Certificate Policy
for OCES personal certificates
(Public Certificates
for Electronic Services)

Contents

Rights

Preface

This certificate policy is a translation of the Danish version of the certificate policy issued and administered by the Danish National IT and Telecom Agency. In case of doubt as to the understanding and interpretation of the certificate policy, the original Danish version takes precedence.

The National IT and Telecom Agency is the public authority which authorises the issue of OCES personal certificates for the selected certification authorities (CAs), and which is in charge of the approval of the CAs in accordance with this CP.

The National IT and Telecom Agency also holds the responsibility for the contents of this CP. The most recent version of this CP as well as earlier versions, according to which valid certificates exist, can be found at www.signatursekretariatet.dk.
Please direct inquiries regarding digital signatures to the National IT and Telecom Agency. For further information, please go to www.digitalsignatur.dk.

Introduction

A digital signature is an electronic signature which may be used, for example, in situations where it is important to know who you are communicating with electronically. The use of digital signature presupposes the establishment of a public key infrastructure (PKI).

The OCES is such a public key infrastructure. OCES is the Danish designation for Public Certificates for Electronic Services ("Offentlige Certifikater til Elektronisk Service"). The National IT and Telecom Agency has prepared three OCES certificate policies (CPs): One for personal, employee and company certificates, respectively. The CPs constitute a common public standard which regulates the issue and use of the digital OCES signature. The CPs thereby set down requirements to the public key infrastructure, and consequently the level of security applied for the digital signature.

The digital signature can be used when a person has been identified and registered with a certification authority (CA). The CA grants the individual a personal electronic certificate, which contains this individual's public key. In addition, the CA ensures that the required software, including the private key, can be installed on the individual's PC. The CP stipulates requirements as to how and under which circumstances the CA is to perform such tasks.

In addition, qualified certificates exist that have been issued in pursuance of Act no. 417 of 31 May 2000 on Electronic Signatures. A qualified certificate is not based on the above-mentioned common public standard. Among other things, personal attendance is required when issuing a qualified certificate.

1 Overview and scope

This certificate policy (CP) describes the guidelines that apply to the issue of an OCES personal certificate, where OCES is the abbreviation for "Offentlige Certifikater til Elektronisk Service" (Public Certificates for Electronic Services).

This CP has been prepared on the basis of the guidelines that appear in ETSI TS 102 042 v 1.2.1. (2005-05): *"Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*

A personal certificate guarantees that the subscriber has the identity that appears from the certificate.

A certificate is only an OCES certificate if it has both been issued according to an OCES CP and has been issued by a certification authority (CA), which has been approved by the National IT and Telecom Agency as an issuing authority of OCES certificates.

A CP forms part of the contractual basis that exists between the National IT and Telecom Agency and the individual certification authority (CA) regarding the right to issue OCES certificates.

The CP lays out a number of conditions that the CA must meet in order to achieve and maintain the right to issue OCES certificates.

Thus, the basic principle governing the CP is that the public authority that holds the main responsibility for the field in question, i.e. the National IT and Telecom Agency, prepares it. The CP specifies the Agency's minimum requirements to systems and agreements, which the certification authorities (CAs), acting as commercial providers of certificates, must meet in relation to their "customers", i.e. subscribers and verifiers (relying parties). Thus, the certificate policy ensures that the signatures can be applied in a manner that is secure for all parties.

This CP doesn't specify requirements regarding cross certification and independent time stamping.

2 References

The reader's attention is directed to the current regulations:

ACT no. 417 of 31/05/2000: *Lov om elektroniske signaturer (Act on Electronic Signatures)*

ACT no. 429 of 31/05/2000: *Lov om behandling af personoplysninger (Act on Processing of Personal Data)*

CEN Workshop Agreement 14167-2:2002: *"Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – part 2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)*"

DS (Danish Standard) 2391:1995 *"Registrering af identifikatorer i datanetværk" (Registration of identifiers in data networks)*, parts 1 and 3

DS (Danish Standard) 844: *"Specifikation for kvalificerede certifikater" (Specification for qualified certificates)*

ETSI TS 102 042 v 1.2.1. (2005-05): *"Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*

ETSI SR 002 176 v 1.1.1. (2003-03): *"Algorithms and Parameters for Secure Electronic Signatures"*

FIPS PUB 140-1: "*Security Requirements for Cryptographic Modules*"

ISO/IEC 15408 (parts 1 to 3): "*Information technology - Security techniques - Evaluation criteria for IT security*"

ISO/IEC 9794-8/ITU-T Recommendation X.509: "*Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*"

In case of discrepancy between technical documents or standards and this CP, the provisions of this CP shall be applicable to the CA.

3 Definitions and abbreviations

3.1 Definitions

This section contains definitions of specific terms used in this CP. Danish terms are given in parenthesis.

certificate policy ("certifikatpolitik"): A set of rules specifying the requirements to the issue and use of a certificate in one or several specific connections where common security requirements exist.

certificate Revocation List ("spærreliste"): A list of certificates, which are no longer considered valid because they have been permanently revoked.

certification authority – CA ("certificeringscenter"): A physical or legal person, who has been authorised to generate, sign and issue certificates.[1]

certification practice statement – CPS ("certificeringspraksis"): A specification of the principles and procedures that a CA applies when issuing certificates.

cryptographic module: Hardware module which can generate and store keys and apply the digital signature independently of the operating system.

digital signature: Data in electronic form, which is attached to or logically associated with other electronic data and which serves as a method of authentication of that data.

public key certificate/certificate ("certifikat"): An electronic certificate, which specifies the subscriber's public key together with additional information, and which unambiguously links the public key to the identification of the subscriber. A public key certificate must be signed by a certification authority (CA), which thus confirms the validity of the certificate.

registration authority – RA ("registreringsenhed"): The physical or legal person, who is responsible for the identification and authentication of a (future) subscriber.

root certificate ("rodcertifikat"): A certificate issued by a CA, which is to be used for the validation of other certificates. A root certificate is signed with its own signing key (self signing ("egensignering")).

root key: The root certificate's signing key (private key).

[1] The term "key centre" is used for this entity in Act on Electronic Signatures. However, the terminology has been changed for practical reasons. A certification authority corresponds to a key centre in Act on Electronic Signatures apart from the fact that the certification authority does not issue qualified certificates, but OCES certificates.

subscriber ("certifikatindehaver"): A physical person, who enters into an agreement with the issuing certification authority (CA), and to whom an OCES certificate is being or has been issued.

verifier (**relying party**) ("signaturmodtager"): A physical or legal person, who receives signed data from a subscriber.

3.2 Abbreviations

CA Certificate Authority ("Certificeringscenter")
CRL Certificate Revocation List ("Spærreliste")
CPR The Central Office of Civil Registration ("Det Centrale Personregister")
CPS Certification Practice Statement ("Certificeringspraksis")
CP Certificate Policy ("Certifikatpolitik")
LDAP Lightweight Directory Access Protocol
OCES Public Certificates for Electronic Services ("Offentlige Certifikater til Elektronisk Service")
OCSP Online Certificate Status Protocol
PID Person-specific Identification Number ("Personspecifikt Identifikationsnummer")
PKI Public Key Infrastructure
RA Registration Authority
UTC Universal Time Coordinate

3.3 Notation

The requirements contained in this CP include:

1. Compulsory requirements, which must be met. Such requirements are stipulated using the term "must".
2. Requirements, which should be met. Non-fulfilment of such requirements must be reasoned. Such requirements are stipulated using the term "should".
3. Requirements, which may be met, provided that the CA so wishes. Such requirements are stipulated using the term "may".

4 Concept

A public key infrastructure (PKI) is used for the exchange of information between two parties on the Internet where a common, trusted third party guarantees the signer's identity. A certificate policy describes the relationship that exists between these three parties.

As stated in section 1, the basic principle of the certificate policy is that the public authority that holds the main responsibility for the field in question, i.e. the National IT and Telecom Agency, prepares it. The certificate policy specifies the Agency's minimum requirements to the systems and agreements, which the certification authorities (CAs), acting as the commercial providers of the certificates, must meet in relation to their "customers", i.e. subscribers and verifiers. The purpose of the certificate policy is to ensure that the signatures can be applied in a manner that is secure for all parties. Thus, the subscribers and verifiers (relying parties) should be able to base their trust on the fact that the CAs have been approved by the National IT and Telecom Agency.

4.1 CA

A certification authority (CA) is a physical or legal person, who has been entrusted – by both subscribers and verifiers – with the task of issuing, signing and administering electronic certificates. The CA holds the overall responsibility for the provision of services that are necessary to issue and maintain certificates. The CA's own private keys are used to sign issued certificates, and the CA is identified as the issuer in the certificate.

The CA may cooperate with other parties in order to offer the necessary services; however, the CA will always hold the overall responsibility for all actions regarding the handling of certificates, and the CA is responsible for always meeting the requirements governing the CAs' services as specified in this CP.

An OCES CA is at the top of the trust hierarchy. Therefore, OCES certificates will be signed with a signing key, which has been self signed, i.e. the root key in this trust hierarchy.

4.2 CA services

The services required to issue and maintain certificates may be divided into the following groups:

- Registration: Verification of the subscriber's identity and other attributes, if any. The result of the registration will be passed on to the certificate generation
- Certificate generation: Generation and electronic signing of certificates based on the registered, verified identity and other attributes, if any
- Certificate distribution: Distribution of certificates to the subscriber

- Catalogue service: Publication of certificates, giving verifiers (relying parties) access to the certificates
- Publication of business terms: Publication of terms and rules, including CP and CPS
- Certificate revocation: Reception and handling of requests for revocation of certificates
- Publication of revocation information: Publication of status information for all certificates, in particular certificates which have been revoked. It is a requirement that this be updated on a real time basis.

4.3 CP and CPS

4.3.1 Purpose

The purpose of a CP like this one is to specify the requirements, which must be met, while the purpose of a CPS is to specify how the requirements are met at the individual CA. The certificate refers to the CP, thus allowing a verifier to determine which minimum requirements have been met via the CA's CPS.

4.3.2 Degree of specification

A CP is less specific than a CPS, as the CPS specifies the detailed description of conditions and terms, including business procedures and operating procedures for the issue and maintenance of certificates.

The CPS specifies how a specific CA meets the technical, organisational and procedural requirements identified in this CP.

4.3.3 Differences

As a result, the CP and CPS take a different approach. A CP, like this one, has been defined independently of specific details that apply to the operating environments at the CA, whereas the CPS is tailored to the organisational structure, operating processes and IT facilities that apply at the CA. The National IT and Telecom Agency has prepared this CP, while the CPS is always prepared by a CA.

As a CPS contains business-sensitive information, the entire CPS may not be accessible to the general public. An independent third party (systems auditor) must make an audit of the CPS and must declare that the CPS meets all requirements made in the CP, and that the CA observes such requirements.

4.3.4 Other CA conditions

In addition to the CP and the CPS, a CA will typically lay out other terms and conditions. Such terms and conditions will normally include any commercial terms and conditions, according to which the CA issues certificates and makes status information available.

5 Introduction to certificate policy

5.1 General

This document describes the certificate policy that governs OCES personal certificates.

5.2 Identification

This CP is identified by the following object identifier (OID):

Personal certificate:

{ 1 2 208 stat(169) pki(1) cp(1) nq(1) person(1) ver(3) }.

The OID is registered with the Danish Standards Association in accordance with DS 2391:1995, parts 1 and 3.

All OCES personal certificates issued according to this CP must refer to this CP by indicating the relevant OID in the "certificate policy" field of the OCES certificate. Reference must only be made to the mentioned OIDs following written agreement with the National IT and Telecom Agency.

5.3 Field of use

An OCES personal certificate may be used to secure the authenticity of the sender and message, including the electronic signature and integrity of the message. It may also be used to ensure secrecy (encryption).

OCES personal certificates are not qualified certificates, i.e. they must not be used in situations, which require the use of qualified certificates.

OCES personal certificates must not be used to sign other certificates.

OCES personal certificates may be valid for a maximum period of four years.

5.4 CA's right to issue OCES certificates

The CA may issue OCES personal certificates in accordance with this version of the CP, provided that the CA

- has concluded a written agreement with the National IT and Telecom Agency in this respect, and
- has submitted a report, cf. section 7.1, to the National IT and Telecom Agency containing a declaration from an external systems auditor. The auditor's statement must show that the CA meets all requirements laid out in this CP, and that the CA has implemented control measures that are necessary to comply with the requirements governing operation and security at any time, and

- has received a declaration of conformity from the National IT and Telecom Agency, which confirms that the National IT and Telecom Agency has approved the submitted report and considers the requirements in this CP to have been met.

6 Obligations and liability

6.1 CA obligations

The CA must ensure that all requirements, as specified in section 7, have been implemented.

Certification authorities (CAs), which are entitled to issue certificates in accordance with this CP (OCES personal certificates), are published on the National IT and Telecom Agency's web site: https://www.signatursekretariatet.dk.

There is no requirement for cross certification between these authorities.

The CA must ensure that all aspects are attended to in connection with the following activities:

- distribution of root certificates
- instructions on how to generate and store keys
- distribution of OCES personal certificates to subscribers
- revocation of OCES personal certificates upon request
- publication of revocation lists
- informing subscribers about impending expiry of certificates and possible renewal of key pairs
- renewal of OCES personal certificates

The CA must maintain a technical operating environment, which meets the security requirements, set out in this CP.

The CA must prepare a CPS that addresses all requirements made in this CP. The CPS must comply with this CP.

The CA must submit to audit requirements, cf. this CP.

The registration authority (RA) may either be closely affiliated with the CA, or may be an independent function. In any circumstance, the CA is responsible for ensuring that the RA complies with the same requirements and obligations that the CA itself is required to comply with.

The CA must ensure that the affiliated RA/RAs follow(s) the rules that are set out in this CP.

In addition, the CA must ensure that the RA:

- sets up web access for registration procedures (may form part of the CA's web service, if the RA is an integral part of the CA);
- verifies the applicant's identity and details; and
- maintains a technical operating environment that meets the requirements laid out in this CP.

6.2 Subscriber obligations

The CA must conclude an agreement with the subscriber, obliging him/her to fulfil the following conditions:

- to give satisfactory and correct answers to all requests for information made by the CA (or RA) during the application process;
- to generate, store and use the key pair as directed by the CA. The private key may be kept on a hard disk, diskette or similar device;
- to take reasonable steps in order to protect the private key from being compromised, altered, lost or subjected to unauthorised use;
- to protect the private key with an activation code consisting of a minimum of eight characters and containing at least one small letter, one capital letter and one digit;
- use of a different activation code, e.g. biometric, must have a complexity of at least 128 bit;
- activation codes used in environments, which can effectively block against exhaustive searches may, however, consist of a minimum of four digits;
- to protect the activation code so that nobody can learn about it;
- to ensure that a back-up copy of the private key, if any, is kept in an encrypted form in a secure manner;
- to ensure, when receiving the OCES certificate, that the contents of the OCES certificate are in accordance with the real situation;
- only to use the OCES certificate and the related private keys in accordance with the provisions of this CP;
- immediately to request the issuing CA to revoke the OCES certificate if the private key is compromised or if it is suspected that it has been compromised; and
- to immediately request a renewal of the certificate if the contents of the OCES certificate are no longer in agreement with the real situation.

In addition, the CA must inform the subscriber that the private key is considered to have been compromised and must be revoked if any third party learns about the activation code.

6.3 Information to verifiers (relying parties)

Via its web site among other ways, the CA must inform verifiers of the terms and conditions that apply to the use of a digital signature, including that in order to rely on a certificate, the verifier must ensure:

- that the certificate received is valid and has not been revoked, i.e. it is not listed in the CA's revocation list;
- that the purpose for which the certificate is to be used is appropriate in relation to the limitation of the usage indicated in the OCES certificate, and
- that the use of the certificate is in every other respect appropriate in relation to the level of security described in this CP.

6.4 Liability

In relation to any person who reasonably relies on the certificate, the CA must assume liability for damages in relation to the general provisions of Danish law.

In addition, the CA must assume liability for damages for loss incurred by subscribers and verifiers who have reasonably relied on the certificate, provided that the loss is due to one of the following:

- that the information specified in the certificate was incorrect at the time of issuing the certificate;
- that the certificate does not contain all information as required by section 7.3.3;
- failure to revoke the certificate, cf. section 7.3.6;
- lacking or erroneous information relating to the revocation of the certificate, the expiry date of the certificate or whether the certificate is subject to limitation of purpose or amount, cf. sections 7.3.3 and 7.3.6, or
- disregard of section 7.3.1

unless the CA can prove that the CA has not acted negligently or intentionally.

The CA prepares its own agreements etc. with its contracting parties. The CA is entitled to attempt to limit its liability in the relationship that exists between the CA and its contracting parties to the extent that such joint contracting parties are business operators or public authorities. Thus, the CA is not entitled to attempt to limit its liability in relation to private citizens who are contracting parties.

In addition, the CA is entitled to deny liability in relation to contracting parties who are business operators and public authorities for loss as described in s. 11 (3) in Act no. 417 of 31 May 2000.

Insurance

The CA must take out and maintain an insurance to cover any claims for damages made against the CA and RA by all contracting parties (subscribers and verifiers, relying parties) and the National IT and Telecom Agency. The minimum annual coverage must be 2 million Danish kroner.

7 CA practice requirements

7.1 Certification practice statement (CPS)

The CA must prepare a certification practice statement (CPS) containing a detailed description of how the requirements of this CP are met, including:

- CA administrative and managerial procedures;
- qualifications, experience etc. of CA staff;
- systems and products used by the CA;
- CA security measures and related work process, including information about measures applied in connection with maintaining and protecting the certificates as long as they exist;
- CA procedures in relation to registration (identity control), issue of certificates, catalogue and revocation services, and registration and storage of information relating to certificates, including identity information;
- CA financial resources;
- CA procedures concerning the entering into agreements relating to the issue of certificates and its notification duty,
- to the extent that the CA has outsourced CA tasks to other companies or authorities, the CPS must also encompass the performance of such tasks.

CA practices must always comply with the conditions specified in the CPS.

Approval and ongoing audit

In order to issue OCES personal certificates, a CA must enter into a written agreement with the National IT and Telecom Agency.

Once the agreement has been signed, the CA must prepare and submit a report to the National IT and Telecom Agency. The report must be approved by the National IT and Telecom Agency and must include the following information:

- the CA's CPS;
- the audit protocol;
- a declaration from the CA's management as to whether the CA's data, system and operating security as a whole is to be considered secure, and that the CA complies with its own CPS;
- a declaration from the systems auditor as to whether the CA's data, system and operating security as a whole is to be considered secure, and whether the CA complies with its own CPS, and
- documentary proof that a professional indemnity insurance that covers the CA liability exists.

The report must subsequently be submitted annually to the National Telecom and IT Agency no later than three months after the end of the CA's fiscal year. The timeframe of the report must follow the CA's fiscal year.

Systems audit
Systems audits must be performed at the CA. Systems audits include audits of the following:

- general IT reviews in the company;
- computer-based user systems etc. for the generation of keys and key components as well as the registration, issue, verification, storage and revocation of certificates;
- computer systems for the exchange of data with other parties.

Appointment of systems auditor – auditor's authorities and obligations
The CA must appoint an external state-authorised auditor to perform the systems audit at the CA. In special cases, the National IT and Telecom Agency may grant an exemption from the requirement that the systems auditor must be a state-authorised auditor. Within one month after the appointment of the systems auditor, the CA must inform the National IT and Telecom Agency hereof.

The CA must hand out information necessary to perform the systems audit at the CA. The CA must grant the appointed systems auditor access to the management protocol.

The CA must grant the appointed systems auditor access to management meetings when discussing cases that are of importance to the systems audit. A management meeting is understood as a meeting held among the senior management of the CA, in practice often a board meeting. In this connection, the term "CA's management" is understood as the senior management of the CA, i.e. the board or a similar management body, depending on the organisation of the CA. If any one board member so requires, the CA must ensure that the appointed systems auditor takes part in the management's discussion of matters relevant to the systems audit.

In CAs where general meetings are held, the stipulations of the Danish Financial Statements Act regarding the auditor's obligation to reply to questions posed at a company's general meeting shall also apply to the appointed systems auditor.
The CA must inform the appointed systems auditor that, in accordance with generally accepted auditing standards, the systems auditor must perform the systems audit mentioned below, including checks to ensure the following:

- that CA systems comply with the requirements made in this CP;
- that CA security, control and auditing requirements are considered adequate for the development, maintenance and operation of CA systems, and
- that CA procedures, both computerised and manual, are secure in terms of security and control, and that they comply with the CA certification practice statement (CPS).

The CA must ensure that a vulnerability assessment of the logging procedure is performed as part of the systems audit.

The appointed systems auditor may cooperate with the CA internal auditing team, if one exists.

To the extent that the appointed systems auditor finds significant weaknesses or irregularities, the CA management must discuss the matter at the next management meeting.

The CA must inform the appointed systems auditor that the auditor is under obligation to report the matter(s) to the National IT and Telecom Agency, provided that the systems auditor continues to find significant weaknesses or irregularities. In addition, the CA must inform the systems auditor that, upon inquiry from the National IT and Telecom Agency, the auditor is obliged to provide information about matters at the CA, which have or may have an influence on the CA management of the task of issuing OCES certificates, and must provide this information without obtaining prior acceptance from the CA. The systems auditor is, however, obliged to inform the CA about the inquiry.

The CA and the systems auditor must inform the National IT and Telecom Agency without delay about matters of significant consequence for the continued activities of the CA.

Auditor's records
The CA must inform the appointed systems auditor that the auditor must continuously keep separate auditor's records, which are to be presented at each management meeting, and that each addition to the records must be signed by the CA management and the appointed systems auditor.
In addition, the CA must inform the systems auditor that the contents of the records must be specified as indicated below.

The appointed systems auditor's records must include a report of the systems audit performed as well as its conclusions. Also, any matter, which may have given rise to significant comments, must be accounted for.
The records prepared by the appointed systems auditor must also indicate whether the systems auditor has received all the information requested while performing the task.
At the end of the CA fiscal year, the appointed systems auditor must prepare a protocol for the CA management.
The protocol must include declarations as to whether

- the systems audit has been performed in accordance with generally accepted auditing standards;
- the appointed systems auditor meets the qualification requirements as required by legislation;
- the appointed systems auditor has received all information requested;
- the specified systems audit tasks have been performed in accordance with the requirements laid out in this CP, and
- the data, system and operating security as a whole is considered satisfactory.

The National IT and Telecom Agency may direct the CA to appoint a different systems auditor within a stipulated time, in case the acting systems auditor is found to be obviously unqualified to perform the auditor's duty.

In case of a change of auditors, the CA and the resigned systems auditor(s) must each provide the National IT and Telecom Agency with a statement.

Expenses related to systems audits
The CA must bear all expenses incurred in relation with systems audits, including systems audits ordered by the National IT and Telecom Agency.

7.2 Key management

The CA key management must be in accordance with ETSI SR 002 176 v 1.1.1. (2003-03): *"Algorithms and Parameters for Secure Electronic Signatures"*, defining a list of recognised cryptographic algorithms and their parameter requirements.

7.2.1 CA key generation
CA root keys and other private keys must be generated under the surveillance of two persons each holding a trusted position at the CA.

CA private keys must be generated in a cryptographic module that meets the requirements identified in FIPS 140-1 level 3, CWA 14167-2, or higher. The cryptographic module must be stored in accordance with the requirements specified in section 7.4.4.

If CA root keys or other private keys are to be transferred from the cryptographic module, such transfer must be performed in an encrypted form and in cooperation by at least two persons holding different trusted positions at the CA.

CA root keys must be RSA keys of a minimum length of 2,048 bit or similar. CA root keys must be valid for a minimum of five years.

The "OCES" designation must form part of the root certificate's Common Name.

7.2.2 CA key storage, back-up and recovery
The CA must ensure that CA root keys are not compromised and always maintain their integrity.

Storage, back-up and transport of CA root keys and other private keys must be made under the surveillance of two persons each holding a trusted position at the CA.

CA root keys and other private keys must be stored and used in cryptographic modules, which comply with FIPS140-1 level 3 or higher, or CWA 14167-2.

Back-up copies of CA private keys must be stored in a cryptographic module that complies with the requirements laid out in FIPS 140-1 level 3 or higher, or CWA

14167-2. The cryptographic module must be stored in accordance with the requirements specified in section 7.4.4.

7.2.3 CA public key distribution

The CA root certificate must be made available for verifiers (relying parties) via web access with TLS/SSL communication. Verification of the root certificate fingerprint (a control value) must be made via a different channel.

7.2.4 Key storage and recovery

The CA must ensure that the subscriber's private keys that are used for sender and message authentication (signing), including electronic signature and message integrity, are not stored and cannot be recovered at the CA.

The CA must ensure that the subscriber's private keys that are used for ensuring secrecy (encryption) are not stored and cannot be recreated at the CA without the subscriber's consent.

The CA must ensure that no such consent is required on the part of the subscriber as a precondition for issuing OCES personal certificates.

The CA must ensure that the procedure for handing over stored or recovered keys is agreed upon at the same time as the subscriber consents to storage and/or recovery.

7.2.5 CA key usage

The CA must ensure that the CA private keys are not being used for any other purpose than signing certificates and providing status information about certificates.

The CA must ensure that certificate signing keys are only used in physically secured facilities in accordance with section 7.4.4.

7.2.6 End of CA key life cycle

The CA private key must have a fixed period of validity. Upon expiry the private key must either be destroyed in such a manner that it cannot be recovered, or stored in such a manner that it cannot be put to use again.

Before the private key expires, the CA must ensure generation of a new CA key pair to be used for the issue of subsequent certificates.

7.2.7 Management of cryptographic modules

The CA must manage and store cryptographic modules in accordance with the requirements specified in section 7.4 during the entire life cycle of the cryptographic modules.

The CA must ensure that cryptographic modules for certificate and status information signing have not been compromised prior to installation.

The CA must ensure that cryptographic modules for certificate and status information signing are not compromised during use.

The CA must ensure that all management of cryptographic modules for certificate and status information signing is performed in cooperation by a minimum of two persons each holding a trusted position at the CA.

The CA must ensure that cryptographic modules for certificate and status information signing are always functioning correctly.
The CA must ensure that keys stored in a cryptographic module for certificate and status information signing are destroyed upon device retirement.

7.2.8 CA Generated subscriber keys

The CA must ensure that CA generated subscriber keys, are generated securely, and that the secrecy of the subscriber's private keys is assured.

- CA-generated subscriber keys must be RSA keys of a minimum length of 1,024 bit or similar;
- CA generated subscriber keys must be generated and stored securely prior to delivery to the subscriber;
- The subscriber's keys must be delivered in such a manner that the secrecy of the keys is not compromised;
- If a copy of the subscriber's keys is not required to be kept by the CA, cf. section 7.2.4, once delivered to the subscriber, the private key must be maintained under the subscriber's sole control. Any copies of the subscriber's keys held by the CA must be destroyed.

7.3 Certificate management

7.3.1 Subscriber registration

Prior to the issue of an OCES personal certificate, the CA must ensure that, the subscriber is made aware of and accepts the terms and conditions that apply to the use of the certificate.

Physical presence is not required when issuing an OCES personal certificate.

The CA must establish a procedure for the verification of the applicant's identity to ensure that:

- the subscriber states his/her civil registration number and postal code;
- the OCES subscriber's name and national register address is collected by means of an on-line look-up in the Danish Civil Registration System as part of the registration process;
- the OCES subscriber is provided with a single-use code sent in a pin code letter to the national register address.

In the event that the CA is already familiar with the subscriber's identity or applies other secure procedures for carrying out identity checks, the above-mentioned procedure for certificate application may be partly or fully deviated from.

Generating and installing subscriber keys

The CA must establish an installation procedure, which technically ensures that

- the subscriber must enter his/her single-use code to start the installation of the private key and related certificate;
- key pairs are generated with the subscriber
- subscriber keys are RSA keys with a minimum length of 1,024 bit or similar;
- the public key is transferred to the CA together with information in a message that has been signed by the private key;
- the private key is encrypted and protected by an activation code;
- the activation code for activating the private key is generated and entered during key generation;
- the private key is activated once the subscriber has specified an activation code consisting of a minimum of eight characters and containing at least one small letter, one capital letter and one digit;
- the use of a different activation code, e.g. biometric, must have a complexity of at least 128 bit;
- activation codes used in environments, which can effectively block against exhaustive searches may, however, consist of a minimum of four digits;
- the root certificate has been installed with the subscriber;
- the root certificate may be verified via a different channel, and
- the time and date of the issue of the certificate can subsequently be determined.

In the event that subscriber keys are generated by the CA, cf. section 7.2.8, the CA must establish a procedure for transfer and installation which technically ensures that

- the private key is encrypted and protected by the activation code;
- the private key and activation code are delivered separately to the subscriber;
- the private key is only activated once the subscriber has specified an activation code consisting of a minimum of eight characters and containing at least one small letter, one capital letter and one digit;
- the use of a different activation code, e.g. biometric, must have a complexity of at least 128 bit;
- activation codes used in environments, which can effectively block against exhaustive searches may, however, consist of a minimum of four digits;
- the root certificate may be verified via a different channel, and
- the time and date of the issue of the certificate can subsequently be determined.

The CA must support the generation and storage of keys by means of hardware.
The CA must indicate to the subscriber cryptographic modules for this purpose. No specific requirements have been specified regarding cryptographic modules for OCES subscribers.

Upon request, the CA must, if possible, provide the subscriber with a method to back-up the private key, if relevant, ensuring that it is stored in an encrypted form in a secure manner.

The RA must approve a certificate application if:

- the procedure is carried out as specified;
- it is possible to verify the applicant via on-line look-up with the Danish Civil Registration System, and
- the applicant enters a correct single-use code within a maximum of five attempts.

The CA must ensure that within a running month, from the time at which an RA has received a certificate application and until the information required for the issue of the certificate has been sent to the certificate applicant, no more than an average of one working day should pass, however a maximum of three working days is accepted. If the certificate applicant's address cannot be obtained by accessing the Civil Registration System, a maximum of five working days may pass before the information required for the issue should be sent.

7.3.2 Certificate Renewal

Renewal of an OCES certificate means issuing of a new certificate to the same subscriber as in the existing certificate, however with a new key, new validity period, a new certificate serial number and the current OID. An OCES certificate may be renewed for four years at a time.

Upon subscriber request and following proper identification, a certificate can be renewed only if the keys validity period has not expired and if the private key has not been compromised.

The CA must ensure that the request for renewal is signed using the subscriber's private key.

The CA must accept the proof of holding the private key belonging to the existing certificate as being adequate authentication in cases where a certificate is to be renewed. Thus, the RA must ensure that the subscriber possesses the private key that corresponds to the public key, which is presented in the certificate application. Verification is considered adequate if the subscriber signs the certificate application with his/her private key. The verifying RA must validate the signature using the public key, which was provided in the certificate application.

Certificate application and issue must meet the requirements specified in section 7.3.1 regarding subscriber key generation and installation, except for the sending of the single-use code which in relation to renewal, is replaced by validation with the existing certificate.

A certificate cannot be renewed following revocation or expiry, or if the private key has been compromised. In such cases, the CA must ensure that a new certificate can be issued with a new key, and that the request for a new OCES certificate in such cases is handled like a new issue following the same guidelines as specified in section 7.3.1.

No later than 14 days before expiry, the CA must notify the subscriber hereof via email sent to the email address indicated in the certificate or to the national register address.

The CA must ensure that the request for and issue of a renewed OCES certificate can be made on-line.

7.3.3 Generating certificates

OCES personal certificates must follow DS 844: Specification for qualified certificates ("Specifikation for kvalificerede certifikater"). QcStatements, however, must not state that the certificate is a qualified certificate.

OCES personal certificates must include:	***Solution***
Identification of the issuing CA and the country in which the certification authority is established	Issuer information contains the required information, i.e. as a minimum unambiguous name and country code
Subscriber name or pseudonym. In case of the latter, it must appear that a pseudonym is used	Common Name contains name and/or pseudonym. If a pseudonym is used, it must also appear from the Pseudonym field
Specific information about the subscriber may be added, if relevant, depending on the purpose of the certificate	Subject serialNumber and other attributes contain information with suitable qualifiers. See further ETSI TS 101 862 and RFC 3039. The Subject SerialNumber format must follow the specifications for personal certificates as laid out in DS 844, section 4.3
Signature verifying data corresponding to signature generating data, which is subject to the signer's control	X.509.v3
Certificate commencement and expiry dates	X.509.v3 and RFC 2459
Certificate identification code	The CA assigns to the certificate a unique CA serial number. Together with the CA's identification, the number is completely unique. X.509.v3 and RFC 2459
The issuing CA's advanced electronic signature	X.509.v3 and RFC 2459
Limitations on the scope of the use of the certificate, if applicable	KeyUsage, CertificatePolicies and ExtendedKeyUsage

The Subject certificate field

In the "Requirements" column, M stands for Mandatory and O stands for Optional.

Attribute	**Require-ment**	**Comment**
countryName:	M	Country code
organizationName:	O	"No organisational affiliation"
OrganizationalUnitName:	M	See rules below
serialNumber:	M	Qualifier PID: Concatenated with serial number. See DS 843-1 Person-specific Identification Numbers (PID)
givenName:	O	The person's first name
surname:	O	The person's surname
commonName	M	The person's full name or pseudonym. See rules below
postalAddress	O	The person's national register address
emailAddress	O	The person's email address
Pseudonym	O	The person's pseudonym

Example:
countryName=DK,
serialNumber= PID:9208-2001-3-279815395,
commonName= Test Tester
emailAddress=tester@validdnsdomain.dk
organisationName=”No organisational affiliation”

Rules:
countryName=DK, serialNumber, givenName, surName, commonName and **pseudonym** must collectively and unambiguously point to the person who is the subscriber of the certificate.
OrganizationName: If this field is used, its contents must be set to "No organisational affiliation".
SerialNumber: Used for unique identification (see: Person-specific Identification Numbers ("Personspecifikke Identifikationsnumre"): DS 843-1).
Pseudonym: Must not be used if **givenName** or **surName** is used.
If the OCES certificate contains a pseudonym in **commonName**, the pseudonym must also be specified in **pseudonym**.
OrganizationalUnitName: If the person is of legal age, the field is empty/absent. If, at the time of issue, the person is under the age of 18, but over the age of 15, the following must be stated: "Young person aged 15 to 18 – In general not allowed to enter into legally binding agreements". If, at the time of issue, the person is under the

age of 15, the following must be added: "Young person under the age of 15 - Cannot enter into legally binding agreements."
CommonName: If, at the time of issue, the person is under the age of 18, the following must be added: ”(Young person under the age of 18)”.
Fields that have not been mentioned are optional.

Other fields (extensions)

Version number must be "v3".

In case of a combined certificate, which is to be used for signing, authentication and encryption, the **keyUsage** extension must be set with the following specifications:

digitalSignature (0)
contentCommitment (1)
keyEnchipherment (2)
dataEncipherment (3)
keyAgreement (4)

The following specifications must be set for certificates, which are used for authentication and signature:

digitalSignature (0)
contentCommitment (1)

The contentCommitment specification is set to ensure that the certificate can be used to verify signatures, the purpose of which is to increase the degree of non-repudiation.

The following specifications must be set with certificates that are used for encryption only:

keyEnchipherment (2)
dataEncipherment (3)
keyAgreement (4)

In all cases, the extension must be defined as critical.

The following codes are used in the tables below:
O: Optional
C: The extension must be marked as "Critical"
X: The extension must not be marked as "Critical"
(C): Optional for the CA to mark the extension as "Critical"
R: The extension is "Required"
M: The extension must be addressed ("Mandatory")
- : The extension has no meaning.

Extension		Generation		
		Signature		4. Key Man.
	1. Usage	2. CA	3. End user	
AuthorityKeyIdentifier	O	O	O	O
SubjectKeyIdentifier	O	O	O	O
KeyUsage	CM	CMR	CMR	CMR
ExtendedKeyUsage	O	O	O	O
PrivateKeyUsagePeriod	O	O	O	O
CertificatePolicies	M	(C)MR	(C)MR	(C)MR
PolicyMappings	O	O	-	-
SubjectAltName	O	O	O	O
IssuerAltName	O	O	O	O
SubjectDirectoryAttributes	O	O	O	O
BasicConstraints	M	CMR	O	O
NameConstraints	O	O	-	-
PolicyConstraints	O	O	-	-
CRLDistributionPoints	M	R	R	R
QcStatements	O	O	O	O

Comments to the table:
Extension management is divided into four columns:
1. Software using certificates issued.
2. Generation of certificates for CA software.
3. Generation of certificates to the end user to be used for electronic signature.
4. Generation of certificates to the end user to be used for handling/exchanging keys, e.g. in connection with the authentication/control of access rights.

CertificatePolicies must at least specify the relevant object identifiers for this CP.

Once the CA has issued a certificate, the subscriber must be notified via a channel different to the channel used in the issuing procedure.

7.3.4 Dissemination of terms and conditions

The CA must inform the subscriber that the OCES personal certificate cannot be used to sign other certificates.

The CA must inform the subscriber that the private key must not be used until the subscriber has received the OCES certificate, except from use that occurs in connection with the certificate application.

The CA must inform the subscriber that the private key must not be used for signing following a request for revocation or a notification of revocation, or following expiry.

In addition, the CA must inform the subscriber that if he/she suspects that the private key has been compromised, the key must only be used to make a request for revocation.

In both cases, the private key may still be used for decrypting data, which was encrypted using the affiliated public key before the key was revoked or before the subscriber suspected that the key had been compromised.

When issuing new keys and renewing existing keys the CA must inform the subscriber that data encrypted with a public key can only be decrypted using the affiliated private key.

The CA must inform the subscriber about the validity period of an OCES personal certificate and of the fact that an OCES personal certificate may be renewed if renewal takes place before the certificate expires.

7.3.5 Certificate dissemination

The CA must make the following types of information available to all:

- the root certificate used to issue certificates in accordance with this CP as well as the root certificate's fingerprint by a different channel;
- other certificates used to sign information between the CA, subscribers and verifiers (relying parties);
- this CP, so long as valid certificates issued in accordance with this CP exist, and so long as certificates appear in the revocation list for this CP;
- the CPS approved by the systems auditor, except trade secrets;
- all OCES personal certificates for a minimum of two months after expiry of the validity period, except certificates which must be kept secret,
- a revocation list for all OCES personal certificates which have been issued in accordance with this CP.

Information about the revocation list must be available without any kind of access control.

The CA must ensure that the requirements made by the CA to the subscriber and verifier based on this CP are summarised and documented, cf. sections 6.2 and 6.3.

7.3.6 Certificate revocation

The CA must revoke an OCES certificate immediately if the CA has been informed of any of the below-mentioned circumstances:

- certainty or suspicion exists that the subscriber's private key has been compromised;
- the private key has been destroyed;
- inaccuracies have been ascertained in the certificate content or other information associated with the subscriber;
- the subscriber wishes to terminate the use of the OCES certificate;
- the subscriber has passed away, or
- the subscriber has been placed under guardianship and has been deprived of his/her legal capacity.

The CA should revoke a certificate if the CA learns that

- the subscriber has lost access to the private key, e.g. as a result of losing the activation code.

The CA may revoke a certificate if the CA learns that

- the rules laid out in this CP have not been met, and
- the terms from the agreement between the CA and the subscriber have been breached.

CA breach of the CP does not give the CA the right to revoke a certificate.

As far as possible, the CA must ensure that a request for revocation of a certificate, takes place by stating the specific cancellation code assigned by the CA at the time of issue, or by signature by the subscriber private key.

If the cancellation code or the private key have been lost or are not available, the CA must ensure that identification is made in a way that ensures the identity in the best possible manner, e.g. by stating a combination of name, national register address and email address.

The following persons and bodies may request a certificate revocation:

- the subscriber upon showing proper documentation;
- the CA, if the rules laid out in this CP have not been met or where circumstance otherwise so dictates;
- an administrator appointed by the probate court or heirs to the subscriber, provided that the subscriber has passed away;
- a guardian upon showing proper documentation, or

- a supervisor, trustee in bankruptcy or liquidator, provided that the subscriber has suspended payments or has entered into liquidation.

To the extent possible, the CA must ensure that the procedure for requesting revocation does not allow for unauthorised revocation to take place while at the same time accepting authorised revocation following telephone contact, e-mail or web access.

The CA must ensure that in case of revocation by telephone, information is stated as specified above, as well as the reason for the requested revocation. The CA must acknowledge the revocation by sending an email to the specified email address and by sending a letter to the official postal address as specified in the Danish Civil Registration System.

If the request is made via email, the CA must make sure that the email is signed using the private key.

If the request is made via the web, the CA must ensure that the request includes a reason for revocation and that the web form is signed using the private key or that the assigned revocation code has been specified.

The CA must acknowledge revocation via signed email, if possible sent to the email address specified in the certificate. If not, the receipt must be sent by ordinary post. The subscriber is entitled to request that the receipt be sent by ordinary post.

If the CA revokes the certificate without having been requested to do so, the CA must send a notification stating the reason for revocation via signed email to the subscriber as well as by letter to the official postal address as specified in the Civil Registration System.

In case of liquidation, the probate court or the liquidator can make the request for revocation. The above-mentioned methods may also be used. However, the CA must also acknowledge revocation by post to the postal address specified by the probate court and the liquidator, respectively.

The CA must ensure that, following ascertainment of a reason to revoke, a request for revocation is put forward without undue delay.

The CA must ensure that revocation is done immediately after reception of the revocation request and if relevant, confirmation of the requesting party's identity.

The CA must publish an updated revocation list at the same time as a receipt is sent out confirming revocation of a certificate. This must take place no later than 1 minute after revocation.

The CA must ensure that a separate revocation list for OCES certificates exists.

As a minimum the CA must, publish a new revocation list every 12 hours.

The CA must make revocation lists available for downloading via LDAP and HTTP as CRL files, as well as for manual look-up via a web browser.

An OCES certificate cannot be suspended. If it is suspected that the private key has been compromised, the CA must make sure that the certificate is revoked.

The CA must make sure that revocation lists are not compromised, and must ensure daily, round-the-clock Internet access to the revocation lists and OCSP services. The average response time for the services must not exceed 1 second measured at server entry, i.e. from the time at which the server has registered the request and until it returns a reply.

As regards revocation lists, the CA must use a profile as specified in IETF RFC 3280. **thisUpdate** and **nextUpdate** must be specified in **UTCTime** format YYMMDDHHMMSSz.

The version number must be specified and set at "v2". There is no requirement to use CRL extensions.

A CA may also offer on-line status checks (e.g. via Online Certificate Status Protocol, OCSP).

The CA must ensure that the reply is electronically signed and contains the OCES certificate's unique identification number, certificate status and the reply time specified in UTC format with an accuracy of 1 second.

As regards OCSP, the CA must use a profile in accordance with IETF RFC 2560.

The **thisUpdate** field must not be more than 1 minute older than the **producedAt** field. Both fields must be specified in **generalizedTime.**

Version 1 must be supported. There is no requirement to use the OCSP extension.

7.4 CA management and operation

7.4.1 Security management

The CA must ensure that administrative and management procedures are applied which are adequate and correspond with recognised standards.

The CA must carry out a risk assessment to evaluate business risks and determine and implement the necessary requirements and operational procedures.

The CA must assume full responsibility for all aspects of the provision of certification services even if some functions are outsourced to subcontractors.

The CA must implement an information security organisation, which is responsible for the secure and correct operation of the CA's function at any time.

The CA must make sure that persons performing auditing functions within the CA do not refer to the same management as operational officers and administrators.

The information security at the CA must be defined in according to internationally recognised standards and must be subject to the supervision of the information security organisation.

Security controls and operating procedures for CA facilities, systems and information assets providing the certification services must be documented, implemented and continuously maintained.

In cases where the responsibility for the CA certification functions are outsourced to another organisation or unit, the CA must make sure that information security is being maintained in the same way.

7.4.2 Asset identification and classification

The CA must perform a risk assessment of all IT assets, specifying vulnerabilities.

Each IT asset must be assigned a classification according to their importance to the operation of the CA's primary functions and consistent with the risk assessment.

7.4.3 Personnel security

Requirements to qualifications, experience and security classification

Persons holding trusted positions at the CA, including systems auditors, must have verified qualifications within their field of responsibility and must have at least 1 year's experience.

All persons holding managerial positions at the CA must be familiar with security procedures for employees with security responsibility, and must have experience with information security and risk assessment.

Security classification procedures
The CA must check that managers and employees who are to perform trusted assignments at or for the CA have not been convicted of a crime that makes them unsuitable for performing their job.

Educational requirements
All persons holding trusted positions at the CA must have completed education or training that is relevant for their job area. The CA management is responsible for ensuring that each employee is suitable to perform the relevant job.

Requirements to and frequency of updating qualifications
General
Relevant qualifications of CA employees must be updated if they have not been used during the last four years.

CA operating staff
CA operating staff must update their knowledge once a year.

Procedure for handling unauthorised actions
Clear procedures must be established to handle any kind of unauthorised action. These procedures must be announced to all persons holding trusted positions at the CA.

Check of subcontractors
The CA must make sure that subcontrators' personnel meet the same requirements regarding education, experience and security classification as required for the CA's own employees undertaking the functions performed by the subcontractors' personnel.

By means of access procedures, the CA must ensure that subcontractors' personnel cannot work without surveillance anywhere at the CA.

Documentation for personnel use
The CA must document and publish all procedures, rules and sanctions to CA personnel. The CA management must be able to prove that all personnel have been informed of procedures, rules and sanctions.

7.4.4 Physical security
General
The CA must clearly identify in which facilities employees and data centres related to CA activities are located. Facilities housing key generation systems are designated CA operation facilities.

All facilities used for employees at the CA must be defined as special security areas in accordance with DS 484:2005.

CA operation facilities
CA operation facilities must be defined according to a security level and must meet the requirements laid out in DS 484:2005.

CA operation facilities must be physically separated from other CA facilities.

In case of evacuation, the CA operation facilities must be able to function via remote control without changes in operation. Remote control is understood to be the possibility to operate CA functions via a PC from a facility that is physically separate from the CA operation, e.g. in a place where the CA has set up a back-up system.

The CA operation facilities must be protected against penetrating air pollution, smoke and radioactive fallout.

Physical access
General
The CA must ensure that all facilities are equipped with perimeter protection corresponding to DS 471 or better.

The CA must ensure that access to and presence in central CA operation facilities are limited to specific groups of personnel by means of electronic access control.

The CA must ensure that watch is kept 24 hours a day.

CA operation facilities
The CA must ensure that access to and stays in the central operation facilities are monitored by video.

Power supply and air conditioning
The CA must protect the power supply against power failure. The protection must cover all operating systems and all telecommunications equipment located at the CA.

CA operation facilities
The CA must double and protect the air conditioning system in CA operation facilities against power failure.

The CA must protect the air conditioning system against pollution, smoke and radioactive fallout via the air intake.

Water pressure
General
The CA must protect its facilities against penetrating water and leaking pipes.

CA operation facilities
The CA must make sure that no water installations are placed in CA operation facilities. Similarly, water installations must not be run through CA operation facilities.

The CA must implement water detection systems in CA operation facilities and must install relevant alarms.

Fire prevention and fire protection
General
The CA must install an automatic fire alarm system.

CA operation facilities
The CA must set up the individual functional rooms as separate fire cells.

In addition, the CA must install automatic fire-fighting equipment.

Keeping of storage medium
The CA must set up archives for the keeping of storage media with back-up copies of data and applications in separate cells, divided according to function.

Waste handling
General
The CA must ensure that waste containing confidential information is considered confidential material and is destroyed in a safe manner.

CA operation facilities
The CA must make sure that waste from CA operation facilities is treated separately and destroyed before being removed from the area.

Back-up system in a different location
If the CA sets up back-up systems in a different location, the CA must ensure that such locations meet the same requirements as main systems. If back-up systems are established, the CA must ensure that the back-up system is physically located so far from the main system that the risk of cumulative breakdowns is minimised.

7.4.5 IT systems and networks operations management
The CA must define its trusted functions, and a description must be prepared of the responsibilities of each trusted function at the CA.

General
The CA must ensure participation of at least two persons holding different trusted positions at the CA when performing any task where it is possible to make changes to settings and functionality.

The CA must ensure that all IT equipment and data are protected against viruses, and faulty and unauthorised software.

Damage from security incidents and malfunctions must be minimized through the use of incident reporting and response procedures.

The CA must ensure that all media used are protected against damage, theft and unauthorised use.

The CA must ensure that sensitive data cannot be recreated via discarded media.

CA operation facilities
The CA must ensure participation of at least two persons holding different trusted positions at the CA when performing any task in CA operation facilities.

The CA must make sure that employees in each trusted position can be unambiguously identified by means of clear picture identification.

The CA must ensure that access to systems is connected to the individual trusted position. Where several people need to have access to systems, the CA must ensure that such access is supported technically to the greatest possible extent.

7.4.6 Systems, data and networks access management

The CA must ensure that all IT equipment used is safe and is operated correctly with a minimum risk of errors.

By means of rules and technical arrangements, the CA must limit access to the CA systems to an absolute minimum.

The CA must limit external persons' access to the CA system to the highest possible degree.

The CA internal network must be protected against other networks by means of correctly configured firewalls.

The CA must ensure protection of sensitive data when such data is exchanged via networks. Such protection is normally obtained by means of encryption.

The CA must ensure that the administration of user rights to the systems is described in written instructions, that logs are made of all changes to rights, and that checks are performed on such logs.

The CA must ensure that all systems support strict access control to data and prevent unintended exchange across trusted functions at the CA.

The CA must ensure that access to systems can only be obtained following correct identification of the individual employee.

The CA must ensure that a person is appointed to be responsible for allocating access rights to all systems. In addition, the CA must ensure that the individual employee has been made aware of measures that will be taken in case of irregularities.

Operation facilities
The CA must ensure that all network components are located in physically secured facilities in accordance with section 7.4.4, and that the configuration of network components is reviewed periodically.

The CA must ensure that all IT components in operation facilities are under constant surveillance, and that alarms will sound for all attempts to gain access to and revise configurations and data.

The CA must ensure that alarms will be triggered for all unauthorised changes made to data regarding certificates and associated information and status information.

7.4.7 Development, procurement and maintenance of IT systems
The CA must use recognised systems and products, which are protected against changes. The products must comply with an adequate protection profile in accordance with ISO/IEC 15408 or similar.

Regarding internal development, the CA must ensure that a plan has been prepared and approved by the management regarding the integration of security measures in the systems. This requirement also applies in cases where development work has been ordered.

The CA must ensure that control procedures are established for new versions, changes and back-up systems.

7.4.8 Preparedness planning
The following incidents must be considered serious:

- Compromising of the CA private key
- Suspicion of compromising of the CA private key
- Breakdown and critical errors on the CA operating components (revocation lists etc.)
- Stop of the CA operating environment as a consequence of fire, power failure etc.

The CA must ensure that a preparedness plan exists which can bring the CA operations back to normal as quickly as possible following the occurrence of a serious incident.
Subsequently the preparedness plan must be revised for the purpose of preventing similar incidents from recurring.

If the CA private key is compromised, or if there is suspicion hereof, the CA must inform all subscribers and the National IT and Telecom Agency. Verifiers must be informed to the extent that it is possible. Such information may, for example, be given via public media and by advertising in the daily press.

In case of serious incidents to data processing equipment, software and/or data, the CA must inform subscribers hereof to the extent that it is relevant for their use of the CA services. Verifiers must be informed to the extent that it is possible. Such information may, for example, be given via public media and by advertising in the daily press.

The CA must ensure that all procedures relating to revocation lists, including requests for revocation, are given the highest priority in connection with re-establishing business procedures.

7.4.9 CA termination

In the event that a CA function is to cease operations, the CA must ensure that a stop is immediately put to all issues and renewals of certificates.

The CA must ensure the continued operation of revocation lists and requests for revocations until all certificates issued by this CA have expired or have possibly been transferred to another CA, which meets the requirements laid out in this CP.

The CA must ensure that all files are accessible for a minimum of six years following the expiry of the last certificate issued by this CA.

7.4.10 Compliance with legislation

The CA must ensure compliance with legal requirements, particularly in relation to personal data.

Special obligations regarding the protection of confidential information

Information, which is not included in certificates and revocation lists, is considered confidential.

Information, which is included in certificates and revocation lists, is considered non-confidential and non-private.

Person-related information, which is not included in the certificate, is considered to be private information.

The CA must ensure that it is possible for a subscriber to require that name and address information, including email address, does not appear from the certificate *(this only applies to personal certificates).*

The CA must ensure that confidential information is protected from being compromised, and the CA must not use confidential information for any other purpose than what is required for operating the CA.

The CA must ensure that private information is protected from being compromised, and the CA must not use private information for any other purpose than what is required for operating the CA.

The CA must ensure that statistical information about the use of OCES personal certificates cannot be related to the individual OCES certificate.

In case of disagreement, which cannot be solved by negotiation between the parties, the general rules of Danish law shall apply.

7.4.11 Recording of certificate information

The CA is responsible for establishing a data storage system, which must contain all data necessary for the safe operation of the CA in accordance with this CP. In addition, the CA must ensure that:

- all other information is protected against unlawful access;
- all activities, which require participation by more than one person, are logged;
- all information regarding registration, including certificate renewals, is logged;
- all access and attempts of gaining access to areas, which must be protected by access control, are logged;
- all video monitoring is logged;
- written rules exist for regular reviews of all logs;
- all audit logs are signed electronically and time stamped;
- audit logs are treated as confidential material,
- audit logs are backed up at regular intervals.

The CA must ensure that back-up media are stored in accordance with the requirements laid out in section 7.4.4 in a media fire alarm box.

The CA must ensure that the National IT and Telecom Agency is informed of significant irregularities in the logging procedure and notified once annually in all other cases.

The CA must ensure that the following information is filed:

- all logs;
- certificate applications and relevant communication;
- signed orders and written agreements;
- certificate renewals, and
- CPS and CP.

The CA must ensure that filed information can be made accessible in case of disputes, and that all filed material is kept for a minimum of six years.

The CA must ensure that all filed material is stored in accordance with the requirements laid out in section 7.4.4.

The CA must ensure that back-up copies are made of all electronic archive material at regular intervals.

The CA must ensure that all electronic archive material is endorsed with an electronic timestamp at the time of archiving. Other archive material must be entered in a log.

7.5 Organisational aspects

The CA organisation must be reliable.

The CA must be a registered physical or legal person.

The CA must ensure that all services are offered on equal terms to everybody within the field of use of the OCES personal certificates. Thus, there must be no difference in terms and conditions regarding access to services.

All CA administrative and business procedures must be adapted to the security level necessary for operating a CA.

The CA must have sufficient financial strength to cover the liability, which is assumed as a CA, including the obligations stated in section 7.4.9, partly through insurance, and partly through the CA equity capital.

The CA must at all times have at its disposal sufficient numbers of trained personnel necessary to operate all services offered in a responsible manner. The personnel must at all times possess the skills prescribed by the definition of each trusted position.

The CA must ensure that policies and procedures are in place for the handling of all kinds of customer inquiries or inquiries made by verifiers.

The CA must ensure that written agreements are in place with all CA service subcontractors.

7.6 Data centre location

CAs that wish to place all or parts of the operating environment abroad, must meet the same requirements that are laid out in this CP as the requirements that are made to a local CA. Thus, it must be possible to perform ongoing checks, irrespective of the CA's geographical location.

If a state-authorised accountant does not perform the systems audit, an exemption granted by the National IT and Telecom Agency is required, cf. section 7.1.