställer signeringscertifikat för organisationens (företagets) räkning kontrolleras av Tullverkets RA-funktion.

3.2.6 Kriterier för samverkan
[Criteria for interoperation]

Ingen samverkan sker med andra CA.

3.3 Identifiering och autentisering vid förnyelse av nyckelpar
[Identification and authentication for re-key requests]

Ej tillämpligt. Vid behov av förnyelse av nyckelpar görs ny beställning varvid både nytt nyckelpar och nytt certifikat skapas. Identifiering och autentisering görs då enligt 3.2.

3.3.1 Identifiering och autentisering vid förnyelse av nyckelpar för giltigt certifikat
[Identification and authentication for routine re-key]

Ej tillämpligt.

3.3.2 Identifiering och autentisering vid förnyelse av nyckelpar efter att certifikatet blivit spärrat
[Identification and authentication for re-key after revocation]

Ej tillämpligt.

3.4 Identifiering och autentisering vid begäran om spärrning
[Identification and authentication for revocation request]

Nyckelinnehavaren i form av ett företag har möjlighet att begära spärrning av certifikat utfärdade för företaget genom:

- e-post
- fax
- telefon
- brev

Tullverkets RA-funktion identifierar person och företag som begär spärr och säkerställer att personen är behörig att begära spärrning av certifikat.

4 Operativa krav utifrån certifikatets livscykel

[Certificate life-cycle operational requirements]

4.1 Beställning av certifikat

[Certificate Application]

4.1.1 Vem kan beställa certifikat?

[Who can submit a certificate application?]

Utsedda kontaktpersoner (beställare) som autentiserats enligt 3.2 kan beställa certifikat för informationsutbyte via EDI med Tullverket.

4.1.2 Beställningsprocess och ansvar

[Enrollment process and responsibilities]

Tullverkets behandling av beställningen förutsätter att företaget har tillstånd eller har sökt tillstånd till någon typ av elektroniskt uppgiftslämnande till Tullverket. En kontroll görs därför av detta.

Vid beställning genererar kontaktpersonen nyckelpar, skapar CSR samt sänder CSR:en via e-post och underskrivet brev till Tullverkets RA-funktion.

4.2 Hantering av certifikatbeställning

[Certificate application processing]

4.2.1 Identifiering och autentisering

[Performing identification and authentication functions]

Identifiering och autentisering av organisation och kontaktperson (beställare) sker enligt 3.2 ovan.

4.2.2 Godkännande eller avslag på certifikatbeställning

[Approval or rejection of certificate applications]

För att Tullverkets RA-funktion ska godkänna beställningen av signeringscertifikat efter mottagande av CSR:en krävs att:

- företagets identitet har kunnat verifieras
- kontaktpersonens (beställarens) identitet har kunnat verifieras
- kontaktpersonen är behörig
- företaget är godkänt av Tullverket för någon typ av informationsutbyte via EDI.

4.2.3 Behandlingstid för certifikatbeställning
[Time to process certificate applications]

Efter verifiering av mottagen CSR och bekräftelse av beställningen från beställaren utfärdas certifikatet. Behandlingstid från att CSR:en inkommit till att certifikatet är utfärdat och levererat till företaget bör inte vara mer än 3 dagar.

4.3 Certifikatutfärdande
[Certificate issuance]

4.3.1 Aktiviteter under certifikatutfärdandet
[CA actions during certificate issuance]

Vid mottagandet av en CSR skall Tullverkets CA med stöd av RA verifiera certifikatbeställarens identitet, och behörighet samt kontrollera CSR-informationens autenticitet. Efter dessa kontroller skapar CA certifikatet.

4.3.2 Certifikatutfärdarens anmälan till den ansökande om utfärdande av certifikat
[Notification to subscriber by the CA of issuance of certificate]

Tullverkets CA skall efter genomförda aktiviteter enligt 4.3.1 informera nyckelinnehavaren om att certifikatet skapats samt göra certifikatet tillgängligt för nyckelinnehavaren.

4.4 Acceptans av certifikatet
[Certificate acceptance]

4.4.1 Handlingssätt som fastställer acceptans av certifikatet
[Conduct constituting certificate acceptance]

I och med att nyckelinnehavaren börjat använda certifikatet har denne bekräftat att uppgifterna i certifikatet är korrekta.

4.4.2 Certifikatutfärdarens publicering av certifikatet
[Publication of the certificate by the CA]

Tullverkets CA publicerar inte företagens certifikat.

4.4.3 Certifikatutfärdarens information till andra parter om utfärdade certifikat
[Notification of certificate issuance by the CA to other entities]

Tullverkets CA kommer inte att meddela andra parter om utfärdade certifikat.

4.5 Användning av nyckelpar kopplat till certifikatet
[Key pair and certificate usage]

4.5.1 Användning av privat nyckel kopplat till certifikatet
[Subscriber private key and certificate usage]

Nyckelinnehavarens privata nyckel enligt denna policy är avsedd att användas endast för att skapa elektronisk signatur och därvid uppnå oavvislighet för informationsutbytet via EDI mellan företaget och Tullverket.

4.5.2 Användning av publik nyckel kopplat till certifikatet
[Relying party public key and certificate usage]

Publik nyckel enligt denna policy är avsedd att användas vid informationsutbyte via EDI mellan företag och Tullverket för att verifiera äktheten i informationen samt identifiera nyckelinnehavaren.

4.6 Förnyelse av certifikat (ej tillämpligt)
[Certificate renewal]

Ej tillämpligt. Förnyelse av certifikat hanteras i denna CP/CPS som inledande beställning (se 4.1), där både nytt nyckelpar och nytt certifikat skapas.

4.6.1 Orsaker till förnyelse av certifikat
[Circumstance for certificate renewal]

Ej tillämpligt.

4.6.2 Vem får begära förnyelse
[Who may request renewal?]

Ej tillämpligt.

4.6.3 Hantering av begäran om förnyelse av certifikat
[Processing certificate renewal requests]

Ej tillämpligt.

4.6.4 Anmälan till den ansökande om nytt utfärdande av certifikat
[Notification of new certificate issuance to subscriber]

Ej tillämpligt.

4.6.5 Handlingssätt som fastställer acceptans av förnyat certifikat
[Conduct constituting acceptance of a renewal certificate]

Ej tillämpligt.

4.6.6 Certifikatutfärdarens publicering av det förnyade certifikatet
[Publication of the renewal certificate by the CA]

Ej tillämpligt.

4.6.7 Certifikatutfärdarens anmälan till andra parter om certifikatets utfärdande
[Notification of certificate issuance by the CA to other entities]

Ej tillämpligt.

4.7 Förnyelse av certifikatets nyckelpar (ej tillämpligt)
[Certificate re-key]

Ej tillämpligt. Förnyelse av certifikatets nyckelpar hanteras i denna CP/CPS som inledande beställning (se 4.1), där både nytt nyckelpar och nytt certifikat skapas.

4.7.1 Orsaker till förnyelse av certifikatets nycklar
[Circumstance for certificate re-key]

Ej tillämpligt.

4.7.2 Vem får begära förnyelse av certifikatets nycklar
[Who may request certification of a new public key?]

Ej tillämpligt.

4.7.3 Hantering av begäran om förnyelse av certifikatets nycklar
[Processing certificate re-keying requests]

Ej tillämpligt.

4.7.4 Anmälan till ansökanden om nytt utfärdande av certifikat
[Notification of new certificate issuance to subscriber]

Ej tillämpligt.

4.7.5 Handlingssätt som fastställer acceptans av certifikat med nya nycklar
[Conduct constituting acceptance of a re-keyed certificate]

Ej tillämpligt.

4.7.6 Utfärdarens publicering av certifikat med nya nycklar
[Publication of the re-keyed certificate by the CA]

Ej tillämpligt.

4.7.7 Certifikatutfärdarens anmälan till andra parter om utfärdandet av certifikat
[Notification of certificate issuance by the CA to other entities]

Ej tillämpligt.

4.7.8 Modifiering av certifikat (ej tillämpligt)
[Certificate modification]

Ej tillämpligt. Modifiering av certifikatet hanteras i denna CP/CPS som inledande beställning (se 4.1), där både nytt nyckelpar och nytt certifikat skapas.

4.7.9 Orsaker till modifiering av certifikat
[Circumstance for certificate modification]

Ej tillämpligt.

4.7.10 Vem får begära modifiering av certifikat?
[Who may request certificate modification?]

Ej tillämpligt.

4.7.11 Hantering av begäran om modifiering av certifikat
[Processing certificate modification requests]

Ej tillämpligt.

4.7.12 Anmälan till ansökanden om nytt utfärdande av certifikat
[Notification of new certificate issuance to subscriber]

Ej tillämpligt.

4.7.13 Handlingssätt som fastställer acceptans av modifierat certifikat
[Conduct constituting acceptance of modified certificate]

Ej tillämpligt.

4.7.14 Certifikatutfärdarens publicering av det modifierade certifikatet
[Publication of the modified certificate by the CA]

Ej tillämpligt.

4.7.15 Certifikatutfärdarens anmälan till andra parter om utfärdandet av nytt certifikat
[Notification of certificate issuance by the CA to other entities]

Ej tillämpligt.

4.8 Spärrning och suspension av certifikat
[Certificate revocation and suspension]

Tillfällig spärrning (suspension) av certifikat görs inte.

4.8.1 Orsaker till spärrning
[Circumstances for revocation]

Certifikatutfärdaren spärrar utfärdade certifikat i följande fall:

a) Nyckelinnehavaren begär spärr av sitt certifikat.

b) CA har belägg för att nyckelinnehavarens privata nyckel är röjd eller att certifikatet på annat sätt har missbrukats.

c) CA har belägg för att nyckelinnehavaren bryter mot villkor riktade till nyckelinnehavaren i Tullverkets ”*Riktlinjer och anvisningar avseende säkerhet vid informationsutbyte via EDI*”.

d) CA får kännedom om att en väsentlig förändring har gjorts av företagets orgainsationsorienterade uppgifter som gör att certifikatet inte längre är korrekt.

e) CA har väsentliga behov av att byta ut nuvarande policy till ny version

f) Tullverkets CA upphör med sin CA-verksamhet.

g) Den privata nyckel som Tullverkets CA använder vid signering av certifikat har blivit röjd.

4.8.2 Vem kan begära spärrning
[Who can request revocation]

Spärrning av certifikat kan begäras av nyckelinnehavaren eller på initiativ av certifikatutfärdaren utifrån de orsaker som angivits i 4.9.1 ovan.

4.8.3 Förfarande vid begäran om spärrning
[Procedure for revocation request]

Nyckelinnehavaren (företaget) har möjlighet att begära spärrning av certifikat utfärdade för företaget genom

- e-post
- fax
- telefon
- brev

Att spärra ett certifikat kan leda till betydande ekonomiska konsekvenser. Tullverkets RA-funktion måste därför identifiera person och företag som begär spärr och säkerställa att personen är behörig att begära spärrning av certifikatet.

4.8.4 Möjlig tidsfrist för nyckelinnehavaren innan spärrning måste göras
[Revocation request grace period]

Nyckelinnehavaren ansvarar för att begära spärr av certifikatet då denne misstänker att den privata nyckeln kopplat till certifikatet har blivit avslöjad för icke behörig.

4.8.5 Tid inom vilken certifikatutfärdaren måste bearbeta begäran om spärrning
[Time within which CA must process the revocation request]

Normalt verifieras alltid inkommen spärrbegäran mot nyckelinnehavaren (företaget) inom ett dygn, men detta förutsätter att verifieringen mot företaget kan göras inom denna tid.

4.8.6 Krav på förlitande part att kontrollera om spärrning gjorts
[Revocation checking requirement for relying parties]

Förlitande part (företaget) skall kontrollera mot aktuell spärrlista om spärrning gjorts av certifikat kopplat till den mottagna signerade informationen.

4.8.7 Utgivningsfrekvens för CRL
[CRL issuance frequency (if applicable)]

Tullverkets CA uppdaterar och publicerar ny CRL löpande innan giltighet för tidigare CRL upphört samt då ny godkänd spärrbegäran inkommit.

4.8.8 Maximal fördröjning för CRL
[Maximum latency for CRLs (if applicable)]

Normalt publiceras CRL i direkt anslutning till att den har skapats.

4.8.9 Tillgång till on-line kontroll av spärrning
[On-line revocation/status checking availability]

Tillhandahålls ej.

4.8.10 Krav på on-line kontroll av spärrning
[On-line revocation checking requirements]

Ej tillämpligt.

4.8.11 Andra tillgängliga former av tillkännagivande av spärrning
[Other forms of revocation advertisements available]

Tillhandahålls ej.

4.8.12 Speciella krav då förnyad nyckel är röjd
[Special requirements re key compromise]

Ej tillämpligt.

4.8.13 Orsaker till suspension
[Circumstances for suspension]

Ej tillämpligt.

4.8.14 Vem kan begära suspension
[Who can request suspension]

Ej tillämpligt.

4.8.15 Förfarande vid begäran om suspension
[Procedure for suspension request]

Ej tillämpligt.

4.8.16 Begränsningar för suspensionsperiod
[Limits on suspension period]

Ej tillämpligt.

4.9 Tjänster avseende certifikatstatus
[Certificate status services]

4.9.1 Operativa egenskaper
[Operational characteristics]

Tullverkets CA tillhandahåller aktuell statusinformation för certifikat i form av spärrlista (CRL).

4.9.2 Tjänstens tillgänglighet
[Service availability]

Aktuell spärrlista (CRL) kan hämtas via Internet från Tullverkets webbplats dygnet runt alla dagar i veckan med undantag från vissa kortare avbrott på grund av underhåll.

4.9.3 Tillvalsfunktioner
[Optional features]

Ej tillämpligt.

4.10 Nyckelinnehavarens abonnemang avslutas
[End of subscription]

Ej tillämpligt. Om behov inte längre finns av certifikatet ska nyckelinnehavaren spärra detta.

4.11 Nyckeldeponering och nyckelåtervinning
[Key escrow and recovery]

Ej tillämpligt. Nyckeldeponering och nyckelåtervinning stöds inte.

4.11.1 Policy och praxis för nyckeldeponering och nyckelåtervinning
[Key escrow and recovery policy and practices]

Ej tillämpligt.

4.11.2 Policy och praxis för sessionsnyckelinkapsling och återvinning
[Session key encapsulation and recovery policy and practices]

Ej tillämpligt.

5 Faciliteter, förvaltning och verksamhetsstyrning

[Facility, management and operational controls]

5.1 Fysisk säkerhet

[Physical controls]

Fysisk säkerhet syftar till att skydda CA:s lokaler, utrustning och informationskapital. Fysisk säkerhet omfattar naturkatastrofer, olyckor och fel i tekniska system samt mänskliga misstag och slarv eller kriminella handlingar. Målen med fysisk säkerhet skall vara att förhindra obehörigt fysiskt tillträde, skador och störningar i organisationens lokaler och information. Målen skall sättas i rimlig proportion till förekommande risker.

5.1.1 Fysisk placering och uppbyggnad

[Site location and construction]

CA-funktionen skall vara fysiskt placerad i skyddad datorhall.

5.1.2 Fysiskt tillträde

[Physical access]

Tillträde till CA-funktionen skall skyddas mot obehörigt tillträde.

5.1.3 Strömförsörjning och kylning

[Power and air conditioning]

Strömförsörjning och kylning skall ha tillräcklig kapacitet och tillgänglighet.

5.1.4 Vattenexponering

[Water exposures]

CA-funktionen skall vara skyddad mot vattenexponering.

5.1.5 Brandskydd

[Fire prevention and protection]

CA-funktionen skall skyddas mot brand.

5.1.6 Lagring av media

[Media storage]

Media skall förvaras på ett säkert sätt.

5.1.7 Avfallshantering
[Waste disposal]

Känsligt material skall förstöras på ett säkert sätt.

5.1.8 Säkerhetskopia på annan plats
[Off-site backup]

Säkerhetskopior skall lagras på mer än en plats.

5.2 Styrning av CA-funktion
[Procedural controls]

5.2.1 Betrodda roller
[Trusted roles]

Nedanstående roller är specifika för CA-tjänsten:

- RA-operatör (validerar och registrerar nyckelinnehavens uppgifter i CA-systemet).
- CA-operatör (genererar och levererar certifikat till nyckelinnehavaren).
- CA-administratör (genererar nya rot- och CA-certifikat)
- Säkerhetsansvarig för CA-tjänsten.
- Granskare av CA-funktionen

I Tullverkets organisation skall finnas utpekat ansvar för tillsättning av de betrodda rollerna inom CA-funktionen. Samma person kan inneha flera roller, exempelvis RA-operatör och CA-operatör. Undantag anges i 5.2.4 nedan.

5.2.2 Krav på antal personer per uppgifter
[Number of persons required per task]

CA-administratörens generering av nya rot- och CA-certifikat kräver mer än en person (se 6.2.2).

5.2.3 Identifiering och autentisering för respektive roll
[Identification and authentication for each role]

Identifiering och autentisering för respektive roll skall göras på ett säkert sätt.

5.2.4 Roller som kräver separation av uppgifter
[Roles requiring separation of duties]

Granskare kan inte vara samma person som CA-administratör, CA-operatör eller RA-operatör.

5.3 Personal
[Personnel controls]

5.3.1 Krav på kompetens, erfarenhet och formella kvalifikationer
[Qualifications, experience, and clearance requirements]

Personal som innehar roller som ur säkerhetssynpunkt betraktas som kritiska skall ha tillräcklig kompetens och erfarenhet som gör att uppgifterna kan genomföras på ett korrekt sätt. Denna typ av personal får inte ha andra uppgifter som är i konflikt med de skyldigheter och ansvar som följer av de roller de har i CA-systemet.

5.3.2 Kontroll av bakgrund
[Background check procedures]

Kontroll av anställd och inhyrd personal görs enligt Tullverkets normala rutiner.

5.3.3 Krav på utbildning
[Training requirements]

Personal som innehar roller som ur säkerhetssynpunkt betraktas som kritiska skall ha tillräcklig utbildning som gör att uppgifterna kan genomföras på ett korrekt sätt.

5.3.4 Krav på kompetensutveckling
[Retraining frequency and requirements]

Personal som innehar roller som ur säkerhetssynpunkt betraktas som kritiska, skall ges nödvändig kompetensutveckling vid förändring av system eller rutiner.

5.3.5 Arbetsrotation
[Job rotation frequency and sequence]

Ej tillämpligt.

5.3.6 Sanktioner vid obehöriga aktiviteter
[Sanctions for unauthorized actions]

Åtgärder skall vidtas vid obehöriga aktiviteter.

5.3.7 Krav på oberoende för leverantörer
[Independent contractor requirements]

Leverantörer och underleverantörer till CA-tjänsten får inte ha andra uppgifter som är i konflikt med de skyldigheter och ansvar som följer med deras uppgifter mot CA-tjänsten.

5.3.8 Dokumentation levererad till personal
[Documentation supplied to personnel]

Personal skall erhålla tillräckliga anvisningar för att korrekt kunna genomföra sina uppgifter i CA-systemet.

5.4 Loggning
[Audit logging procedures

5.4.1 Typer av händelser som registreras
[Types of events recorded]

Relevant information om genomförda transaktioner skall loggas för att erhålla spårbarhet.

5.4.2 Frekvens för analys av loggar
[Frequency of processing log]

Frekvens för analys av loggas skall göras utifrån genomförd analys enligt 5.4.8.

5.4.3 Bevaringstid för loggar
[Retention period for audit log]

Loggar enligt 5.4.1 skall bevaras utifrån tillämpliga krav för logginformationen.

5.4.4 Skydd av loggar
[Protection of audit log]

Loggar skall skyddas mot otillbörlig förändring och förlust och endast kunna läsas av behörig personal.

5.4.5 Säkerhetskopiering av loggar
[Audit log backup procedures]

Säkerhetskopiering skall göras av loggar.

5.4.6 Insamlingssystem för loggar
[Audit collection system (internal vs. external)]

Aktuella loggar samlas in till centralt loggsystem.

5.4.7 Meddelande till den som orsakat logghändelse
[Notification to event-causing subject]

Ej tillämpligt.

5.4.8 Uppskattning av sårbarhet
[Vulnerability assessments]

Minst en gång per år bör en risk och sårbarhetsanalys göras av CA-verksamheten.

5.5 Arkivering
[Records archival]

5.5.1 Typ av information som arkiveras
[Types of records archived

Nedan ges exempel på information som arkiveras:

- Utfärdade CA-certifikat (inklusive rotcertifikat) och eventuella korscertifikat för korscertifierade CA.
- Inkomna beställningar av certifikat
- Utfärdade certifikat
- Inkomna begäran om spärrning av certifikat
- Utgivna spärrlistor (CRL)
- Utgivna versioner av denna CP/CPS-dokument
- Information om procedur för beställning av certifikat.

5.5.2 Arkiveringstid
[Retention period for archive]

Arkiverad information enligt 5.5.1 skall bevaras utifrån tillämpliga krav för respektive dokument.

5.5.3 Skydd av arkiv
[Protection of archive]

Arkivinformation skall skyddas mot otillbörlig förändring och förlust och endast kunna läsas av behörig personal.

5.5.4 Säkerhetskopiering av arkiv
[Archive backup procedures]

Säkerhetskopiering skall göras av elektronisk arkivinformation.

5.5.5 Krav på tidsstämpling av arkivdokument
[Requirements for time-stamping of record]

Tidpunkt för arkivering skall registreras.

5.5.6 Insamlingssystem för arkivering
[Archive collection system (internal or external)]

Ej tillämpligt.

5.5.7 Förfarande för att erhålla och verifiera arkivdokument
[Procedures to obtain and verify archive information]

Enligt normalt förfarande för svenska myndigheter.

5.6 Övergång till ny CA-nyckel
[Key changeover]

Mot slutet av ett CA-certifikats (inklusive rotcertifikats) giltighetstid genereras nytt CA-nyckelpar samt nytt certifikat. Det nya certifikatet publiceras och efter en övergångsperiod signeras alla certifikat och CRL:er med det nya CA-certifikatet. Under övergångsperioden kan båda det gamla och det nya CA-certifikatet samtidigt vara aktiva.

5.7 Hantering vid katastrof avseende CA-verksamheten
[Compromise and disaster recover]

5.7.1 Förfarande vid allvarliga incidenter
[Incident and compromise handling procedures]

Om ett intrångsförsök eller annan form av möjlig kompromettering av en CA blir känt, skall detta utredas för att fastställa arten och graden av skada. Omfattningen av möjliga skador bedöms utifrån detta, t ex huruvida CA-certifikat behöver spärras.

5.7.2 Datorer, programvara och/eller data är skadade
[Computing resources, software, and/or data are corrupted]

Tullverkets CA skall löpande skapa säkerhetskopior av system och information som möjliggör att ett återställande av CA:s verksamhet kan göras vid skada.

5.7.3 Förfarande då CA-nyckel är röjd
[Entity private key compromise procedures]

I händelse av att en CA-nyckel har röjts ska bedömning enligt 5.7.4 göras. Om beslut har fattats om spärrning ska CA-certifikatet spärras, spärrinformationen omedelbart publiceras samt nytt CA-certifikat med nya nycklar skapas. Såväl nyckelinnehavare som förlitande parter behöver informeras. Utfärdade certifikat behöver snarast bytas ut.
Är det CA:s självsignerade rotcertifikat som har röjts, måste förlitande parters applikationer lägga in det nya rotcertifikatet.

5.7.4 Förmåga till kontinuitet efter katastrof
[Business continuity capabilities after a disaster]

Säkerhetsansvarig för CA-tjänsten (se 5.2.1) har det övergripande ansvaret att bedöma säkerhetsläget och fastställa de åtgärder som ska vidtas.

5.8 Upphörande av CA eller RA
[CA or RA termination]

Vid upphörande av Tullverkets CA skall
- förlitande parter och nyckelinnehavare informeras
- utfärdandet av certifikat upphöra
- utgivande och publicering av spärrlistor (CRL) upphöra
- utgivna certifikat spärras
- CA-nyckel inklusive eventuella kopior förstöras

Om möjligt ska förlitande parter och nyckelinnehavare informeras i god tid före upphörandet.

6 Tekniska säkerhetsåtgärder
[Technical security controls]

6.1 Generering och installation av nyckelpar
[Key pair generation and installation]

6.1.1 Generering av nyckelpar
[Key pair generation]

Nyckelinnehavare (företag) genererar själva sina nyckelpar. CA genererar endast nycklar för CA-certifikat (inklusive rotcertifikat).

Nycklarna genereras utifrån slumptal. Processen att generera slumptal, som bas för nyckelgenerering, är slumpmässig på så sätt att det är beräkningsmässigt ogörligt att återskapa ett genererat slumptal, oavsett mängden kunskap om genereringsprocessens beskaffenhet eller vid vilken tidpunkt eller med hjälp av vilken utrustning slumptalet skapades.

Nyckelgenereringsprocessen är så beskaffad att ingen information om den privata nyckeln hanteras utanför nyckelgenereringssystemet annat än genom säker överföring till avsedd plats.

6.1.2 Leverans av privat nyckel till nyckelinnehavare
[Private key delivery to subscriber]

Ej tillämpligt. Nyckelinnehavare genererar själva sina nyckelpar.

6.1.3 Leverans av publik nyckel till certifikatutfärdare
[Public key delivery to certificate issuer]

Nyckelinnehavare genererar själva sina nyckelpar och publika nyckeln levereras via CSR vid beställning av certifikat.

6.1.4 Leverans av CA:s publika nycklar till förlitande parter
[CA public key delivery to relying parties]

Förlitande part ansvarar för att hämta korrekta och gällande versioner av CA:s publika nycklar (se avsnitt 2).

6.1.5 Nyckelstorlek
[Key sizes]

För CA-certifikat (inklusive rotcertifikat) används RSA nycklar med 2048 bitars längd.

6.1.6 Parametrar för generering av publik nyckel och kvalitetskontroll
[Public key parameters generation and quality checking]

Parametrar skall väljas för att förhindra kända attacker.

6.1.7 Ändamål för nyckelanvändning (certifikatens *key usage*-fältet)
[Key usage purposes (as per X.509 v3 key usage field)]

CA-certifikaten (inklusive rotcertifikaten) skall ha nyckelanvändning med bitarna *keyCertSign* och *cRLSign* satta i certifikatets *key usage*-fält (se RFC 5280).

Enbart rotcertifikatet ska kunna skapa CA-certifikat (CA-certifikat skall ha *pathLenConstraint* satt till 0, se RFC 5280).

Nyckelinnehavarnas certifikat, vilka används för signering av meddelanden, skall ha biten *nonRepudiation* satt i certifikatets *key usage*-fält. Denna bit benämns även *contentCommitment*. Se även RFC 5280.

6.2 Skydd av CA:s privata nycklar och utformning av kryptografisk modul (HSM)
[Private Key Protection and Cryptographic Module Engineering]

6.2.1 Standard och förfarande vid användning av kryptografisk modul
[Cryptographic module standards and controls]

Ej tillämpligt. Tullverkets CA använder ingen separat HSM (Hardware Security Module).

6.2.2 Krav på flera personer för att hantera privat nyckel (n av m)
[Private key (n out of m) multi-person control]

För hantering av privata nycklar för CA:s rotcertifikat krävs två utsedda personer som hanterar varsin del av aktiveringsinformationen (se 6.4). Tillgängligheten i hanteringen kräver att dessa personer kan ersättas med bibehållen säkerhet.

6.2.3 Nyckeldeponering av privat nyckel
[Private key escrow]

Ej tillämpligt.

6.2.4 Säkerhetskopiering av privat nyckel
[Private key backup]

Säkerhetskopia skall tas av CA:s privata nycklar. Hantering av säkerhetskopian omgärdas av motsvarande regler för åtkomstskydd som gäller för originalet. Säkerhetskopian får inte arkiveras för annat syfte än att säkerställa tillgängligheten.

CA hanterar inte säkerhetskopiering av nyckelinnehavarnas privata nycklar.

6.2.5 Arkivering av privat nyckel
[Private key archival]

Ej tillämpligt.

6.2.6 Transport av privat nyckel till och från kryptografisk modul
[Private key transfer into or from a cryptographic module]

Ej tillämpligt.

6.2.7 Lagring av privat nyckel i kryptografisk modul
[Private key storage on cryptographic module]

Ej tillämpligt.

6.2.8 Metod för att aktivera den privata nyckeln
[Method of activating private key]

Aktivering av CA:s privata nycklar för rotcertifikat kräver hantering av två personer och görs endast då nya CA-certifikat ska skapas.

Tillgång till CA-nycklar för signering av nyckelinnehavares certifikat ges efter att behörig person autentiserats mot CA-systemet.

6.2.9 Metod för att deaktivera den privata nyckeln
[Method of deactivating private key]

Rotcertifikats CA-nyckel deaktiveras omedelbart efter det att CA-certifikat med nycklar har skapats.

6.2.10 Metod för att förstöra den privata nyckeln
[Method of destroying private key]

CA:s privata nycklar skall förstöras då giltighetstiden gått ur eller de blivit spärrade. Detta sker bland annat genom att aktiveringsinformation förstörs.

6.2.11 Säkerhetsvärdering av kryptografisk modul
[Cryptographic Module Rating]

Ingen formell säkerhetsvärdering görs.

6.3 Andra aspekter på hantering av nyckelpar
[Other aspects of key pair management]

6.3.1 Arkivering av publik nyckel
[Public key archival]

CA:s publika nyckel arkiveras.

6.3.2 Giltighetsperioder för certifikat och nyckelpar
[Certificate operational periods and key pair usage periods]

CA:s rotcertifikat utfärdas med giltighetsperiod på 20 år.
Övriga CA-certifikat utfärdas med giltighetsperiod på 10 år.
Nyckelinnehavarnas certifikat utfärdas med giltighetsperiod på 14 månader.

6.4 Aktiveringsinformation
[Activation data]

6.4.1 Generering och installation av aktiveringsinformation
[Activation data generation and installation]

Information för aktivering av CA:s rotnycklar skapas via två separata delar.

6.4.2 Skydd av aktiveringsdata
[Activation data protection]

Aktiveringsinformation för CA:s rotnycklar skall skyddas mot stöld, brand etc. genom förvaring i säkerhetsskåp med två exemplar i separata lokaler. En person får inte ha tillgång till båda delarna av aktiveringsinformationen.

6.4.3 Övriga aspekter på aktiveringsinformation
[Other aspects of activation data]

Ej tillämpligt.

6.5 Styrning av IT-säkerhet
[Computer security controls]

6.5.1 Särskilda IT-säkerhetstekniska krav
[Specific computer security technical requirements]

För hantering av CA-systemet krävs hög säkerhetsnivå. Speciellt gäller att privata nycklar för CA:s rotcertifikat lagras säkert i separat väl skyddad datormiljö.

6.5.2 Värdering av IT-säkerheten
[Computer security rating]

Inga formella krav ställs på värdering av IT-säkerheten.

6.6 Livscykeltekniska krav
[Life cycle technical controls]

6.6.1 Säkerhetskrav avseende systemutveckling
[System development controls]

Ändringar som görs i CA-systemet skall testas i separat utvecklingsmiljö innan de tas i drift.

6.6.2 Säkerhetskrav avseende säkerhetsadministration
[Security management controls]

Konfigurering och modifiering av CA-systemet skall dokumenteras.
Säkerhetsadministrationen skall endast kunna göras av person som tilldelats roll för att hantera detta, se 5.2 ovan.

6.6.3 Säkerhetskrav avseende livscykel
[Life cycle security controls]

Ej tillämpligt.

6.7 Säkerhetskrav avseende nätverk

[Network security controls]

Känslig information såsom privata nycklar, aktiveringsinformation får inte sändas i klartext via nätverket.

6.8 Tidsstämpling

[Time-stamping]

CA-systemet skall ges tillgång till korrekt tid som uppfyller verksamhetens behov för att skapa certifikat, spärrlistor och loggar.

7 Certifikat, CRL och OCSP profiler

[Certificate, CRL and OCSP profiles]

7.1 Certifikatprofil

[Certificate profile]

Grundläggande certifikatfält

Fältnamn	Kommentar
Version	X.509 version 3 (värde = 2)
Serial Number	Unikt nummer för varje certifikat utgivet av en viss CA (Issuer)
Signature Algorithm	sha1WithRSAEncryption (se även 7.1.3)
Issuer	Se 3.1.1
validity, notBefore	Se RFC 5280
validity, notAfter	Se RFC 5280
subject	Se 3.1.1
subjectPublicKeyInfo	Signaturalgoritm samt publik nyckel kodad enligt RFC 5280

7.1.1 Versionsnummer

[Version number(s)]

Versionsnummer för certifikat är X.509 version 3.

7.1.2 Certifikatutökningar

[Certificate extensions]

Certifikatutökningar för CA-certifikat (inklusive rotcertifikat)

Fältnamn	Critical	Kommentar
authorityKeyIdentifier	non-critical	Se RFC 5280
subjectKeyIdentifier	non-critical	Se RFC 5280
keyUsage	critical	Följande bitar ska vara satta: *keyCertSign* *cRLSign*
certificatePolicies	non-critical	Pekar ut aktuell certifikatpolicy via OID.
basicConstraints	critical	Är uppdelat i två delfält. Fält 1 = TRUE (anger att det är ett CA-certifikat) Fält 2 = Ej satt för rotcertifikat. 0 För övriga CA-certifikat

Certifikatutökningar för nyckelinnehavares certifikat

Fältnamn	Critical	Kommentar
authorityKeyIdentifier	non-critical	Se RFC 5280
subjectKeyIdentifier	non-critical	Se RFC 5280
keyUsage	critical	Följande bit ska vara satt: *nonRepudiation*
certificatePolicies	non-critical	Pekar ut aktuell certifikatpolicy via OID.
basicConstraints	critical	Är uppdelat i två delfält. Fält 1 = FALSE Fält 2 (Ej tillämpligt)
cRLDistributionPoints	non-critical	Detta fält innehåller uppgift om var CRL finns att hämta.

7.1.3 Objektidentifierare för algoritmer
[Algorithm object identifiers]

För att signera certifikatet används:
sha1WithRSAEncryption
{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5)}

7.1.4 Namnformat
[Name forms]

Se 3.1.1.

7.1.5 Certifikatfältet ”Name constraints”
[Name constraints]

Certifikatfältet *Name constraints* används ej.

7.1.6 Objektidentifierare för certifikatpolicy
[Certificate policy object identifier]

I certifikatfältet *certificatePolicies* lagras objektidentifierare för denna certifikatpolicy (se avsnitt 1.2).

7.1.7 Användning av certifikatutökning ”Policy Constraints”
[Usage of Policy Constraints extension]

Certifikatfältet *Policy Constraints* används ej.

7.1.8 Syntax och semantik för policykvalificerare
[Policy qualifiers syntax and semantics]

Ej tillämpligt.

7.1.9 Bearbetning av semantik för kritiska certifikatpolicyutökningar
[Processing semantics for the critical Certificate Policies extension]

Ej tillämpligt.

7.2 CRL profil
[CRL profile]

Fältnamn	Kommentar
Version	Se 7.2.1
Signature Algorithm	Objektidentifierare för SHA 1 RSA (se 7.1.3)
Issuer	Se 3.1.1
thisUpdate	Tidpunkt då denna CRL utfärdades
nextUpdate	Senaste tidpunkt för utfärdande av nästa CRL
Authority Key Identifier	Se 7.2.2
CRL Number	Se 7.2.2
RevokedCertificates	Lista över spärrade certifikat med följande delfält per spärrat certifikat: • userCertificate – Innehållande certifikatets serienummer • revocationDate – Innehållande tidpunkt för spärrning av certifikatet • ReasonCode – Se 7.2.2

7.2.1 Versionsnummer
[Version number(s)]

Skall vara X.509 version 2 CRL.

7.2.2 CRL- and CRL-post utökningar
[CRL and CRL entry extensions]

Authority Key Identifier	För att identifiera publika nyckeln som signerat CRL:en. Speciellt behov om man använder flera nycklar att signera med.
CRL Number	Löpande numrering av utgivna CRL
Reason Code	Orsak till spärr (en kod per certifikatpost)

7.3 OCSP profil
[OCSP profile]

Ej tillämpligt.

7.3.1 Versionsnummer
[Version number(s)]

Ej tillämpligt.

7.3.2 OCSP utökningar
[OCSP extensions]

Ej tillämpligt.

8 Överensstämmelse utifrån revision och andra granskningar

[Compliance audit and other assessments]

8.1 Frekvens och omständigheter för granskning

[Frequency or circumstances of assessment]

Säkerhetsansvarig för CA-tjänsten (se 5.2.1) avgör frekvens och omständigheter för granskning av CP/CPS.

8.2 Identitet/kvalifikationer för granskare

[Identity/qualifications of assessor]

Säkerhetsansvarig för CA-tjänsten utser granskare.

8.3 Granskares relationer till bedömd enhet

[Assessor's relationship to assessed entity]

Se avsnitt 5.2.

8.4 Områden som täcks av granskning

[Topics covered by assessment]

Granskning avser att hanteringen i Tullverkets CA för informationsutbyte via EDI överensstämmelse med denna CP/CPS.

8.5 Åtgärder som vidtas till följd av upptäckt brist

[Actions taken as a result of deficiency]

Utifrån sammanställning av eventuella brister sker en planering av åtgärder under ledning av Säkerhetsansvarig för CA-tjänsten.

8.6 Kommunikation av resultat

[Communication of results]

Sammanställning och åtgärder enligt 8.5 publiceras inte.

9 Andra affärsmässiga och juridiska frågor

[Other business and legal matters]

9.1 Avgifter

[Fees]

Ej tillämpligt.

9.1.1 Avgifter för certifikatutfärdande

[Certificate issuance or renewal fees]

Ej tillämpligt.

9.1.2 Avgifter för åtkomst till certifikat

[Certificate access fees]

Ej tillämpligt.

9.1.3 Avgifter för åtkomst till spärrinformation

[Revocation or status information access fees]

Ej tillämpligt.

9.1.4 Avgifter för andra tjänster

[Fees for other services]

Ej tillämpligt.

9.1.5 Återbetalningspolicy

[Refund policy]

Ej tillämpligt.

9.2 Finansiellt ansvar

[Financial responsibility]

Ej tillämpligt.

9.2.1 Försäkringsskydd
[Insurance coverage]

Ej tillämpligt.

9.2.2 Övriga tillgångar
[Other assets]

Ej tillämpligt.

9.2.3 Försäkringar och garantier för slutanvändare
[Insurance or warranty coverage for end-entities]

Ej tillämpligt.

9.3 Sekretess för affärsinformation
[Confidentiality of business information]

Ej tillämpligt. Regleras inte i detta dokument

9.3.1 Omfattning för sekretessbelagd information
[Scope of confidential information]

Ej tillämpligt.

9.3.2 Information som inte är sekretessbelagd
[Information not within the scope of confidential information]

Ej tillämpligt.

9.3.3 Ansvar för att skydda sekretessbelagd information
[Responsibility to protect confidential information]

Ej tillämpligt.

9.4 Sekretess för personlig information
[Privacy of personal information]

Ej tillämpligt. Regleras inte i detta dokument.

9.4.1 Sekretessplan
[Privacy plan]

Ej tillämpligt.

9.4.2 Informations som behandlas som privat
[Information treated as private]

Ej tillämpligt.

9.4.3 Information som inte bedöms som privat
[Information not deemed private]

Ej tillämpligt.

9.4.4 Ansvar att skydda privat information
[Responsibility to protect private information]

Ej tillämpligt.

9.4.5 Anmälan och samtycke att använda privat information
[Notice and consent to use private information]

Ej tillämpligt.

9.4.6 Utlämning i enlighet med juridiska och administrativa processer
[Disclosure pursuant to judicial or administrative process]

Ej tillämpligt.

9.4.7 Övriga omständigheter avseende utlämning av information
[Other information disclosure circumstances]

Ej tillämpligt.

9.5 Immateriella rättigheter
[Intellectual property rights]

Vid spridning av denna policy får ingen information förändras, tas bort, eller läggas till. Det ska tydligt anges att Tullverket är utfärdare av detta policydokument.

9.6 Förpliktelser och garantier
[Representations and warranties]

9.6.1 CA:s förpliktelser och garantier
[CA representations and warranties]

CA skall tillhandahålla CA-tjänster enligt denna CA/CPS.

9.6.2 RA:s förpliktelser och garantier
[RA representations and warranties]

RA skall tillhandahålla RA-tjänster för identifiering och registrering enligt denna CA/CPS.

9.6.3 Nyckelinnehavares förpliktelser och garantier
[Subscriber representations and warranties]

Nycklar skall genereras med god kvalitet och skyddas mot spridning och obehörig användning. För varje ny CSR som skickas till Tullverket skall ett nytt nyckelpar genereras.

9.6.4 Förlitande parts förpliktelser och garantier
[Relying party representations and warranties]

Vid kontroll av signaturer skall certifikatets giltighet kontrolleras. Detta innefattar även kontroll mot spärrlista.

9.6.5 Förpliktelser och garantier avseende andra deltagare
[Representations and warranties of other participants]

Ej tillämpligt.

9.7 Friskrivningar avseende garantier
[Disclaimers of warranties]

Tullverkets CA tar inget ansvar för otillåten användning av certifikat (se 1.4.2).

9.8 Ansvarsbegränsningar
[Limitations of liability]

Tullverkets CA tar inget ansvar för otillåten användning av certifikat (se 1.4.2).

9.9 Ersättningar
[Indemnities]

Ej tillämpligt.

9.10 Giltighetsperiod för denna CP/CPS
[Term and termination]

9.10.1 Period startar
[Term]

Denna CP/CPS börjar gälla utifrån angiven starttidpunkt i samband med publicering av Tullverket.

9.10.2 Period upphör
[Termination]

Denna CP/CPS gäller tills den ersätts av ny version eller tills CA upphör med sin verksamhet.

9.10.3 Fortsatt giltighet efter upphörande
[Effect of termination and survival]

CP/CPS gäller i tillämpliga delar efter uppsägning.

9.11 Kommunikation med ingående parter angående CA-tjänsten
[Individual notices and communications with participants]

Tullens CA kan komma att lämna viss typ av information om CA-tjänsten via e-post eller Tullverkets webbplats när detta inte strider mot bestämmelser i denna CP/CPS.

9.12 Ändringar av denna CP/CPS

[Amendments]

9.12.1 Förfarande för ändring

[Procedure for amendment]

Synpunkter beträffande denna policy kan lämnas till Tullverkets CA via brev med adress enligt avsnitt 1.5.

Beslut om att genomföra ändringar i CP/CPS som kräver ny OID (se 9.12.3) tas av Säkerhetsansvarig för CA-tjänsten (se 5.2.1).

9.12.2 Meddelande om ändring och drifttagande

[Notification mechanism and period]

Publicering av ny version av CP/CPS skall ske innan den tas i drift. Publiceringen skall även innehålla uppgifter om vad som ändrats.

9.12.3 Omständigheter under vilka OID måste ändras

[Circumstances under which OID must be changed]

Små förändringar av CP/CPS som inte påverkar innebörden av CP/CPS kan göras utan att OID behöver ändras.

9.13 Hantering vid tvist

[Dispute resolution provisions]

Tvist i anledning av denna certifikatpolicy skall slutligt avgöras i svensk domstol.

9.14 Tillämplig lag

[Governing law]

Vid tolkning av denna certifikatpolicy och vid bedömning av CA:s agerande i samband med utfärdande av certifikat enligt denna certifikatpolicy skall svensk lag tillämpas.

9.15 Överensstämmelse med gällande lag

[Compliance with applicable law]

Hantering av CA-systemet sker i överensstämmelse med svensk lag.

9.16 Övriga förpliktelser
[Miscellaneous provisions]

Ej tillämpligt.

9.16.1 Hela avtalet
[Entire agreement]

Ej tillämpligt.

9.16.2 Överlåtelse
[Assignment]

Ej tillämpligt.

9.16.3 Bestämmelsers ogiltighet
[Severability]

Skulle någon bestämmelse eller del därav i denna policy befinnas vara ogiltig, ska detta inte innebära att policyn i dess helhet är ogiltig.

9.16.4 Verkställighet (advokatkostnader och avstående av rättigheter)
[Enforcement (attorneys' fees and waiver of rights)]

Ej tillämpligt.

9.16.5 Force Majeure
[Force Majeure]

Ej tillämpligt.

9.17 Övriga bestämmelser
[Other provisions]

Ej tillämpligt.

Box 12854, 112 98 Stockholm
Telefon: 0771-520 520
tullverket.se