CERTIFIKATPOLICY
SJÖFARTSVERKET

KUNDCERTIFIKAT

VERSION 1

CERTIFIKATPOLICY
SJÖFARTSVERKET

KUNDCERTIFIKAT

VERSION 1

Datum: 2006-12-06

SJÖFARTSVERKET

601 78 Norrköping
Tel: 011-19 10 00
Fax: 011-10 19 49

DEFINITIONER

Autentisering	Verifiering av uppgiven identitet eller av ett meddelandes riktighet.
CA-miljö	CA-miljö omfattar CA-system med kringutrustning, inkluderande både hårdvara och mjukvara.
CA-policy	Se Certifikatpolicy.
CA-system	Det isolerade systemet där Utfärdarens privata nyckel lagras
Certificate Revocation List(CRL)	Periodiskt uppdaterad, tidstämplad och signerad lista, utgiven av Utfärdaren, vilken anger certifikat som återkallats innan deras giltighetstid gått ut
Certification Authority (CA)	Se Certifikatutfärdare.
Certification Practice Statement (CPS)/ (utfärdardeklaration)	Beskrivning, framtagen av Utfärdaren, av de regler och kontroller Utfärdaren tillämpar i avsikt att uppfylla kraven i en Certifikatpolicy.
Certifikat	Ett elektroniskt, av CA-systemet, signerat intyg av en publik nyckels tillhörighet till en specifik nyckelinnehavare.
Certifikatkedja	Ordnad sekvens av (kors-) certifikat som med hjälp av en rotnyckel för det första certifikatet medger att det sista (användar-) certifikatet kan verifieras.
Certifikatpolicy (CP)	Regelverk som Utfärdaren skall tillämpa vid utfärdande av certifikat.
Certifikatutfärdare	Betrodd instans som har till uppgift att skapa och utge användarcertifikat eller andra typer av certifikat.
Digital signatur	Digital motsvarighet till traditionell underskrift. Den digitala signaturen skapas genom att signatären signerar digital information med sin privata nyckel enligt en speciell procedur. Den digitala signaturen kan användas dels för att spåra vem som signerat informationen och dels för att verifiera att informationen inte förändrats sedan den signerades.

Elektronisk identifiering	Att en användare kan identifiera sig elektroniskt, dvs. användning av till exempel certifikat som innehåller uppgifter som gör att innehavaren kan identifiera sig elektroniskt.
Förlitande Part	Part som litar på uppgifter i ett certifikat för sina beslut.
Identifiering	Process där en användare eller resurs anger sin identitet på ett sätt som är möjligt att verifiera.
Integritetsskydd	Skydd mot att information obehörigen eller oavsiktligt modifieras utan att det kan upptäckas.
Korscertifikat	Certifikat utfärdat av en certifikatutfärdare, som associerar en annan certifikatutfärdare med dennes publika nyckel.
Kryptering	Omvandling av klartext till kryptotext med hjälp av ett krypteringssystem och aktuell kryptonyckel i syfte att förhindra obehörig åtkomst av konfidentiell information.
Kundcertifikat	Certifikat som utfärdas till person inom kundens organisation
Logg	(Kontinuerligt) insamlad information om de operationer som utförs i ett system.
Nyckelgenerering	Den process under vilken publika och privata nycklar skapas.
Oavvislighet	Princip med innebörden att utförande av en specifik handling inte i efterhand skall kunna förnekas av utföraren.
Objektidentifierare (OID)	En typ inom standarden för ASN.1 (Abstract Syntax Notation One), SS-ISO 8824 (§ 26), som tillhandahåller en mekanism lämpad för tilldelning av unika namn på objekt, t.ex. denna policy.
Personalisering	Processen att förse kundcertifikat med logisk information som erfordras för att knyta användaren till ett specifikt kundcertifikat.

Privat nyckel	1) Hemlighållen nyckel (dekrypteringsnyckel) i ett asymmetriskt kryptosystem, 2) Hemlighållen nyckel som främst används vid generering av digitala signaturer samt för dekryptering av krypterad information.
Publik nyckel	1) Nyckel som kan göras känd och som används vid kryptering i ett asymmetriskt kryptosystem, 2) Nyckel som kan göras känd och som används vid verifiering av digitala signaturer.
Registration Authority (RA)	Instans som är betrodd att svara för registrering och autentisering av användare och deras personuppgifter så att de kan tilldelas korrekta certifikat.
Revokeringslista	Se Certificate Revocation List.
Signera	Förse ett meddelande eller en datamängd med en digital signatur.
Smarta kort	Ett plastkort med chip. Kortet är vanligen av kreditkortsstorlek.
Spärrlista	Se Certificate Revocation List.
Sökanden	Individ som ansöker om Certifikat, eller av företaget utsedd person att företräda individen.
Utfärdarcertifikat	Certifikat som intygar att en viss publik nyckel är publik nyckel för en specifik CA.
Utfärdardeklaration	Se Certificate Practice Statement
Utfärdare	Se Certifikatutfärdare.
Verifiering	Processen att kontrollera att ett antagande är korrekt. Detta begrepp avser främst processen att kontrollera att en signatur är framställd av den som signerade informationen.

DOKUMENTSTRUKTUR OCH TOLKNINGAR

Nedan anges vilken grundstruktur som används för detta dokument samt riktlinjer för tolkning av detta dokument:

Rubriker och underrubriker i detta dokument är utformade för att till stor del överensstämma med internationell praxis. Vid tolkning av detta dokument skall texten under rubriken ges företräde före texten i rubriken

Som en generell regel gäller att ”Utfärdaren”, vilken lyder under denna policy, skall vidta nödvändiga åtgärder och steg för att säkerställa att man efterlever de krav som anges i denna Certifikatpolicy.

Dokumentet förses med en objektidentifierare (OID) som kan införas i certifikaten under "Certificate policy extensions" i enlighet med X.509 version 3.

Strukturen i denna Certifikatpolicy följer tillämpbara delar av RFC 2527, men i förenklad form förhållande till denna. Innehållet och utformning har anpassats till att endast omfatta det som Utfärdaren anser vara nödvändigt för att åtnjuta förlitande parts förtroende.

SEIS Certificate policy SEIS – S10, har varit utgångspunkten vid framtagandet av denna Policy och tillhörande utfärdardeklaration (CPS).

Innehållsförteckning

1 INTRODUKTION 1

1.1 ALLMÄNT 1
1.2 IDENTIFIERING 1
1.3 MÅLGRUPP OCH TILLÄMPLIGHET 1
1.3.1 Utfärdare 1
1.3.2 Registration authorities (RA) 2
1.3.3 Kundcertifikat 2
1.3.4 Tillämplighet 2
1.4 KONTAKTUPPGIFTER 2
1.4.1 Administrationsansvarig 2
1.4.2 Kontaktperson 2
1.4.3 Överensstämmelse mellan denna policy och utfärdardeklaration (CPS) 3

2 ALLMÄNNA BESTÄMMELSER 3

2.1 ÅTAGANDEN 3
2.1.1 Utfärdarens åtaganden 3
2.1.2 RA:S åtaganden 4
2.1.3 Kundcertifikatsinnehavarens åtaganden 4
2.1.4 Förlitande parts åtaganden 5
2.2 ANSVAR 5
2.2.1 Utfärdarens ansvar 5
2.2.2 Ansvar för RA 6
2.3 FINANSIELLT ANSVAR 6
2.3.1 Fullmaktsförhållanden 6
2.4 TOLKNING OCH GENOMFÖRANDE 6
2.4.1 Tillämplig lag 6
2.4.2 Tvistelösning 6
2.5 AVGIFTER 6
2.6 PUBLICERING OCH ÅTKOMST AV INFORMATION 6
2.6.1 Publicering av information 6
2.6.2 Periodicitet för publicering 7
2.6.3 Behörighetskontroll 7
2.7 GRANSKNING 7
2.7.1 Utföranden 7
2.7.2 Information om resultatet av granskning 7
2.8 KONFIDENTIALITET 7
2.8.1 Typ av information som skall hållas konfidentiell 7
2.8.2 Typ av information som inte anses vara konfidentiell 8
2.8.3 Tillhandahållande av information om anledning till spärrning av kundcertifikat 8
2.8.4 Tillhandahållande av konfidentiell information till polis, åklagare eller annan 8
2.9 IMMATERIELLA RÄTTIGHETER 8
2.10 AVTALSVILLKOR FÖR KUNDCERTIFIKATS-INNEHAVARE 8
2.11 TILLGÄNGLIGHET OCH SVARSTID 9

3 IDENTIFIERING OCH AUTENTISERING 9

3.1 INITIAL REGISTRERING 9
3.1.1 Typer av namn 9
3.1.2 Namnsättning 9
3.1.3 Fastställande av sökandens identitet 10
3.2 FÖRNYELSE AV NYCKLAR OCH CERTIFIKAT 10
3.2.1 Förnyelse av nycklar och certifikat 10
3.3 BEGÄRAN OM SPÄRRNING 10

4 OPERATIONELLA KRAV 10

4.1 ANSÖKAN OM KUNDCERTIFIKAT 10
4.2 UTFÄRDANDE AV KUNDCERTIFIKAT 11
4.3 UTLÄMNADE AV KUNDCERTIFIKAT 11
4.4 SPÄRRNING AV KUNDCERTIFIKAT 11
4.4.1 Anledning till spärrning 12
4.4.2 Behörig att begära spärrning 12
4.4.3 Rutin för begäran om spärrning 12
4.4.4 Behandlingstid vid begäran om spärrning 12
4.4.5 Öppettid för spärrtjänsten 13
4.4.6 Periodicitet för utgivning av spärrlista 13
4.4.7 Krav på spärrkontroll 13
4.5 LOGGNING 13
4.5.1 Händelser som loggas 13
4.5.2 Kontroll av loggar 14
4.5.3 Skydd av loggar 14
4.6 ARKIVERING 14
4.6.1 Information som arkiveras 14
4.6.2 Lagringstid 14
4.6.3 Skydd av arkiv 15
4.6.4 Rutiner för åtkomst och verifiering av arkivmaterial 15
4.7 BYTE AV UTFÄRDARNYCKEL 15
4.8 KATASTROFPLAN VID MISSTANKE OM RÖJDA UTFÄRDARNYCKLAR 15
4.9 UPPHÖRANDE AV UTFÄRDARENS VERKSAMHET 16

5 SÄKERHETSKONTROLLER 16

5.1 FYSISK SÄKERHET 16
5.2 PROCEDURORIENTERAD SÄKERHET 17
5.2.1 Betrodda roller inom ca-funktionen 17
5.2.2 Krav på antal personer per uppgift 18
5.2.3 Identifiering och autentisering av personer i betrodda roller 18
5.3 PERSONORIENTERAD SÄKERHET 18
5.3.1 Bakgrund och kvalifikationer 18
5.3.2 Krav på utbildning 18
5.3.3 Personorienterad säkerhet för RA 18

6 TEKNISK SÄKERHET 19

6.1 GENERERING OCH INSTALLATION AV NYCKELPAR 19
6.1.1 Generering av nyckelpar 19
6.1.2 Leverans av kundcertifikat 19
6.1.3 Nyckelstorlek 20
6.1.4 Generering av publik nyckel 20
6.2 SKYDD AV PRIVATA NYCKLAR 20
6.2.1 Säkerhetsmodul och kundcertifikat 20
6.2.2 Flerpersonskontroll av privata nycklar 20
6.2.3 Säkerhetskopiering av privata nycklar 21
6.2.4 Arkivering av privata nycklar 21
6.2.5 Lagring av kundcertifikatens privata nyckel 21
6.2.6 Aktivering av privata nycklar i kundcertifikaten 21
6.2.7 Förstörelse av utfärdarens privata nycklar 21
6.3 ANDRA ASPEKTER PÅ NYCKELHANTERING 22
6.3.1 Arkivering av publika nycklar 22
6.3.2 Privata nycklars livslängd 22
6.3.3 Certifikatens giltighetstid 22
6.4 AKTIVERINGSDATA 22
6.4.1 Generering och installation av aktiveringsdata 22
6.4.2 Skydd av aktiveringsdata 22
6.5 SÄKERHET I DATORSYSTEM 22
6.5.1 Tekniska krav 23

6.6 KONTROLL AV SÄKERHET HOS SYSTEMET UNDER LIVSCYKELN 23
6.6.1 Kontroller av systemutveckling 23
6.6.2 Kontroller av säkerhetsadministration 23
6.7 KONTROLL AV NÄTVERKSSÄKERHET 23

7 PROFILER FÖR CERTIFIKAT OCH SPÄRRLISTOR 23

7.1 CERTIFIKATENS PROFIL OCH VERSION 23
7.2 PROFIL FÖR SPÄRRLISTA 24

8 FÖRVALTNING AV POLICYN 24

8.1 FÖRÄNDRING AV POLICYN 24
8.1.1 Förändringar som kan ske utan underrättelse 24
8.1.2 Förändringar som kan ske med underrättelse 24
8.2 PUBLICERING OCH DISTRIBUTION AV POLICY OCH UTFÄRDARDEKLARATION (CPS) 24
8.2.1 Publicering och distribution av policy 24

1 INTRODUKTION

1.1 ALLMÄNT

Detta dokument ägs och förvaltas av Sjöfartsverket, nedan kallad Utfärdaren. Dokumentet utgör en Certifikatpolicy för utfärdande av filbaserade kundcertifikat för sjöfartsverkets kunder, nedan endast kallad policy.

Denna policy beskriver rutiner och säkerhetskrav vid utfärdande och användning av kundcertifikat.

Dokumentet har försetts med namn och objektidentifierare (OID). (Se avsnitt 1.2.)

I de fall relationen mellan Utfärdare, RA, certifikatsinnehavare, och Förlitande Part bygger på ett avtal, skall hänvisning till denna policy anges. Policyn skall, oberoende av om avtal upprättas eller inte, användas av en Förlitande Part för att bedöma om ett certifikat är tillförlitligt.

Denna policy ger möjlighet att utfärda följande kundcertifikat.

- Filbaserat kundcertifikat

Utfärdande av kundcertifikat i enlighet med denna policy innebär att:

- Kundcertifikatet ställs ut till en person inom en organisation.
- utfärdade kundcertifikat följer den internationella versionen av PKCS#12-standarden
- utfärdade kundcertifikat lagras på fil skyddad av ett lösenord, för distribution och lagring lokalt på innehavarens lagringsmedia.

1.2 IDENTIFIERING

Namn på policyn: Certifikatpolicy Sjöfartsverket kundcertifikat v1

Objektidentifierare: 1.2.752.150.1.1

OID införs i skapade kundcertifikat som "Certificate Policy Extension" enligt X.509 version 3

1.3 MÅLGRUPP OCH TILLÄMPLIGHET

Detta kapitel anger vilka som berörs av policyn samt dess tillämpningsområde.

1.3.1 Utfärdare

Ansvarig utfärdare för denna policy är Sjöfartsverket, nedan kallad Utfärdaren.

Utfärdaren skall upprätta och publikt publicera en utfärdardeklaration (CPS), som beskriver den praktiska implementeringen av denna policy.

1.3.2 Registration authorities (RA)

Registration Authority utses av Utfärdaren och skall arbeta i enlighet med denna policy, och avtal upprättade med Utfärdaren.

Avtal behöver endast upprättas om en extern leverantör anlitas som RA

1.3.3 Kundcertifikat

Kundcertifikat är ett elektroniskt mjukvarubaserat certifikat för identifiering, kryptering och signering av elektroniska transaktioner. Kundcertifikatet är utfärdat till en person inom en organisation med en giltighetstid på 2 år.

En förutsättning för att kunna ge ut den denna typ av Certifikat är att organisationen har ett registreringsnummer eller VAT-nummer.

1.3.4 Tillämplighet

Denna policy är relevant för Utfärdaren, RA, Kundcertifikatsinnehavare, samt för Förlitande Part.

Det är Förlitande Part eller dennes organisation som avgör för vilka ändamål de utställda kundcertifikaten kan godtas.

1.3.4.1 Lämpliga användningsområden

Kundcertifikat utställda enligt denna policy används normalt för att säkerställa äkthet och trovärdigheten för vissa dokument/system/tjänster.

Primärt kommer Sjöfartsverkets kundcertifikat att användas för:

- Legitimering (Autenticering), vid tillträde och uppgiftslämnande till Sjöfartsverkets e-tjänster
- Elektronisk underskrift
- Insynsskydd (kryptering) för kommunikation

Denna policy anger inte skydd för bedrägeri, eller annat oönskat nyttjande av kundcertifikat.

1.4 KONTAKTUPPGIFTER

1.4.1 Administrationsansvarig

Policyn är registrerad av Sjöfartsverket (Utfärdaren). Utfärdaren är fullt ansvarig för att administrera och uppdatera denna policy.

1.4.2 Kontaktperson

Frågor angående policyn adresseras till:

Sjöfartsverket

Torbjörn Mellblom

SE 601 78 Norrköping

Sweden

Telefon: +46 11 19 14 68

E-post: Torbjorn.mellblom@sjofartsverket.se

1.4.3 Överensstämmelse mellan denna policy och utfärdardeklaration (CPS)

Utfärdaren är ansvarig för granskning av policyn enligt 2.7.

2 ALLMÄNNA BESTÄMMELSER

Detta kapitel redogör bestämmelserna för Utfärdaren, RA kundcertifikatsinnehavare, och Förlitande Parts åtaganden.

2.1 ÅTAGANDEN

En och samma juridiska person, nedan kallad Utfärdaren, är ansvarig som Certifikatutfärdare (CA). Om någon eller några delar av utgivarprocessen utförs av en eller flera underleverantörer är Utfärdaren ansvarig för dessa åtgärder som om han hade utfört dem själv. Det åligger Utfärdaren att tillse att underleverantörer följer denna policy i tillämpliga delar.

2.1.1 Utfärdarens åtaganden

2.1.1.1 Allmänna bestämmelser

Utfärdaren åtar sig enligt denna policy att:

a) utfärda kundcertifikat i enlighet med policy

b) tillhandahålla kontrollåtgärder enligt kapitel 4 till och med 6

c) upprätta och publicera en utfärdardeklaration (CPS)

d) spärra certifikat och tillhandahålla spärrtjänst enligt 4.4.

e) Tillföra tillräckliga finansiella resurser för att kunna driva verksamheten i enlighet med policyn.

2.1.1.2 Beställning av kundcertifikat

Utfärdaren skall tillse att:

a) beställning av kundcertifikat sker enligt bestämmelserna i denna policy,

b) avtalet om och ansökningshandling för kundcertifikat innehåller de uppgifter som krävs enligt kapitel 3 och kapitel 4,

c) kontroller av sökandens identitet sker enligt bestämmelserna i 3.1.3

2.1.1.3 Distribution

Utfärdaren skall tillse att:

a) kontroller av beställda och levererade kundcertifikat före nyckelinitiering och personalisering sker enligt bestämmelserna i 6.1,

b) personaliserade kundcertifikat förvaras och levereras på sätt som beskrivs i 6.1.

c) kundcertifikatsinnehavaren förses med uppgifter för att säkerställa nedladdning av certifikat.

2.1.1.4 Skydd av CA-systemets privata nycklar

Utfärdaren åtar sig att skydda de privata nycklarna enligt bestämmelserna i 6.2.6

2.1.1.5 Begränsningar av användandet av Utfärdarens privata nycklar

Utfärdarens privata nycklar, som används för att utge certifikat i enlighet med denna policy, får endast användas för att signera certifikat, spärrlistor och loggar, eller andra funktioner i enlighet med dessa.

2.1.2 RA:S åtaganden

2.1.2.1 Allmänna bestämmelser

RA åtar sig att:

a) utlämningen av kundcertifikat endast sker efter vedertagen identifiering av certifikatsinnehavaren enligt 3.1.3 samt 6.1.2,

b) leverans av kundcertifikat bekräftas av kunden genom att svara på e-post som innehåller certifikatfilen, att svar erhållits registreras hos RA.

c) tillhandahålla kontrollåtgärder enligt kapitel 3 till och med 6,

d) skydda sin privata nyckel i enlighet med avtal med denna policy och avtal med Utfärdaren.

2.1.3 Kundcertifikatsinnehavarens åtaganden

2.1.3.1 Ansökan om kundcertifikat

Sökanden skall vid ansökan om kundcertifikat åta sig att följa tillämpliga rutiner som anges i kapitel 3 och 4, samt avtalet för ansökan om kundcertifikat och där till att lämna sanningsenliga uppgifter.

2.1.3.2 Mottagande av kundcertifikat

Kunden ska bekräfta mottagandet av certifikatet enligt rutiner som anges i kapitel 3 och 4, samt avtalet för ansökan om kundcertifikat.

2.1.3.3 Skydd av kundcertifikatsinnehavarens privata nyckel

Kundcertifikatsinnehavaren skall tillse att denne har kontroll över sitt kundcertifikat och skydda den i enlighet med relevanta delar ur kapitel 6 i denna policy.

Kundcertifikatsinnehavaren skall vidta åtgärder att förhindra obehörigt utnyttjande av certifikatet med tillhörande privata nyckel genom att:

a) byta det lösenord som medföljer från Utfärdaren innan kundcertifikatet tas i bruk.

b) lösenord eller annan säkerhetsrutin som används inte avslöjas för annan,

c) kundcertifikatet skyddas på motsvarande sätt som värdeföremål,

d) lösenord aldrig förvaras tillsammans med kundcertifikatet,

e) ett aktiverat kundcertifikat aldrig lämnas oskyddat.

f) ej utnyttja de funktioner för cachning av lösenord som finns inbyggda i de flesta webbläsare.

Kundcertifikatsinnehavaren skall omedelbart om det föreligger anledning enligt avtal eller enligt punkt 4.4.1 anmäla om spärrning av kundcertifikat.

2.1.4 Förlitande parts åtaganden

2.1.4.1 Användande av kundcertifikat för lämpliga ändamål

Det är Förlitande Parts eget ansvar att säkerställa att kundcertifikaten används för lämpliga ändamål. Till vägledning för beslutet har Förlitande Part kundcertifikaten och denna policy.

Punkten om lämpliga användningsområden 1.3.4.1 skall särskilt beaktas.

2.1.4.2 Skyldighet att verifiera och kontrollera

Det är Förlitande Parts eget ansvar att verifiera kundcertifikatens äkthet och tillämplighet, samt dess giltighet i enlighet med 4.4.

2.2 ANSVAR

2.2.1 Utfärdarens ansvar

2.2.1.1 Garantier och ansvarsbegränsningar

Genom att signera ett certifikat som innehåller objektidentifierare för denna policy, intygar Utfärdaren att denne har kontrollerat informationen i kundcertifikatet i enlighet med de rutiner som fastslagits i denna policy.

Utfärdaren ansvarar inte för skada som uppkommit på grund av uppgifterna i ett kundcertifikat eller spärrlista är felaktiga så vida Utfärdaren inte gjort sig skyldig till grov vårdslöshet.

2.2.2 Ansvar för RA

Utfärdaren ansvar för de tjänster som RA utför på uppdrag av Utfärdaren. Avtal mellan Utfärdaren och RA skall återspegla RA:s ansvars och förpliktelser i enlighet med denna policy.

2.3 FINANSIELLT ANSVAR

2.3.1 Fullmaktsförhållanden

Utfärdande av kundcertifikat i enlighet med denna policy medför inte att Utfärdaren skall betraktas som agent, fullmäktig, eller på annat sätt som representant för kundcertifikatsinnehavaren eller Förlitande Part.

2.4 TOLKNING OCH GENOMFÖRANDE

2.4.1 Tillämplig lag

Svensk rätt skall äga tillämpning på denna policy samt därur uppkomna rättsförhållanden.

2.4.2 Tvistelösning

Tvist i anledning av denna policy skall slutligt avgöras genom skiljedom vid och enligt Regler för Stockholms Handelskammares Skiljedomsinstitut (Institutet).

Överstiger inte tvisteföremålets värde vid tvistens påkallande ett belopp som motsvarar 25 gånger prisbasbeloppet enligt lagen (1962:381) om allmän försäkring skall Institutets Regler för förenklat skiljeförfarande tillämpas.

2.5 AVGIFTER

Kundcertifikaten är avgiftsfria för Sjöfartsverkets kunder.

2.6 PUBLICERING OCH ÅTKOMST AV INFORMATION

2.6.1 Publicering av information

Utfärdare skall tillhandahålla följande:

a) denna policy, och tillhörande utfärdardeklaration (CPS),

b) spärrlistor (CRL),

c) samtliga utfärdarcertifikat som utfärdats,

d) resultat av granskningar i enlighet med 2.7.2, med undantag för säkerhetskänslig information,

e) villkor för kundcertifikatsinnehavare.

Policy, utfärdardeklaration (CPS), spärrlistor, utfärdarcertifikat och resultat av granskningar skall alltid vara tillgängliga via http://eservices.sjofartsverket.se/pki

2.6.2 Periodicitet för publicering

Spärrlistor skall publiceras enligt 4.4.7.

2.6.3 Behörighetskontroll

Det förekommer inte någon behörighetskontroll för att läsa denna policy. Behörighetskontroll tillämpas däremot vid förändring av denna policy.

2.7 GRANSKNING

2.7.1 Utföranden

Utfärdaren skall löpande (min var 36:e månad) göra interna granskningar för att säkerställa att denna policy efterlevs.

Vid granskning skall speciellt följand undersökas:

- utfärdardeklaration (CPS) lämplighet och överensstämmelse med policy
- Den praktiska implementeringen av utfärdardeklaration (CPS)
- Avtal och samverkansförhållanden som rör underleverantörer och RA

2.7.2 Information om resultatet av granskning

Redovisningen skall innehålla information om samtliga upptäckta brister som är av sådan art att de kan anses påverka en Förlitande Parts förtroende för ett utfärdat kundcertifikat och innefatta uppgifter om typ av brister samt bedömning av eventuella risker och konsekvenser. Däremot skall redovisningen inte innehålla detaljerade uppgifter om brister som kan tänkas äventyra säkerheten i systemet.

Redovisningar från de senaste granskningarna skall finnas tillgängliga enligt 2.6.1

2.8 KONFIDENTIALITET

2.8.1 Typ av information som skall hållas konfidentiell

Rutiner för Sjöfartsverkets skapande-, utgivnings- och återkallande processer av kundcertifikat kan sekretessbeläggas enligt sekretesslagen 5 kap 3 § 2 p. Information om vilka företag och anställda som har certifikat och därmed behörighet att utbyta känslig information med Sjöfartsverket kan sekretessbeläggas enligt sekretesslagen 5 kap 2 § 4 p.

Loggar skall inte göras tillgängliga i sin helhet, såvida inte annat är föreskrivet i lag. Endast händelser beträffande enstaka transaktioner får utlämnas enligt 4.6.4.

2.8.2 Typ av information som inte anses vara konfidentiell

Följande uppgifter anses inte vara konfidentiella:

a) utfärdade kundcertifikat,

b) uppgift om spärrade kundcertifikat,

c) publika nycklar,

d) redovisning av granskning enligt 2.7.2, med undantag för säkerhetskänslig information,

e) denna policy, och tillhörande utfärdardeklaration (CPS),

f) villkor för kundcertifikatsinnehavare.

2.8.3 Tillhandahållande av information om anledning till spärrning av kundcertifikat

Anges i spärrlista i enlighet med standard.

2.8.4 Tillhandahållande av konfidentiell information till polis, åklagare eller annan

Konfidentiell information kan lämnas till polis, åklagare eller annan i enlighet med lag eller beslut i domstol.

2.9 IMMATERIELLA RÄTTIGHETER

Policy och dokument tillhörande kundcertifikatstjänsten får endast reproduceras och spridas i sin helhet, under förutsättningarna att detta sker utan avgift. Ingen information får förändras, tas bort, eller läggas till.

2.10 AVTALSVILLKOR FÖR KUNDCERTIFIKATS-INNEHAVARE

Olika avtal används för kundcertifikat, i och med detta kan handhavande, beställning etc. ske på ett varierande sätt.

Avtalsvillkor för kundcertifikatsinnehavare reglerar:

a) rättigheter och skyldigheter för båda parterna,

b) erkännande av kundcertifikat och riktigheten av den information som har lämnats,

c) att kundcertifikatsinnehavaren accepterar de villkor och förutsättningar som gäller för användningen av kundcertifikaten,

d) villkor för hantering av personuppgifter.

Utfärdaren ansvarar för att avtal utarbetas med eventuella underleverantörer. I avtalet skall klart framgå rättigheter och skyldigheter för båda parterna.

2.11 TILLGÄNGLIGHET OCH SVARSTID

Spärrfrågor kan ställas under avtalad drifttid, dvs. 24 timmar om dygnet 7 dagar i veckan med undantag för servicefönster.

3 IDENTIFIERING OCH AUTENTISERING

Detta kapitel beskriver regler och rutiner som gäller vid identifiering och autentisering av fysiska personer och organisationer involverade i certifieringsprocessen. Personuppgifter hanteras i enlighet med personuppgiftslagen, eller annan gällande rätt/avtal som ger stöd till behandling av personuppgifterna.

3.1 INITIAL REGISTRERING

3.1.1 Typer av namn

Följande uppgifter är obligatoriska:

Uppgift	**Krav på innehåll**
Kund	Kundens namn
Adress	Adress till kundens huvudsäte
Förnamn	Innehavare av kundcertifikatets förnamn, Pseudonymer är inte tillåtna
Efternamn	Innehavare kundcertifikatets efternamn. Pseudonymer är inte tillåtna
Identifierare	Organisationsnummer/registreringsnr/VAT-nr
Unik identifierare	/Registreringsnr/VAT-nr plus löpnummer med start på 000
E-postadress	Till innehavare av kundcertifikatet

Certifikat kan innehålla andra typer av uppgifter om kundcertifikatsinnehavaren (se 7.1).

3.1.2 Namnsättning

De obligatoriska uppgifterna enligt 3.1.1 skall på ett unikt sätt identifiera kundcertifikatsinnehavaren. Endast officiellt registrerade identitetsuppgifter om den sökande organisationen accepteras. Av kunden utsedda kontaktpersoner accepteras.

3.1.3 Fastställande av sökandens identitet

RA ansvarar för att vidta de åtgärder som här beskrivs i syfte att fastställa att sökande organisation är den juridiska person han eller hon uppger sig vara och att sökandens representant har en anställning/koppling till sökande organisation samt att de uppgifter som sökanden uppger och som ligger till grund för det kundcertifikat som skall utfärdas är korrekta.

Den person hos RA som ansvarar för identifieringen skall personligen signera att identiteten har fastställts och hur detta skett. Denna signering kan ske digitalt.

3.1.3.1 Metod för att styrka sökandens identitet

Sökandens identitet har tidigare säkerställts via relationen med sjöfartsverket.

Kunder till Utfärdarens webbtjänst kan när denna är inloggad beställa, och spärra eget kundcertifikat.

3.1.3.2 Kontroll av identitetsuppgifter

Obligatoriska uppgifter samt adress på den sökande kontrolleras gentemot Sjöfartsverkets befintliga kundregister.

3.2 FÖRNYELSE AV NYCKLAR OCH CERTIFIKAT

3.2.1 Förnyelse av nycklar och certifikat

Om kundens förhållande till sjöfartsverket inte har förändrats och om kundens övriga uppgifter inte ändrats kan en förnyelse av certifikat och nycklar ske med det gamla certifikatet som identifieringsmekanism.

3.3 BEGÄRAN OM SPÄRRNING

Spärrningsbegäran skall hanteras i enlighet med 4.4.

4 OPERATIONELLA KRAV

Detta kapitel beskriver de operationella krav som gäller för Utfärdaren, RA, sökanden och kundcertifikatsinnehavaren.

Kraven omfattar ansökan, utfärdande, spärrning, arkivering och loggning.

4.1 ANSÖKAN OM KUNDCERTIFIKAT

Nedanstående rutiner skall tillämpas vid ansökan om kundcertifikat. Sökanden skall identifiera sig i enlighet med kapitel 3, samt att:

a) sökande skall fylla i ansökan och underteckna avtal där alla villkor enligt 2.10 accepteras,

b) sökanden skall skriftligen instrueras att byta initialt lösenord till personligt valt lösenord vid första lämpliga tillfälle,

c) utfärdaren arkiverar ansökningshandlingar enligt 4.6.

d) Sökande ska bekräfta att certifikat är mottaget genom att svara på e-post som innehåller certifikatfil.

Ansökan får innehålla mer än bara certifikatsansökan och avtala om mer än bara själva kundcertifikatet.

4.2 UTFÄRDANDE AV KUNDCERTIFIKAT

Utfärdandet av kundcertifikat bekräftar Utfärdarens acceptans av ansökan samt av de uppgifter som sökanden lämnat.

Registrering och hantering av den information som krävs för att utfärda kundcertifikaten skall ske i system och miljöer som är väl skyddade och utformade så att det förhindrar sammanblandning av identitetsuppgifter, certifikatfiler och nycklar.

Varje godkänd beställning av kundcertifikat hos Utfärdaren eller RA, ska kunna spåras individuellt till den person som begärt beställningen.

4.3 UTLÄMNADE AV KUNDCERTIFIKAT

Nedanstående rutiner skall tillämpas vid utlämnande av kundcertifikat. Sökanden skall identifiera sig i enlighet med kapitel 3, samt att:

a) sökanden skall skriftligen upplysas om att lösenord till kundcertifikaten levereras separat från certifikatfilen,

b) sökanden skall skriftligen instrueras att byta initialt lösenord till personligt valt lösenord vid första lämpliga tillfälle. Lösenordet ska vara av god kvalitet och följa gällande rekommendtionen från Sjöfartsverket.

c) sökanden accepterar utfärdandet av kundcertifikat och gällande villkor genom ansökan enligt 4.1.

d) Sökande ska bekräfta att certifikat är mottaget genom att svara på e-post som innehåller certifikatfil.

4.4 SPÄRRNING AV KUNDCERTIFIKAT

Spärrning av ett kundcertifikat innebär att samtliga certifikat knutna till certifikatinnehavaren spärras.

Utfärdaren tillhandahåller tjänst för att spärra kundcertifikat, som säkerställer information om spärrade kundcertifikat under hela kundcertifikatens livslängd. Publicering och spärrkontrollen görs mot en spärrlista (CRL).

Vid spärr av kundcertifikat informeras innehavaren enligt avtalen i 2.10.

4.4.1 Anledning till spärrning

Kundcertifikat ska spärras om någon uppgift i kundcertifikatet är eller misstänks vara inkorrekt, eller om den privata nyckel som är kopplad till kundcertifikatet är röjd eller att det finns anledning att misstänka att den är röjd.

Exempel på sådana situationer är:

- förlust av certifikatfil,
- ändring av någon av de uppgifter eller förhållanden som kundcertifikaten innehåller t.ex. ändring av namn,
- nycklarna är röjda, eller det finns anledning att misstänka att nycklarna är röjda.

Utfärdaren kan på eget initiativ spärra kundcertifikat om kundcertifikatsinnehavaren inte anses fullgöra sina åtaganden.

4.4.2 Behörig att begära spärrning

Spärrning av kundcertifikat kan endast begäras av kundcertifikatsinnehavaren, eller på initiativ av Utfärdaren vid misstanke om obehörigt nyttjande av kundcertifikat. Övriga möjligheter till spärring regleras i separata avtal med respektive avtalspart.

4.4.3 Rutin för begäran om spärrning

Spärrning skall begäras snarast om anledning föreligger enligt 4.4.1.

Identifiering av den som begär spärrning skall ske på lämpligt sätt. Utfärdaren kan besluta om spärrning även om identifiering inte kan utföras i de fall det föreligger risk för missbruk av kundcertifikat

Mottagen spärrningsbegäran arkiveras tillsammans med information om:

a) datum och tidpunkt,
b) anledning till spärr
c) mottagande handläggare, vid manuell spärrning.

4.4.4 Behandlingstid vid begäran om spärrning

Relevant information om spärrning skall publiceras i spärrlista senast fyra (4) timmar efter beslut om spärrning. Beslut om spärrning sker vanligtvis i direkt anslutning till spärrbegäran, vid eventuella oklarheter eller brister i begäran kan

försening uppstå.

4.4.5 Öppettid för spärrtjänsten

Utfärdarens spärrtjänst är tillgänglig via Utfärdarens kundstöd:

september – april	Helgfria vardagar 08:00 – 16:30
maj – augusti	Helgfria vardagar 08:00 – 16:00
Hela året	Vardag före röd dag 08:00 – 12:00

Planerade avbrott utförs normalt den första torsdagen i varje månad mellan 07:00-09:00.

4.4.6 Periodicitet för utgivning av spärrlista

Nya spärrlistor (CRL eller DeltaCRL) skall publiceras var 4:e timme, dygnet runt med en giltighetstid på 8 timmar. CRLer ska publiceras var 24 timma.

4.4.7 Krav på spärrkontroll

Det är Förlitande Parts eget ansvar att kontrollera om ett kundcertifikat är spärrat eller inte. Kontrollen skall utföras på följande sätt:

a) Förlitande Part som hämtar spärrlista från lagringsplats skall försäkra sig om dess äkthet genom att verifiera dess digitala signatur och certifieringskedja.

b) Förlitande Part skall även kontrollera spärrlistans giltighetstid för att försäkra sig om att den är aktuell.

c) Om ett certifikat är spärrat eller spärrkontroll enligt ovan inte kan genomföras, skall kundcertifikatet inte accepteras. Användandet av kundcertifikatet i sådana fall sker helt på Förlitande Parts egen risk.

4.5 LOGGNING

Här specificeras rutiner för loggning av händelser samt därtill relaterad granskning av säkerheten i CA-systemet på systemnivå och operativsystemnivå.

Regler och krav för säkerhetsmoduler som används i CA-systemet specificeras i kapitel 6.

4.5.1 Händelser som loggas

I CA-miljön skall minst följande händelser loggas:

a) Skapande, förändring och borttagning av användarkonton,

b) initiering av transaktioner, med information om vem som begärde transaktionen, tidpunkt, vilken typ av transaktion som initierats samt uppgift om resultatet av initieringen,

c) installation och uppdatering av mjukvara,

d) relevant information om säkerhetskopiering,

e) start och stopp av systemet eller tjänster i systemet,

f) datum och tid för uppgradering av hårdvara,

g) datum och tid för tömning av loggar.

4.5.2 Kontroll av loggar

Loggarna granskas kontinuerligt och analyseras för att upptäcka oönskade händelser.

4.5.3 Skydd av loggar

Samliga loggar ska skyddas med lämpligt integritetsskydd samt tidstämpel. Samtliga händelser förses med individuella tidstämplar.

4.6 ARKIVERING

4.6.1 Information som arkiveras

Utfärdaren arkiverar följande:

a) transaktioner innehållande av behörig operatör signerad begäran om certifikatproduktion och spärrning av certifikat,

b) avtal rörande kundcertifikat,

c) kundcertifikatens innehåll,

d) historik rörande tidigare utfärdarnycklar,

e) uppgifter om korscertifiering inklusive grunderna på vilka korscertifiering beslutats,

f) begäran om spärrning enligt 4.4.3,

g) protokoll från granskningar enlig 2.7.5,

h) gällande och föregående version av policyn,

i) säkerhetsloggar både från passersystem och CA-system.

4.6.2 Lagringstid

Arkiverad information skall lagras och skyddas mot förändring och förstörelse under en tid av minst 10 år.

Utfärdaren kan lagra informationen längre om lagar så kräver.

4.6.3 Skydd av arkiv

Utfärdaren följer normal standard för skydd av värdehandling.

4.6.4 Rutiner för åtkomst och verifiering av arkivmaterial

Arkiverat material som är klassat som konfidentiellt skall inte vara tillgängligt för externa parter i sin helhet annat än vad som krävs genom lag och beslut i domstol.

Information om enskilda händelser kan erhållas efter begäran av någon involverad part eller representant för involverad part eller annan behörig.

Arkiverat material som inte anses konfidentiellt enligt 2.8.2 kan lämnas ut utan prövning.

Arkiven skall lagras under sådana förhållanden att de är läsbara för granskning under den angivna lagringstiden.

4.7 BYTE AV UTFÄRDARNYCKEL

Nya utfärdarnycklar genereras minst tre månader innan de gamla nycklarnas giltighetstid gått ut.

Vid byte av utfärdarnyckel sker följande:

a) nytt egensignerat certifikat utfärdas för den nya publika utfärdarnyckeln,

b) korscertifikat utfärdas genom att den gamla utfärdarnyckeln signeras med den nya och den nya med den gamla utfärdarnyckeln.

4.8 KATASTROFPLAN VID MISSTANKE OM RÖJDA UTFÄRDARNYCKLAR

Utfärdaren genomför följande åtgärder om det föreligger misstanke om att de privata

utfärdarnycklarna skulle vara röjda:

a) göra en menbedömning för att bedöma omfattning och lämpliga åtgärder,

b) informera kundcertifikatsinnehavarna, korscertifierade CA och andra parter med vilka Utfärdaren har överenskommelser eller andra etablerade relationer,

c) i de fall den utfärdarnyckel som misstänks vara röjd används vid tjänst för spärrkontroll skall denna tjänst omedelbart upphöra. Detta medför att certifikaten inte accepteras av Förlitande Part som utövar spärrkontroll enligt. 4.4.8,

d) omedelbart spärra samtliga kundcertifikat i de fall annan utfärdarnyckel används vid tjänst för spärrkontroll av certifikat utfärdade med den utfärdarnyckel som misstänks vara komprometterad.

e) spärra samtliga utfärdarcertifikat för den röjda utfärdarnyckeln, som utfärdats med annan utfärdarnyckel,

f) säkerställa att spärrinformation finns tillgänglig för utfärdarcertifikat enligt punkten e) fram till dess att de spärrade certifikatens giltighetstid löpt ut.

4.9 UPPHÖRANDE AV UTFÄRDARENS VERKSAMHET

Med upphörande av Utfärdarens verksamhet avses en situation där samtliga tjänster kopplade till Utfärdaren upphör.

Innan Utfärdaren upphör med sin verksamhet skall minst följande åtgärder vidtas:

a) Specifikt informera samtliga kundcertifikatsinnehavare, och alla parter utfärdaren har en relation med, mins sex månader innan verksamheten upphör.

b) Öppet informera om att verksamheten upphör minst tre månader i förväg.

c) Upphöra med tjänst för spärrkontroll av kundcertifikat. Detta medför att kundcertifikaten inte accepteras av Förlitande Part som utövar spärrkontroll enligt. 4.4.8.

d) Avsluta alla rättigheter för underleverantörer att agera i den upphörande Utfärdarens namn.

e) Säkerställa att alla arkiv och loggar kan bevaras på ett betryggande sätt under 10 år eller enligt överenskommen arkiveringstid.

5 SÄKERHETSKONTROLLER

Detta kapitel beskriver fysiska, procedurorienterade och personella kontroller som utförs av Utfärdaren, och RA.

5.1 FYSISK SÄKERHET

Tillträdeskontroll skall tillämpas för att kontrollera tillträde till driftutrymme för CA-systemet. En logg skall föras över alla som bereds tillträde till detta område.

Utrymmet är försett med nödvändiga larm för att säkerställa upptäckt av varje typ av obehörigt intrång.

Utfärdaren skall säkerställa att arkiv- och säkerhetskopior samt distributionsmedia förvaras på ett sådant sätt att förlust, manipulation eller obehörig användning av lagrad information förhindras.

Säkerhetskopior skall förvaras på annat ställe än i den anläggning där Utfärdarens centrala funktioner finns, för att möjliggöra återställande vid en eventuell

katastrofsituation vid Utfärdarens centrala anläggning. Förvaringen av säkerhetskopiorna följer Sjöfartverkets ordinarie rutiner.

Säkerhetskontroll skall ske kontinuerligt vid Utfärdarens centrala anläggning för att säkerställa ovanstående.

5.2 PROCEDURORIENTERAD SÄKERHET

Utfärdaren ansvarar för administration och rutiner för utfärdande av kundcertifikat och spärrlistor. Rutiner för spårbarhet skall finnas, så att missbruk och fel i olika led av denna procedur kan upptäckas och korrigeras.

5.2.1 Betrodda roller inom ca-funktionen

Utfärdaren har definierat tre olika roller. En annan organisation kan accepteras under förutsättning att de har en god förmåga att förhindra insiderattacker.

Följande roller finns inom Utfärdarens organisation:

Certification Authority Administrator (CAA), utför centrala operationer på CA-systemet. Dessa är samtliga personer som hos Utfärdaren har behörighet att utföra registreringar och andra administrativa operationer.

Typiska uppgifter är:

- utfärda certifikat,
- personalisera kundcertifikat,
- generera manuella spärrlistor,
- spärra certifikat,
- logganalys.

System Administrator (SA) utgörs av driftspersonal.

Detta är driftspersonal som utför installationer, systemunderhåll, byte av media för säkerhetskopiering, m.m. Dessa behöver inte alltid ha behörighet enligt CAA, men har lämplig behörighet på operativsystemnivå i systemen beroende på uppgifterna. Typiska uppgifter är:

- installation under övervakning av ISSO (se nedan)/CAA,
- konsolidering av loggar tillsammans med ISSO,
- systemunderhåll,
- byte av media med säkerhetskopior och transport för lagring.

Information Systems Security Officer (ISSO) ansvarar för alla operativa roller.

Dessa personer har högsta ansvaret och ska t.ex. närvara vid särskilt säkerhetskritiska operationer. Typiska uppgifter är:

- Övervaka installationer och generering av CA-nycklar samt konsolidering av loggar,

- godkänna tilldelning av roller,
- ansvara för att alla agerar inom ramen för sina roller

5.2.2 Krav på antal personer per uppgift

Vissa känsliga moment och arbetsuppgifter skall kräva närvaro av fler än en person. Denna policy föreskriver ett antal sådana moment, exempelvis;

- Vid initieringen av CA-systemet krävs närvaro av minst två olika personer som innehar ISSO eller CAA-rollen.
- För konsolidering av loggar av det centrala CA-systemet, krävs två personer med SA och/eller ISSO-roll,
- För fysisk åtkomst till den inlåsta säkerhetskopian av CA:s privata nyckel krävs två personer med SA och/eller ISSO-roll.

5.2.3 Identifiering och autentisering av personer i betrodda roller

Det skall finnas tekniska möjligheter att identifiera och autentisera ovan nämnda roller i CA-systemet.

5.3 PERSONORIENTERAD SÄKERHET

5.3.1 Bakgrund och kvalifikationer

Personal som innehar roller som ur säkerhetssynpunkt betraktas som kritiska skall vara särskilt utvalda och pålitliga personer som uppvisat lämplighet för sådana befattningar.

Personal får inte ha några andra uppgifter som kan vara i konflikt med de åligganden och ansvar som följer av de roller som de har i CA-systemet.

5.3.2 Krav på utbildning

All personal hos Utfärdaren som berörs av CA-systemet skall ha erforderlig utbildning och kunskap för att utföra sina arbetsuppgifter.

5.3.3 Personorienterad säkerhet för RA

Ansvarig personal hos RA/underleverantör utses inom den organisation som är utsedda av Utfärdaren att utföra arbetsuppgiften. RA organisation ansvarar för att lämplig personalkontroll görs.

Separata avtal reglerar säkerheten för RA (om denna är extern) och underleverantörer.

6 TEKNISK SÄKERHET

Detta kapitel innehåller regler för generering och installation av nyckelpar, skydd av nycklar samt andra tekniska säkerhetskontroller.

6.1 GENERERING OCH INSTALLATION AV NYCKELPAR

6.1.1 Generering av nyckelpar

Indata till samtliga nyckelgenereringsprocesser skall vara ett slumptal skapat på sådant sätt och av sådan längd att det är beräkningsmässigt ogörligt att återskapa detsamma även med kunskap om när och i vilken utrustning det genererades.

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

Publika nycklar skall även de hanteras på ett sådant sätt att deras integritet garanteras.

6.1.1.1 Utfärdarnycklar för signering av certifikat och spärrlistor

Utfärdarnycklar som används för signering av certifikat och spärrlistor skall genereras och användas i en skyddad miljö enligt 5.1.

6.1.1.2 Nyckelpar för kundcertifikatsinnehavare

Nycklar för kundcertifikat genereras i certifikatfilen i samband med certifiering. Nycklar kan genereras hos kunden med process godkänd av Utfärdaren.

Kundcertifikatsinnehavarens privata nycklar skall lagras läs- och skrivskyddade i kundcertifikaten. Vid certifieringen skall nycklarnas integritet kontrolleras.

Nyckelgenereringen och tillhörande kontroller (före certifiering) skall ske på sådant sätt att sannolikheten för att nyckelpar dubbleras är försumbar eller obefintlig.

6.1.2 Leverans av kundcertifikat

Det är Utfärdaren/RA som ansvarar för utlämning av kundcertifikaten. Kundcertifikaten skyddas av ett initialt lösenord, detta skall distribueras till innehavaren på sådant sätt att det inte uppträder tillsammans med kundcertifikatet förrän hos innehavaren.

Kundcertifikatsinnehavaren skall identifiera sig enligt 3.1.3. Identifieringsmetoden skall noteras på handling, som också undertecknas av den person som överlämnar certifikaten.

Kundcertifikatsinnehavaren skall bekräfta mottagande av kundcertifikat t ex genom att svara på e-post med certifikatsfil.

Kundcertifikatsinnehavaren skall instrueras tydligt att vid första lämpliga tillfälle byta initialt lösenord mot ett personligt lösenord.

Leverans av kundcertifikaten sker till innehavarens e-postadress angiven i certifikatsansökan.

6.1.3 Nyckelstorlek

Nyckelstorleken skall ha en längd och styrka som är tillförlitliga enligt vid var tid gällande praxis.

Gällande nyckelstorlek för RSA-nyckelpar som genereras i CA-systemet är 2048 bitar.

6.1.4 Generering av publik nyckel

Kundcertifikatsinnehavarens nycklar som i certifikaten markeras med användningsområdena kryptering, autentisering, och/eller verifiering av oavvislig digital information (dokument) ges publika exponenter som förhindrar kända attacker.

Utfärdarens nycklar ges publika exponenter som förhindrar kända attacker.

Det förutsätts att Utfärdaren håller sig ajour med teknikutvecklingen inom PKI och anpassar sina kryptoalgoritmer i enlighet med den för att bibehålla en hög skyddsnivå.

6.2 SKYDD AV PRIVATA NYCKLAR

6.2.1 Säkerhetsmodul och kundcertifikat

Privata utfärdarnycklar avsedda att signera certifikat, spärrlistor, utfärdarcertifikat och korscertifikat, samt andra privata nycklar i CA-systemet, säkras av starka fysiska skydd samt lagras och används på ett smart kort eller annan säkerhetsmodul.

Övriga privata nycklar i Utfärdareprocessen som används utanför CA-systemets miljö och som påverkar certifikatutgivnings- och spärrkontrolltjänster skall lagras och användas i ett smart kort eller annan säkerhetsmodul.

För innehavare av kundcertifikat lagras nycklarna lokalt på innehavarens lokala lagringsmedia.

6.2.2 Flerpersonskontroll av privata nycklar

Vissa känsliga moment och arbetsuppgifter skall kräva närvaro av fler än en person, se 5.2.2.

6.2.3 Säkerhetskopiering av privata nycklar

Personliga nycklar för kundcertifikatsinnehavare säkerhetskopieras ej.

Privata utfärdarnycklar avsedda att signera certifikat, spärrlistor, utfärdarcertifikat och korscertifikat, samt andra privata nycklar i CA-systemet säkerhetskopieras.

Dessa nycklar säkerhetskopieras på ett sådant sätt att kopiorna erhåller minst samma skydd som nycklar som används i produktionsmiljö. Säkerhetskopiorna förvaras inlåst i byggnad som är fysiskt skild från platsen där originalet förvaras.

6.2.4 Arkivering av privata nycklar

Kundcertifikatsinnehavarens privata nycklar arkiveras ej.

Avseende säkerhetskopiering av privata utfärdarnycklar samt andra privata nycklar i CA-miljön, se 6.2.3.

6.2.5 Lagring av kundcertifikatens privata nyckel

Den privata nyckeln för kundcertifikaten lagras lokalt på kundcertifikatsinnehavarens lagringsmedia (hårddisk, diskett el. liknande) och skyddas av ett lösenord.

6.2.6 Aktivering av privata nycklar i kundcertifikaten

De privata nycklarna i kundcertifikaten är skyddade mot exponering och obehörig användning.

Endast de algoritmiska funktionerna i kundcertifikaten som utför operationer hänförliga till den asymmetriska krypteringen, skall ha åtkomst till dessa nycklar.

Användning av nycklarna i kundcertifikaten skall kräva att den först aktiveras med ett korrekt lösenord.

6.2.7 Förstörelse av utfärdarens privata nycklar

När användningsperioden för privata utfärdarnycklar gått ut skall alla exemplar av nycklarna förstöras. Utfärdarnycklarna får ej förstöras om de står i strid med arkiverings krav i denna policy eller krav i lagstiftning.

Säkerhetskopior förstörs genom att förbrukat lagringsmedium förstörs fysiskt.

Utfärdarnycklar som lagras i det centrala CA-systemet gäller följande:

- Om lagringsmedia skall användas vidare i samma skyddande miljö sker överskrivning på sådant sätt att återskapande av nycklar försvåras.
- Om utrustning innehållande lagringsmedia skall användas utanför den skyddade miljön skall lagringsmedia demonteras och förstöras fysisk för att förhindra återskapande av nycklar.

6.3 ANDRA ASPEKTER PÅ NYCKELHANTERING

Ingen känslig information från CA-, nyckelgenererings- eller personaliseringsprocessen får lämna systemen på ett sätt som är i konflikt med denna policy. Lagringsmedia som är utrangerad skall exempelvis förstöras fysiskt, vid service skall aldrig lagringsmedia skickas med utanför CA-miljön.

6.3.1 Arkivering av publika nycklar

Alla publika nycklar skall arkiveras av Utfärdaren. Arkiveringstid enligt 4.6.2.

6.3.2 Privata nycklars livslängd

Privat nyckel för kundcertifikat begränsas av certifikatets giltighetstid.

6.3.3 Certifikatens giltighetstid

Kundcertifikat utfärdas med en livslängd på 2 år.

Utfärdarcertifikat utfärdas med en livslängd på 7 år.

Självsignerat rotcertifikat utfärdas med en giltighetstid på 20 år.

6.4 AKTIVERINGSDATA

6.4.1 Generering och installation av aktiveringsdata

Indata till samtliga genereringsprocesser, t ex nyckelgenerering skall vara ett slumptal.

6.4.2 Skydd av aktiveringsdata

Aktiveringsdata skall lagras i kundcertifikaten på sådant sätt att aktiveringsdata aldrig exponeras.

Utformningen av denna miljö skall säkerställa att ingen kan få kontroll över aktiveringsdata.

6.5 SÄKERHET I DATORSYSTEM

CA-systemet skall ha säkerhetsfunktioner för att säkerställa rollfördelningen beskriven i 5.2.

Säkerhetsfunktionerna skall säkerställa åtkomstkontroll och spårbarhet för varje operatör på individuell nivå för de funktioner som påverkar användning av privata utfärdarnycklar.

6.5.1 Tekniska krav

Initiering av det system som utnyttjar privata utfärdarnycklar skall kräva samverkan av minst två betrodda operatörer. En detaljerad logg skall föras över alla manuella steg i processen.

Installation av operativsystem och CA-system skall ske i direkt anslutning till formatering av diskar och med leverantörens originalutgåva av programmen. Vid registrering av initiala användare och behörigheter i CA-systemet skall minst två personer i betrodda roller samverka. Ett protokoll över installations- och konfigureringsprocessen skall signeras av samtliga deltagare och arkiveras.

6.6 KONTROLL AV SÄKERHET HOS SYSTEMET UNDER LIVSCYKELN

6.6.1 Kontroller av systemutveckling

Utveckling av programvara som implementerar funktionalitet hos CA-systemet, skall utföras i en kontrollerad miljö där leverantören tillämpar ett kvalitetssystem för skydd mot införande av obehörig kod.

6.6.2 Kontroller av säkerhetsadministration

Rollerna enligt 5.2 skall implementeras i Utfärdarens processer och deras tillämpning skall säkerställas.

6.7 KONTROLL AV NÄTVERKSSÄKERHET

Utfärdarens CA-system är anslutet till ett externt nätverk och skyddas av en brandvägg med tillräcklig styrka för att motstå angrepp som kan misstänkas mot systemet.

Brandväggen är konfigurerad för att tillåta passage endast av de protokoll som är nödvändiga för att realisera CA-funktionen.

Kommunikation till och från CA-miljön utnyttjar kryptering av en styrka som är tillförlitligt enligt vid var tid gällande praxis.

7 PROFILER FÖR CERTIFIKAT OCH SPÄRRLISTOR

Certifikat och spärrlistor skall utformas enligt X.509-standarden.

7.1 CERTIFIKATENS PROFIL OCH VERSION

Förekomst och användning av dataelement i certifikaten skall ske i enlighet med denna policy och tillhörande utfärdardeklaration (CPS). Certifikatsstandard är X.509 version 3

7.2 PROFIL FÖR SPÄRRLISTA

I de fall spärrlista utfärdas skall denna följa CRL version 2 enligt X.509.

8 FÖRVALTNING AV POLICYN

Detta kapitel innehåller bestämmelser avseende förändringar och publiceringar av policyn.

8.1 FÖRÄNDRING AV POLICYN

8.1.1 Förändringar som kan ske utan underrättelse

De förändringar som kan göras av denna policy utan underrättelse till berörda parter är språkliga justeringar och omdispositioner som inte påverkar säkerhetsnivån i beskrivna rutiner och regler.

8.1.2 Förändringar som kan ske med underrättelse

Administrationsansvarig för policyn avgör om förändringar av policyn skall ske efter underrättelse till berörda parter inom 90 dagar eller 30 dagar enligt nedan. Administrationsansvarig avgör också om förändringarna är så omfattande att ny policy skall upprättas.

Alla typer av förändringar kan företas i denna policy 90 dagar efter underrättelse.

Mindre förändringar som endast berör ett fåtal kundcertifikatsinnehavare eller Förlitande Parter kan göras 30 dagar efter underrättelse.

8.1.2.1 Underrättelse

Underrättelse om förändringarna sker av Administrationsansvarig inom den tidsperiod som anges i 8.1.1 genom att omedelbart informera om förändringarna på http://eservices.sjofartsverket.se/pki.

Utfärdaren skall så snart som möjligt genom e-post informera kundcertifikatsinnehavare om de förändringar som kan ha reell betydelse för denne.

8.2 PUBLICERING OCH DISTRIBUTION AV POLICY OCH UTFÄRDARDEKLARATION (CPS)

8.2.1 Publicering och distribution av policy

Publicering av aktuell policy och eventuella föreslagna förändringar hålls tillgänglig på http://eservices.sjofartsverket.se/pki.