UTFÄRDARDEKLARATION (CPS) SJÖFARTSVERKET

KUNDCERTIFIKAT

VERSION 1

UTFÄRDARDEKLARATION (CPS)
SJÖFARTSVERKET

KUNDCERTIFIKAT

VERSION 1

Datum: 2006-12-06

SJÖFARTSVERKET

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

Innehållsförteckning

Dokumentstruktur och tolkningar 1

1 INTRODUKTION 2

1.1 ALLMÄNT 2
1.2 IDENTIFIERING 2
1.3 MÅLGRUPP OCH TILLÄMPLIGHET 2
1.3.1 Utfärdare 3
1.3.2 Registration Authorities (ra) 3
1.3.3 Kundcertifikat 3
1.3.4 Tillämplighet 3
1.4 KONTAKTUPPGIFTER 3
1.4.1 Administrationsansvarig 3
1.4.2 Kontaktperson 3
1.4.3 Överensstämmelse mellan denna policy och CPS 4

2 ALLMÄNNA BESTÄMMELSER 4

2.1 ÅTAGANDEN 4
2.1.1 Utfärdarens åtaganden 4
2.1.2 RA:S åtaganden 5
2.1.3 Kundcertifikatsinnehaverens åtaganden 5
2.1.4 Förlitande parts åtaganden 5
2.2 ANSVAR 5
2.2.1 Utfärdarens ansvar 5
2.2.2 Ansvar för RA 5
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 6
2.6.3 Behörighetskontroll 6
2.7 REVISION 7
2.7.1 Utföranden 7
2.7.2 Information om resultatet av revision 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 7
2.8.3 Tillhandahållande av information om anledning till spärrning av kundcertifikat 7
2.8.4 Tillhandahållande av konfidentiell information till polis, åklagare eller annan 7
2.9 IMMATERIELLA RÄTTIGHETER 7
2.10 AVTALSVILLKOR FÖR KUNDCERTIFIKATSINNEHAVARE 7
2.11 TILLGÄNGLIGHET OCH SVARSTID 8

3 IDENTIFIERING OCH AUTENTISERING 8

3.1 INITIAL REGISTRERING 8
3.1.1 Typer av namn 8
3.1.2 Namnsättning 8
3.1.3 Fastställande av sökandens identitet 8
3.2 FÖRNYELSE AV NYCKLAR OCH CERTIFIKAT 8
3.2.1 Förnyelse av nycklar och certifikat 8

3.3 BEGÄRAN OM SPÄRRNING 9

4 OPERATIONELLA KRAV 9

4.1 ANSÖKAN OM KUNDCERTIFIKAT 9
4.2 UTFÄRDANDE AV KUNDCERTIFIKAT 9
4.3 UTLÄMNADE AV KUNDCERTIFIKAT 9
4.4 SPÄRRNING AV KUNDCERTIFIKAT 10
4.4.1 Anledning till spärrning 10
4.4.2 Behörig att begära spärrning 10
4.4.3 Rutin för begäran om spärrning 10
4.4.4 Behandlingstid vid begäran om spärrning 10
4.4.5 Öppettid för spärrtjänsten 10
4.4.6 Periodicitet för utgivning av spärrlista 10
4.4.7 Krav på spärrkontroll 10
4.5 LOGGNING 11
4.5.1 Händelser som loggas 11
4.5.2 Kontroll av loggar 11
4.5.3 Skydd av loggar 11
4.6 ARKIVERING 11
4.6.1 Information som arkiveras 11
4.6.2 Lagringstid 11
4.6.3 Skydd av arkiv 11
4.6.4 Rutiner för åtkomst och verifiering av arkivmaterial 11
4.7 BYTE AV UTFÄRDARNYCKEL 11
4.8 KATASTROFPLAN VID MISSTANKE OM RÖJDA UTFÄRDARNYCKLAR 11
4.9 UPPHÖRANDE AV UTFÄRDARENS VERKSAMHET 12

5 SÄKERHETSKONTROLLER 12

5.1 FYSISK SÄKERHET 12
5.2 PROCEDURORIENTERAD SÄKERHET 12
5.2.1 Betrodda roller inom ca-funktionen 12
5.2.2 Krav på antal personer per uppgift 12
5.2.3 Identifiering och autentisering av personer i betrodda roller 12
5.3 PERSONORIENTERAD SÄKERHET 12
5.3.1 Bakgrund och kvalifikationer 12
5.3.2 Krav på utbildning 13
5.3.3 Personorienterad säkerhet för RA 13

6 TEKNISK SÄKERHET 13

6.1 GENERERING OCH INSTALLATION AV NYCKELPAR 13
6.1.1 Generering av nyckelpar 13
6.1.2 Leverans av kundcertifikat 13
6.1.3 Nyckelstorlek 14
6.1.4 Generering av publik nyckel 14
6.2 SKYDD AV PRIVATA NYCKLAR 14
6.2.1 Säkerhetsmodul och kundcertifikat 14
6.2.2 Flerpersonskontroll av privata nycklar 14
6.2.3 Säkerhetskopiering av privata nycklar 14
6.2.4 Arkivering av privata nycklar 14
6.2.5 Lagring av kundcertifikatens privata nyckel 14
6.2.6 Aktivering av privata nycklar i kundcertifikaten 14
6.2.7 Förstörelse av utfärdarens privata nycklar 14
6.3 ANDRA ASPEKTER PÅ NYCKELHANTERING 14
6.3.1 Arkivering av publika nycklar 15
6.3.2 Privata nycklars livslängd 15
6.3.3 Certifikatens giltighetstid 15
6.4 AKTIVERINGSDATA 15

6.4.1 Generering och installation av aktiveringsdata 15
6.4.2 Skydd av aktiveringsdata 15
6.5 SÄKERHET I DATORSYSTEM 15
6.5.1 Tekniska krav 15
6.6 KONTROLL AV SÄKERHET HOS SYSTEMET UNDER LIVSCYKELN 15
6.6.1 Kontroller av systemutveckling 15
6.6.2 Kontroller av säkerhetsadministration 15
6.7 KONTROLL AV NÄTVERKSSÄKERHET 16

7 PROFILER FÖR CERTIFIKAT OCH SPÄRRLISTOR 16

7.1 CERTIFIKATENS PROFIL OCH VERSION 16
7.2 PROFIL FÖR SPÄRRLISTA 16

8 FÖRVALTNING AV POLICYN 16

8.1 FÖRÄNDRING AV POLICYN 16
8.1.1 Förändringar som kan ske utan underrättelse 16
8.1.2 Förändringar som kan ske med underrättelse 16
8.2 PUBLICERING OCH DISTRIBUTION AV POLICY OCH CPS 17
8.2.1 Publicering och distribution av utfärdardeklaration(CPS) 17

9 REFERENSER 17

Dokumentstruktur och tolkningar

Nedan anges vilken grundstruktur som används för detta dokument samt riktlinjer för hur dokumentet skall tolkas:

- 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

- Strukturen i denna Utfärdardeklaration faller i sin helhet tillbaka på Certifikatpolicyn ”Certifikatpolicy Sjöfartsverket- Kundcertifikat ”

1 INTRODUKTION

1.1 ALLMÄNT

Detta dokument utgör en utfärdardeklaration (CPS) för certifikatpolicyn [Certifikatpolicy Sjöfartsverket Kundcertifikat]. CPS beskriver hur Sjöfartsverket (nedan kallad Utfärdaren) i praktiken som utfärdande CA uppfyller och efterlever de krav som ställts i [Certifikatpolicy Sjöfartsverket –Kundcertifikat].

Dokumentet ägs och förvaltas av Sjöfartsverket.

Utfärdande av kundcertifikat i enlighet med denna Utfärdardeklaration (CPS) innebär att:

- Kundcertifikatet ställs endast ut till fysiska personer i enlighet med [Certifikatpolicy Sjöfartsverket Kundcertifikat],
- CPS beskriver de rutiner och säkerhetsåtgärder som gäller hos Utfärdaren och som säkerställer att kraven i [Certifikatpolicy Sjöfartsverket Kundcertifikat] uppfylls,
- Kundcertifikat ställs ut enligt PKCS#12-standarden,
- CPS förutsätter att Registration Authority (RA) uppfyller de krav som anges för RA-rollen i [Certifikatpolicy Sjöfartsverket Kundcertifikat].

1.2 IDENTIFIERING

Denna utfärdardeklaration (CPS) har en dokumentversion angiven på första sidan (sida 1).

> Namn på detta dokument: Utfärdardeklaration (CPS) Sjöfartsverket – Kundcertifikat
>
> Objektidentifierare för detta dokument: 1.2.752.150.1.2

Denna utfärdardeklaration (CPS) refererar till följande certifikatpolicy och objektidentifierare:

> Namn på policy: Certifikatpolicy Sjöfartsverket - kundcertifikat v1
>
> Objektidentifierare: 1.2.752.150.1.1

OID (för policyn) 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 Utfärdardeklarationen samt dess tillämpningsområde.

1.3.1 Utfärdare

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

1.3.2 Registration Authorities (ra)

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Redovisningsenheten på Sjöfartsverket agerar som RA.

1.3.3 Kundcertifikat

Utöver de i [Certifikatpolicy Sjöfartsverket - Kundcertifikat] beskrivna kundcertifikaten används även speciella CA-certifikat internt med egna RSA-nyckelpar.

Kundcertifikat utfärdas endast till fysiska personer med en anställning hos kunder till Sjöfartsverket.

1.3.4 Tillämplighet

Denna Utfärdardeklaration 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. Bedömningen görs utifrån denna utfärdardeklaration (CPS) och [Certifikatpolicy Sjöfartsverket – Kundcertifikat]

1.3.4.1 Lämpliga användningsområden

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

1.4 KONTAKTUPPGIFTER

1.4.1 Administrationsansvarig

Utfärdardeklarationen är upprättad av Sjöfartsverket (Utfärdaren). Utfärdaren är fullt ansvarig för att administrera och uppdatera denna utfärdardeklaration.

1.4.2 Kontaktperson

Frågor angående utfärdardeklaration 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 CPS

Utfärdaren är ansvarig för granskning av överensstämmelse med policy enligt 2.7 [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2 ALLMÄNNA BESTÄMMELSER

Detta kapitel redogör bestämmelserna för Utfärdaren, RA kundcertifikats-innehavare, och Förlitande Parts åtaganden.

2.1 ÅTAGANDEN

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.1 Utfärdarens åtaganden

2.1.1.1 Allmänna bestämmelser

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.1.2 Beställning av kundcertifikat

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.1.3 Distribution

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.1.4 Skydd av CA-systemets privata nyckel

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.1.5 Begränsningar av användandet av Utfärdarens privata nyckel

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.2 RA:S åtaganden

2.1.2.1 Allmänna bestämmelser

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.3 Kundcertifikatsinnehaverens åtaganden

2.1.3.1 Ansökan om kundcertifikat

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.3.2 Skydd av kundcertifikatsinnehavarens privata nyckel

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.4 Förlitande parts åtaganden

2.1.4.1 Användande av kundcertifikat för lämpliga ändamål

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.1.4.2 Skyldighet att verifiera och kontrollera

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.2 ANSVAR

2.2.1 Utfärdarens ansvar

2.2.1.1 Garantier och ansvarsbegränsningar

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

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

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.3 FINANSIELLT ANSVAR

2.3.1 Fullmaktsförhållanden

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.4 TOLKNING OCH GENOMFÖRANDE

2.4.1 Tillämplig lag

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.4.2 Tvistelösning

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.5 AVGIFTER

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.6 PUBLICERING OCH ÅTKOMST AV INFORMATION

2.6.1 Publicering av information

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Utfärdardeklaration publiceras på följande adress
http://eservices.sjofartsverket.se/pki

2.6.2 Periodicitet för publicering

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.6.3 Behörighetskontroll

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

2.7 REVISION

2.7.1 Utföranden

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.7.2 Information om resultatet av revision

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.8 KONFIDENTIALITET

2.8.1 Typ av information som skall hållas konfidentiell

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.8.2 Typ av information som inte anses vara konfidentiell

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.8.3 Tillhandahållande av information om anledning till spärrning av kundcertifikat

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.8.4 Tillhandahållande av konfidentiell information till polis, åklagare eller annan

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

2.9 IMMATERIELLA RÄTTIGHETER

Utfärdardeklarationen 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 KUNDCERTIFIKATSINNEHAVARE

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Följande villkor gäller för kundcertifikatsinnehavare

- Allmänna villkor för kundcertifikatsinnehavare

De allmänna villkoren kan ingå som en del i andra avtal som Sjöfartsverkets kunder ingår.

2.11 TILLGÄNGLIGHET OCH SVARSTID

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Spärrlistor publiceras inte under annonserade 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.

3.1 INITIAL REGISTRERING

3.1.1 Typer av namn

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

3.1.2 Namnsättning

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

3.1.3 Fastställande av sökandens identitet

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

3.1.3.1 Metod för att styrka sökandens identitet

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

3.1.3.2 Kontroll av identitetsuppgifter

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

3.2 FÖRNYELSE AV NYCKLAR OCH CERTIFIKAT

3.2.1 Förnyelse av nycklar och certifikat

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

3.3 BEGÄRAN OM SPÄRRNING

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

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

Det är endast kunder till Sjöfartsverket som har möjlighet att lämna in en ansökan om kundcertifikat.

4.2 UTFÄRDANDE AV KUNDCERTIFIKAT

Utfärdarprocessen för kundcertifikaten består av följande steg.

Kunden kontakter ansvarig på Sjöfartsverket, om kunden ska tilldelas ett certifikat upprättas ett avtal om detta. Avtalet kan ingå som en del i annat avtal, t ex tillgång till Sjöfartsverkets e-tjänster.

Avtalet signeras av båda parter.

4.3 UTLÄMNADE AV KUNDCERTIFIKAT

Vid utfärdandet genereras följande information:

- Kundcertifikat med privat nyckel enligt PKCS#12 standarden
- Lösenord av god kvalitet som skyddar PKCS#12 filen.

Kundcertifikatet skickas till av kunden angiven E-postadress.

Lösenordet skickat till av kunden angiven mobilnummer med SMS. Har kunden ej angivit mobilnr kan fax alternativt telefon användas.

Leveransen av PKCS#12 filen och lösenordet sker med minst 5 minuters mellanrum.

4.4 SPÄRRNING AV KUNDCERTIFIKAT

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Utfärdarens spärrtjänst nås på följande tider och adresser:

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

Telefon: +46 (0)11 19 15 40

E-post: kundstod@sjofartsverket.se

4.4.1 Anledning till spärrning

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.4.2 Behörig att begära spärrning

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.4.3 Rutin för begäran om spärrning

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.4.4 Behandlingstid vid begäran om spärrning

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Utfärdaren ansvarar inte för förseningar av spärr av kundcertifikat som ligger utan för dennes kontroll.

4.4.5 Öppettid för spärrtjänsten

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Spärrtjänsten är inte tillgänglig under annonserade servicefönster.

4.4.6 Periodicitet för utgivning av spärrlista

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.4.7 Krav på spärrkontroll

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.5 LOGGNING

Här specificeras rutiner för loggning av händelser samt därtill relaterad revision 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 enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.5.2 Kontroll av loggar

Loggar från CA-systemet granskas av ISSO en gång per vecka. Larmrutiner finns implementerade för följande typer av loggar.

4.5.3 Skydd av loggar

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.6 ARKIVERING

4.6.1 Information som arkiveras

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.6.2 Lagringstid

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.6.3 Skydd av arkiv

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.6.4 Rutiner för åtkomst och verifiering av arkivmaterial

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.7 BYTE AV UTFÄRDARNYCKEL

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.8 KATASTROFPLAN VID MISSTANKE OM RÖJDA UTFÄRDARNYCKLAR

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

4.9 UPPHÖRANDE AV UTFÄRDARENS VERKSAMHET

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

5 SÄKERHETSKONTROLLER

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

5.1 FYSISK SÄKERHET

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

5.2 PROCEDURORIENTERAD SÄKERHET

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

5.2.1 Betrodda roller inom ca-funktionen

Angivna roller i [Certifikatpolicy Sjöfartsverket - Kundcertifikat] är implementerade i Utfärdarens verksamhet.

5.2.2 Krav på antal personer per uppgift

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

5.2.3 Identifiering och autentisering av personer i betrodda roller

SA-rollen identifieras endast av operativsystemet för CA-systemet

CAA identifieras i de applikationer (webgränssnitt) som ansluter till CA: ns gränssnitt för certifikatsbegäran.

Applikationen har ett certifikat för att identifiera sig mot CA: ns gränssnitt.

Applikationen identifierar operatören via Trusted Autentication. CAAs anslutningar till CA-tjänsten loggas i anslutande applikation.

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.

De initiala kontrollerna som genomförs vid anställning hos Sjöfartsverket tillsammans med relevanta kunskaper är tillräckliga kvalifikationer.

5.3.2 Krav på utbildning

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Utfärdaren genomför regelbundet utbildningar om säkerhet och CA-systemet för personalen.

Säkerhetsrutiner kring CA-systemet testas årligen i verklighetsrelaterade simuleringar.

5.3.3 Personorienterad säkerhet för RA

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Inga avtal finns tecknade med externa 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

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.1.1.1 Utfärdarnycklar för signering av certifikat och spärrlistor

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.1.1.2 Nyckelpar för kundcertifikatsinnehavare

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.1.2 Leverans av kundcertifikat

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

Kundcertifikatsinnehavaren instrueras i de allmänna villkoren att byta initialt lösenord till ett personligt.

Leverans av kundcertifikaten sker till kontaktpersonens angivna e-postadress i certifikatsansökan.

6.1.3 Nyckelstorlek

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.1.4 Generering av publik nyckel

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.2 SKYDD AV PRIVATA NYCKLAR

6.2.1 Säkerhetsmodul och kundcertifikat

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.2.2 Flerpersonskontroll av privata nycklar

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.2.3 Säkerhetskopiering av privata nycklar

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.2.4 Arkivering av privata nycklar

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.2.5 Lagring av kundcertifikatens privata nyckel

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.2.6 Aktivering av privata nycklar i kundcertifikaten

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.2.7 Förstörelse av utfärdarens privata nycklar

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.3 ANDRA ASPEKTER PÅ NYCKELHANTERING

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.3.1 Arkivering av publika nycklar

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.3.2 Privata nycklars livslängd

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.3.3 Certifikatens giltighetstid

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.4 AKTIVERINGSDATA

6.4.1 Generering och installation av aktiveringsdata

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.4.2 Skydd av aktiveringsdata

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.5 SÄKERHET I DATORSYSTEM

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.5.1 Tekniska krav

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.6 KONTROLL AV SÄKERHET HOS SYSTEMET UNDER LIVSCYKELN

6.6.1 Kontroller av systemutveckling

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.6.2 Kontroller av säkerhetsadministration

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

6.7 KONTROLL AV NÄTVERKSSÄKERHET

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

7 PROFILER FÖR CERTIFIKAT OCH SPÄRRLISTOR

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

7.1 CERTIFIKATENS PROFIL OCH VERSION

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

7.2 PROFIL FÖR SPÄRRLISTA

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

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

Samtliga förändringar av denna utfärdardeklaration (CPS) för att uppfylla krav i [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

8.1.2 Förändringar som kan ske med underrättelse

Samtliga förändringar av denna utfärdardeklaration (CPS) för att uppfylla krav i [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

8.1.2.1 Underrättelse

I enlighet med [Certifikatpolicy Sjöfartsverket - Kundcertifikat].

8.2 PUBLICERING OCH DISTRIBUTION AV POLICY OCH CPS

8.2.1 Publicering och distribution av utfärdardeklaration(CPS)

Publicering av aktuell utfärdardeklaration (CPS) och eventuella föreslagna förändringar hålls tillgänglig på http://eservices.sjofartsverket.se/pki

Denna Utfärdardeklaration (CPS) kan även erhållas från adminstrationsansvarig kontaktperson se 1.4.2.

9 REFERENSER

[Certifikatpolicy Sjöfartsverket - Kundcertifikat]

Certifikatpolicy för vilken denna utfärdardeklaration (CPS) är upprättad. Aktuell version finns publicerad på
http://eservices.sjofartsverket.se/PKI/policykundcert.v1.pdf