Certificate Policy for OCES Employee Certificates (Public Certificates for Electronic Services)

Version 5

Contents

Rights

Preface

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

The National IT and Telecom Agency is the public authority which authorises the issue of OCES employee 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 is also responsible for the content of this CP. The most recent version of this CP as well as earlier versions under which valid certificates are still in existence can be found at www.digitalsignatur.dk.

Please direct inquiries regarding digital signatures to the National IT and Telecom Agency. For further information, see www.digitalsignatur.dk.

Introduction

A digital signature is an electronic signature that may be used in various situations, for instance when it is essential to know who you are communicating with electronically. The use of digital signatures presupposes that a public key infrastructure (PKI) has been established.

OCES is such a public key infrastructure. OCES is short for "Offentlige Certifikater til Elektronisk Service" *(Public Certificates for Electronic Services)*. The National IT and Telecom Agency has prepared four OCES certificate policies (CPs), applicable to personal, employee, company and functional certificates, respectively. The CPs constitute a common public standard regulating the issue and use of the digital OCES signature. Thus the CPs specify requirements for the public key infrastructure, and hence the level of security applicable to the digital signature.

The digital signature can be used when a person has been identified and registered under a certification authority (CA). The CA grants the individual a personal electronic certificate containing this individual's public key. The CP specifies requirements as to how and under what conditions the CA will perform these tasks.

This CP does not address qualified certificates issued pursuant to Act No. 417 of 31 May 2000 on Electronic Signatures.

1 Overview and scope

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

This CP has been prepared on the basis of the guidelines given in ETSI TS 102 042 v 1.3.4 (2007-12). *"Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*.

The rules of the certificate policy regulating the CA's activities provide a high level of security that the subject has the identity indicated in the certificate.

A certificate is only an OCES certificate if it has been issued according to an OCES CP, and has been issued by a certification authority (CA) approved by the National IT and Telecom Agency as an issuer of OCES employee certificates. As an element in the approval, a formal agreement is made between the CA and the National IT and Telecom Agency in which the CA undertakes to fulfil the requirements of this CP, including the requirement that the CA's handling of tasks should be audited, see also section 7.1.

Thus the subscribers and verifiers (relying parties) may base their trust on the certificate policy, the National IT and Telecom Agency's approval of the CA, and the Agency's ongoing supervision of this.

Certification authorities (CAs) entitled to issue certificates under this CP (OCES employee certificates) are published on the National IT and Telecom Agency's website: https://www.digitalsignatur.dk.

2 References

Act No. 417 of 31 May 2000: Lov om elektroniske signaturer *(Act on Electronic Signatures)*

Act No. 429 of 31 May 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)"*

CWA 14167-1:2003: *"Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements"*

CWA 14167-2:2004: *"Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB 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)*

DS (Danish Standard) 471:1993: "Teknisk forebyggelse af indbrudskriminalitet" *(Technical Prevention against Burglar Attack)*

DS (Danish Standard) 484:2005: "Dansk standard for Informationssikkerhed DS 484" *(Code of practice for information security management)*

ETSI TS 102 042 v 1.3.4. (2007-12): *"Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*

ETSI TS 102 176-1 V2.0.0 (2007-11): *"Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms"*

ETSI TS 102 176-2 V1.2.1 (2005-07): *"Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices"*

ETSI TS 101 862 v1.3.3 (2006-01): *"Qualified Certificate profile"*

FIPS PUB 140-2 (2001): *"Security Requirements for Cryptographic Modules"*

ISO/IEC 15408 (parts 1 to 3) 2005: *"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"*

Requests for Comments:

- RFC 3039: *Internet X.509 Public Key Infrastructure - Qualified Certificates Profile*
- RFC 3280: *Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile*
- RFC 5019: *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*

In case of discrepancy between the references above and this CP, the provisions of this CP shall be applicable to the CA unless otherwise provided by law.

3 Definitions and abbreviations

3.1 Definitions

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

Activation Password: Code used for activating the signature when generating and installing keys.

Password/personal password: A personal code kept secret by the subject and used by the subject when applying a digital signature.

Authorised person: A person who, by a member of the company management authorised to sign for the company, has been appointed and accepted as the CA's contact person in the company, and who has been authorised to accept and submit certificate applications on behalf of the company and/or administer the company's certificates.

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.

Subscriber *(certifikatindehaver)*: A natural or legal person entering into an agreement with the issuing certification authority (CA) about issuing certificates to one or more subjects.

Subject *(certifikatholder)*: A natural person identified in the certificate as the right user of the private key associated with the public key given in the certificate, and to whom an OCES certificate is being or has been issued.

Certification authority (CA) *(certificeringscenter)*: A natural or legal person authorised to generate, issue and manage certificates[1].

Certification practice statement (CPS) *(certificeringspraksis)*: A specification of the principles and procedures which a CA employs in issuing certificates.

Certificate policy *(certifikatpolitik)*: A set of rules that indicates requirements for issuing and using a certificate in one or more specific contexts where common security requirements exist.

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

Digital signature: Data in electronic form used for authenticating other electronic data attached to the digital signature or with which it is logically associated.

One-time password: Code used for activating the signature when generating and installing keys.

OTP device *(OTP-enhed)*: Physical unit which is able to deliver one-time passwords to the user.

OTP response code *(OTP-engangskode)*: Response code delivered by the OTP.

Private key *(privat nøgle)*: The subject's key for applying a digital signature or for decrypting. The private key is personal and is kept secret by the subject.

Key escrow *(nøgledeponering)*: Storing of keys for the purpose of giving third parties access to these in order to decrypt information.

Cryptographic module: Hardware module which can generate and store keys and apply the digital signature independently of the operating system. The module must be certified according to FIPS 140-2 level 3, CWA 14167-3 or SSCD-PP Type 3.

Employee: A person associated with the company that appears from the certificate.

Public-key certificate *(offentligt certifikat)*: See certificate.

Registration authority (RA) *(registreringsenhed)*: The natural or legal person responsible for the identification and authentication of a (future) subject.

Root certificate *(rodcertifikat)*: A public certificate issued by a CA for the purpose of validating other certificates. A root certificate is signed with its own signing key (self signing *(egensignering)*).

Root key: The CA's private and public keys used for signing the subscriber's certificates.

RID: Resource identification number.

Verifier (relying party) *(signaturmodtager)*: A natural or legal person receiving an electronic signature created by signing data from a subject.

Sub-certification of CA: A higher-level CA issuing a certificate with the public root key of the lower-level CA. Sub-certification may occur at several levels, thus forming a continuous chain of certificates.

Certificate revocation list *(spærreliste)*: A list of certificates no longer considered valid because they have been permanently revoked.

3.2 Abbreviations

CA Certification Authority *(Certificeringscenter)*

CRL	Certificate Revocation List *(Spærreliste)*
CPS	Certification Practice Statement *(Certificeringspraksis)*
CP	Certificate Policy *(Certifikatpolitik)*
CVR	The Danish Central Business Register
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OCES	Public Certificates for Electronic Services *(Offentlige Certifikater til Elektronisk Service)*
OCSP	Online Certificate Status Protocol
OID	Object Identifier, see ITU-T's ASN.1 standard
OTP	One Time Password
PKI	Public Key Infrastructure
RA	Registration Authority
RID	Resource identification number
UTC	Universal Time, Coordinated

3.3 Notation

The requirements contained in this CP comprise:

1 Mandatory requirements, which must be met. Such requirements are indicated using the term "must".

2 Requirements that should be met. If the requirements are not met, this must be reasoned. Such requirements are indicated using the term "should".

3 Requirements that may be met if the CA so wishes. Such requirements are indicated using the term "may".

4 Concept

4.1 CA

A natural or legal person entrusted by both subscribers and verifiers with the task of generating, issuing and managing electronic certificates is known as a certification authority (CA). The CA has overall responsibility for providing the services necessary for issuing and maintaining certificates. The CA's own private keys are used to sign issued certificates, and the CA is identified in the certificate as the issuer.

The CA may cooperate with other parties in offering parts of the overall CA services, but the CA will always have overall responsibility for all activities regarding the handling of certificates, and the CA is also responsible for the requirements of this CP for CA services being met at all times.

A CA may sub-certify its public OCES root key under other CAs. A CA's OCES root key may also sub-certify another CA's public root key provided that this is approved for OCES.

An OCES CA must always offer a self-signed OCES root certificate to the verifiers (relying parties).

4.2 CA services

The services necessary for issuing and maintaining certificates may be classified as follows:

- Registration: Verification of the subject's identity and any associated ID and registration information. The result of the registration will be passed on to certificate generation.
- Generating certificates: Generation and electronic signing of certificates based on the verified identity and any associated ID and registration information from the registration.
- Certificate distribution: Distribution of certificates to subjects.
- Catalogue service: Publication of certificates, giving verifiers (relying parties) access to the certificates.
- Publication of business conditions etc.: Publication of terms and rules, including CP and CPS.
- Revocation of certificates: Receiving and handling requests for revocation of certificates.
- Publication of revocation information: Publication of status information for all certificates, in particular certificates which have been revoked.

4.3 CP and CPS

4.3.1 Purpose

The purpose of a CP like the present is to specify what requirements must be met, while the purpose of a CPS is to specify how the requirements are met by the relevant

CA. The certificate refers to the CP, thus allowing a verifier to determine what minimum requirements have been met by the CA, including the requirements that a CA must require a subscriber to meet.

4.3.2 Degree of specification

The CPS gives a detailed description of conditions and terms, including business and operating procedures, for the issue and maintenance of certificates. Thus the CPS is more detailed than the CP, which describes general requirements only.

The CPS must indicate 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 the present has for instance been defined independently of specific details in the operating environments of the CA, whereas the CPS is tailored to the organisational structure, operating procedures and IT facilities of the CA. This CP has been prepared by the National IT and Telecom Agency, while the CPS is always prepared by a CA.

An independent third party (system auditor) must make an audit of the CPS and declare that the CPS meets all requirements made in the CP, and that these requirements are observed by the CA.

4.3.4 Other CA conditions

The CP and the CPS describe the basic framework for CA's activities. In addition, the CA will typically employ customer-oriented commercial conditions and terms addressing the issue and use of certificates and the provision of status information.

4.4 Subscribers and subjects

Prior to the issue of employee certificates, the CA will make an agreement with the subscriber in the capacity of the company requesting employee certificates for its employees. The employee to whom a certificate is subsequently issued is referred to as the subject.

In this CP, both terms are used in order to distinguish between the party that has made an agreement with a CA and the party identified as the subject in the certificate.

The subscriber has overall responsibility for the use of the certificate and the associated private keys, although it is the subject that controls the private key.

The term subject is used where explicit reference is made to the person identified in the certificate, while the term subscriber is used in all other instances, also where the difference does not appear clearly from the context.

5 Certificate policy and auditing

5.1 General

This document describes the certificate policy for OCES employee certificates.

5.2 Identification

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

Employee certificate:

{ 1 2 208 stat(169) pki(1) cp(1) nq(1) medarbejder(2) ver(5) }.

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

All OCES employee certificates issued according to this CP must refer to it by indicating the relevant OID in the "certificate policy" field of the OCES certificate. In a certificate, reference must only be made to the OIDs in question following written agreement with the National IT and Telecom Agency, cf. section 1.

5.3 Scope of application

An OCES employee 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 employee certificates are not qualified certificates, i.e. they must not be used in situations where qualified certificates are required.

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

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

5.4 The CA's right to issue OCES certificates

The CA may issue OCES employee certificates according to this CP if the CA:

- has entered into a written agreement with the National IT and Telecom Agency in this respect;
- has submitted a CA report, cf. 5.5, to the National IT and Telecom Agency; and
- has received a declaration of conformity from the National IT and Telecom Agency confirming that the Agency has approved the submitted report and finds that the requirements of the present CP have been met.

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

5.5 CA report

The report must include:

- the CA's CPS;
- the auditor's records;
- a declaration from the CA's management as to whether the CA's data, system and operating security as a whole is considered to be adequate, and that the CA complies with its own CPS;
- a declaration from the system auditor as to whether the CA's data, system and operating security as a whole is considered to be secure, and whether the CA complies with its own CPS; and
- documentation of indemnity insurance covering the CA's liability.

5.6 System audit

System audits must be performed at the CA. System audits include auditing of:

- general IT controls in the company;
- IT-based user systems etc. for generating keys and key components and for registration, issue, verification, storage and revocation of certificates; and
- IT systems for exchanging data with other parties.

Appointing the system auditor - auditor's powers and obligations

The CA must appoint an external state-authorised auditor to perform the system audit of the CA. In special cases, the National IT and Telecom Agency may exempt from the requirement that the system auditor must be a state-authorised auditor. Within one month after the appointment of the system auditor, the CA must notify this to the National IT and Telecom Agency.

The CA must disclose the information necessary to perform the system audit of the CA. The CA must give the appointed system auditor access to the management protocol.

The CA must give the appointed system auditor access to management meetings discussing matters relevant to the system audit. A management meeting means a meeting of the CA's top management, in practice often a board meeting. In this connection, "CA's management" means the top management of the CA, i.e. the board or a similar management body, depending on how the CA is organised. 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 provisions of the Danish Financial Statements Act on the auditor's obligation to reply to questions posed at a company's general meeting shall also apply to the appointed system auditor.

The CA must inform the appointed system auditor that, in accordance with generally accepted auditing standards, the auditor must perform the system audit mentioned below, including checks to ensure the following:

- that the CA's systems comply with the requirements of this CP;

- that the CA's security, control and auditing requirements are allowed for to a sufficient extent in the development, maintenance and operation of the CA's systems;
- that the CA's procedures, both computerised and manual, are adequate 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 system audit.

The appointed system auditor may cooperate with the CA's internal auditing team if one exists.

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

The CA must inform the appointed system auditor that the auditor is under obligation to report the matter(s) to the National IT and Telecom Agency provided that the system auditor continues to find significant weaknesses or irregularities. In addition, the CA must inform the system auditor that, upon inquiry from the National IT and Telecom Agency, the auditor is obliged, without prior acceptance by the CA, to disclose matters relating to the CA that have or may have an impact on the CA's administration of the task of issuing OCES certificates. However, the system auditor is obliged to inform the CA about the inquiry.

The CA and the system auditor must inform the National IT and Telecom Agency without delay about matters of significant importance to the continued operation of the CA.

Auditor's records
The CA must inform the appointed system auditor that the auditor must keep separate auditor's records on a current basis, to be presented at every management meeting, and that any entry into the records must be signed by the CA management and the appointed system auditor. In addition, the CA must inform the system auditor that the contents of the records must be specified as indicated below.

The appointed system auditor's records must include a report of the system audit performed as well as its conclusions. Furthermore, any matter that has given rise to significant comment must be described. The records prepared by the appointed system auditor must also state whether the auditor has received all the information requested while performing the task.

At the end of the CA's fiscal year, the appointed system auditor must prepare a report to the CA management.

The report must include statements as to whether:

- the system audit has been performed in accordance with generally accepted auditing standards;
- the appointed system auditor meets the qualifications required by legislation;

- the appointed system auditor has received all information requested by the auditor;
- the specified system audit tasks have been performed in accordance with the requirements of this CP;
- the data, system and operating security as a whole is found to be adequate.

The National IT and Telecom Agency may direct the CA to appoint a new system auditor within a stipulated time limit in case the acting system auditor is found to be clearly unqualified to perform the auditor's duties.

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 system audits
The CA must bear all expenses incurred in connection with system audits, including system audits ordered by the National IT and Telecom Agency.

6 Obligations and liability

6.1 CA obligations

The CA must fulfil all requirements specified in section 7.

The CA is responsible for its subcontractors meeting the procedures and requirements of this certificate policy.

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

- distribution of root certificates;
- instructions on how to generate and store keys;
- issuance of OCES employee certificates to subscribers;
- revocation of OCES employee certificates on request;
- publication of revocation lists;
- informing subscribers about impending expiry of the validity period of certificates, including the option of renewing key pairs; and
- renewal of OCES employee certificates.

The CA must maintain a technical operating environment that meets the security requirements of this CP.

The CA must use a reliable time source in connection with CA-related activities.

The CA must prepare a CPS addressing all requirements in this CP. The CPS must comply with this CP.

The CA must submit to audit requirements, cf. section 5.6.

The registration authority (RA) may either be closely associated with the CA, or it may be an independent function. In all circumstances the CA is responsible for the RA meeting the specified requirements and obligations as if they applied to the CA itself.

The CA must ensure that the provisions of this CP are followed by the associated RA/RAs.

In addition, the CA must ensure that the RA:

- establishes web access for registration procedures (may be part of the CA's web service);
- verifies the applicant's identity and details; and
- maintains a technical operating environment conforming to the requirements of this CP.

6.2 Subscriber obligations

The CA must enter into an agreement with the subscriber under which the subscriber undertakes to ensure that the subject fulfils the following conditions and that the subscriber's organisation and procedures support the fulfilment thereof:

- to give adequate and correct answers to all requests from the CA (or RA) for information during the application process;
- only to use the OCES certificate and the associated private keys in accordance with the provisions of this CP;
- to take reasonable measures to ensure that the mechanisms securing the private key are protected against compromise, alteration, loss or unauthorised use;
- to keep the password secret so as to prevent its disclosure to others;
- to ensure, when receiving the OCES certificate, that the contents of it are in agreement with the real situation;
- to immediately request revocation and possible renewal of the OCES certificate if the contents of it are no longer in agreement with the real situation;
- to immediately change its password or revoke the certificate if it is suspected that the password has been compromised;
- to immediately request the issuing CA to revoke the OCES certificate in case of the subscriber's bankruptcy or liquidation;
- to immediately stop using the certificate if it comes to the subscriber's knowledge that the CA has been compromised; and
- the use of a different password - e.g. biometrics - must implement a security standard at least at the same level as the security of traditional passwords in this certificate policy.

In case the subscriber's key pair is generated and stored centrally at the CA, the CA must also enter into an agreement with the subscriber under which the subscriber undertakes to meet the following conditions:

- to choose/decide a password in conformity with the provisions of section 7.2.8;
- to use and keep OTP devices, user IDs and passwords as directed by the CA;
- to take reasonable measures to protect the OTP device so as to prevent access by others; and
- to immediately block the OTP device if it is suspected that the device has been compromised.

In case the subscriber's key pair is generated and stored at the subscriber, the CA must also enter into an agreement with the subscriber under which the subscriber undertakes to meet the following conditions:

- to generate, store and use key pairs in a manner that ensures compliance with the requirements of this CP, in particular 6.2;

- to protect the private key with a password in conformity with the provisions of section 7.3.1;
- to ensure that a backup copy of the private key, where applicable, is kept in an encrypted form in a secure manner;
- to immediately revoke the certificate if it is suspected that the password has been compromised; and
- to immediately request the issuing CA to revoke the OCES certificate if the private key has been compromised or if it is suspected that it has been compromised.

In case the subscriber's key pair is generated at the CA, but is sent to the subscriber in a cryptographic module and stored under the subscriber's control, the CA must also enter into an agreement with the subscriber under which the subscriber undertakes to meet the following conditions:

- to keep and use the cryptographic module and password as directed by the CA;
- to protect the private key with a password in conformity with the provisions of section 7.2.8;
- to immediately revoke the certificate if it is suspected that the password and the cryptographic module have been compromised; and
- to immediately revoke the certificate if it is suspected that the cryptographic module has been compromised.

Additional obligations
As regards private keys that are used to ensure secrecy (encryption keys), the subscriber may direct the subject to use alternative procedures for ensuring common control and use of keys. In that case the subscriber must inform the subject of the consequences in relation to secrecy.

If the subject's association with the subscriber ends, the subscriber must inform the CA immediately and request revocation of the subject's certificate.

In case the subscriber changes its business address, this must be notified immediately to the CA.

6.3 Information for verifiers (relying parties)
Via its website and other means, the CA must inform verifiers about terms and conditions for using digital signatures, including that in order to rely on a certificate, the verifier must ensure:

- that a certificate received is valid and has not been revoked, i.e. it is not included in the CA's revocation list;
- that the purpose for which the certificate is to be used is appropriate in relation to any usage limitation in the OCES certificate; and
- that the use of the certificate is appropriate in other respects 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 under the general rules 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 the following:

- that the information specified in the certificate was not correct at the time of issuing the certificate;
- that the certificate does not contain all information required under section 7.3.3;
- failure to revoke the certificate, cf. section 7.3.6;
- lacking or erroneous information about the revocation of the certificate, the expiry date of the certificate, or whether the certificate contains any limitations on scope or amounts, cf. sections 7.3.3 and 7.3.6; or
- failure to comply with section 7.3.1;

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

The CA shall prepare its own agreements etc. with joint contracting parties. The CA is entitled to seek limitation of its liability in the relationship between the CA and its joint contracting parties to the extent that such parties are business operators or public authorities. Thus the CA is not entitled to seek limitation of its liability in relation to private citizens who are joint contracting parties.

In addition, the CA is entitled to disclaim liability in relation to joint contracting parties who are business operators and public authorities for loss of the nature described in section 11(3) of Act No. 417 of 31 May 2000.

Insurance

The CA must take out and maintain an insurance to cover any claims for damages against the CA and RA by all joint contracting parties (subscribers and verifiers, relying parties) as well as the National IT and Telecom Agency. The minimum annual coverage must be DKK 10 million.

7 Requirements on CA practice

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:

- the CA's administrative and management procedures;
- qualifications, experience etc. of CA staff;
- the systems, products and algorithms used by the CA;
- the CA's security measures and related work process, including information about measures applicable with regard to maintaining and protecting the certificates as long as they exist;
- CA procedures regarding registration (identity control), issue of certificates, catalogue and revocation services, and registration and storage of information regarding certificates, including identity information;
- the CA's financial resources;
- CA procedures for entering into agreements about the issue of certificates and its notification duty; and
- to the extent that the CA has outsourced CA tasks to other companies or authorities, the CPS must also include the performance of such tasks; and
- what reliable time source the CA is using.

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

The CA must publish the CPS on its website. Sensitive information, e.g. trade secrets, can be exempted from publication.

7.2 Key management

The CA's 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.

For critical parts of the CA infrastructure, the CA must follow relevant and official recommendations from NIST regarding the use of up-to-date algorithms and key lengths.

7.2.1 CA key generation

The CA must ensure that generation of keys is performed under controlled conditions. The conditions below must be observed in particular:

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 of FIPS 140-2 level 3, CWA 14167-3, or higher. The cryptographic module must be stored in accordance with the requirements in 7.4.4.

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

The certificate issuer's root keys must be RSA keys with a length of at least 2048 bit or similar. The certificate issuer's root keys must be valid for at least five years.

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

7.2.2 CA key storage, backup and recovery

The CA must ensure that CA root keys are not compromised and maintain their integrity at all times.

CA root keys and other private keys must be stored and used in cryptographic modules that comply with the requirements of FIPS 140-2 level 3, CWA 14167-3, or higher.

Storage, backup 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.

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

7.2.3 CA public key distribution

The CA root certificate must be made available to verifiers (relying parties) via the CA's website in a way that ensures the integrity of the public key and authenticates its origin.

The CA must enable verification of the root certificate via a different channel. Verification can be made for instance by using a fingerprint of the certificate.

7.2.4 Key escrow

The CA must not hold the subscriber's keys in escrow.

7.2.5 CA key usage

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

The CA must ensure that certificate signing keys are only used within physically secure premises in accordance with 7.4.4.

7.2.6 End of CA key lifecycle

The CA's private key must have a specified period of validity. After expiry, the private key must either be destroyed or kept in such a manner that it cannot be restored and be put to use again.

Before the private key expires, the CA must ensure generation of a new CA key pair that can be used for issuing certificates.

7.2.7 Management of cryptographic modules

The CA must manage and store cryptographic modules in accordance with the requirements in section 7.4 throughout the lifecycle 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 at least 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 module retirement.

7.2.8 CA provided key management

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

CA generated subject keys must be RSA keys with a minimum length of 2048 bit or similar.

In case the subject's key pair, after having been generated, is stored centrally at the CA, the following conditions must be met:

- It must not be possible to use the subject's private key without the subject having authorised such use in each individual case, thus ensuring that the subject will maintain sole control over its private key.
- The CA must protect access to the subject's private key using authentication of the subject by means of two independent factors in the form of an OTP device and a password.
- The password must be selected from an outcome space of at least 36^6 possible codes, for instance as 6 characters selected from 36 letters, figures and special characters. OTP response code must be selected from an outcome space of at least 10^4 codes, for instance as 4 numeric digits. Validation of the passwords must be implemented in a way that protects effectively against exhaustive searches. The use of a different password - e.g. biometrics - must implement a security standard at least at the same level as these requirements.
- The private key must be available to the subject after revocation to enable the subscriber to decrypt data using the private key.

In case the subject's key pair, after being generated by the CA, is sent to the subject on a cryptographic module and stored under the subject's control, the following conditions must be met:

- CA generated keys must be generated and stored securely prior to delivery to the subject.
- The subject's keys and the associated activation password passwords must be delivered separately and in such a way that the confidentiality of these is not compromised.
- Generation and distribution of the subject's keys must be arranged in such a manner that only the subject itself will have access to the private key.
- The password must be selected from an outcome space of at least 10^4 possible codes, for instance as 4 digits selected from figures between 0 and 9. The use of a different password - e.g. biometrics - must implement a security standard at least at the same level as these requirements.

7.3 Certificate management

7.3.1 Subscriber and subject registration

Subscriber registration
The CA must ensure that the subscriber, before starting to use an OCES employee certificate, is made aware of and accepts the terms and conditions for using the certificate. In this connection, the subscriber is required to appoint an authorised person, to be approved by the management, who is empowered to handle the administration of employee certificates on behalf of the company.

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

- the OCES subscriber states the company's CVR number and the name and e-mail of the authorised person;
- the OCES subscriber's CVR postal address is obtained via online lookup in the Central Business Register;
- the authorised person's activation password is sent in a PIN code letter to the company management at the company's CVR postal address.

It is sufficient that the CVR postal address is verified in connection with the registration of the subscriber. If the company's address changes, the CVR postal address must be verified again.

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 departed from in full or in part. Procedures must be submitted to the National IT and Telecom Agency for approval before implementation.

Subject registration
The CA must establish and maintain a function by which the authorised person can make applications for and issue employee certificates. The CA must ensure that the registration process is conducted via the person authorised by the company.

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

- the authorised person states the company's CVR number;
- the authorised person states the subject's name or pseudonym, and CPR number where applicable;
- the OCES subject is provided with an activation password sent in a PIN code letter for installation of the private key and the associated certificate; or
- the OCES subject is provided with an activation password delivered via the authorised person for installation of the private key and the associated certificate.

If the activation password is delivered to the subject by the authorised person, the CA must also enter into an agreement with the subscriber under which the subscriber undertakes to establish a procedure ensuring that:

- transfer of the activation password from the authorised person to subjects is made in a secure manner;
- the subject acknowledges receipt of the activation password;
- transfer of the activation password from the authorised person and the subject's acknowledgement of receipt are logged; and
- the procedure and log are reviewed periodically by the company's management or a person appointed by the management (not the authorised person).

Generating and installing subject keys at the subject
When issuing a certificate with associated keys generated at the subject, the CA must establish an installation procedure ensuring that:

- the activation password for installation of the private key and the associated certificate is communicated to the authorised person via a secure electronic connection or is sent via a PIN code letter;
- the subject must enter its activation password to begin the installation of the private key and the associated certificate;
- subject keys are RSA keys with a minimum length of 2048 bit or similar;
- the public key is transferred to the CA together with information about the subscriber's identity in a message signed with the private key;
- the private key is encrypted and protected by the password;
- the personal password for activating the private key is generated and entered during the key generation process;
- the private key is activated once the subject has entered a personal password consisting of at least eight characters and containing at least one lower-case

letter, one upper-case letter and one digit; if a password is used in environments which can block effectively against exhaustive searches, it may, however, be selected from an outcome space of at least 10^4 possible codes, for instance as 4 digits selected from figures between 0 and 9; the use of a different password - e.g. biometrics - must implement a security standard at least at the same level as these requirements;
- the root certificate has been installed at the OCES subject; and
- the time and date of issuing the certificate can subsequently be determined.

In case private keys not protected by a cryptographic module are issued, the CA must, on its website, indicate a method for the subscriber to make a backup copy of the private key in encrypted form.

The CA must approve a certificate application if the procedure is completed as indicated.

The CA must ensure that from the time when the CA or an RA appointed by the CA has received a certificate application and until the information required for issuing a certificate has been sent to the certificate applicant, no more than one working day will pass on average within a running month. The time is never allowed to exceed three working days.

7.3.2 Certificate and key renewal

Renewal of an OCES certificate means using a valid certificate for issuing a new certificate according to this certificate policy to the same subject, with a new key pair, new validity period, a new certificate serial number, and the current OID. An OCES certificate may be renewed for up to four years at a time. The CA must ensure that a request for and issue of a renewed OCES certificate can be made online.

An OCES certificate can be renewed by the subject.

The CA must ensure that the request for renewal (certificate application) is signed with the subject's private key.

The verifying RA must validate the signature using the public key given in the certificate application.

The certificate application and issue must also meet the requirements in section 7.3.1 for generating and installing the subject's keys.

After revocation or expiry, or if the private key has been compromised, a certificate cannot be renewed. 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 is then handled like a new issue following the same guidelines as given in 7.3.1.

No later than 4 weeks before expiry, the CA must notify the subject of this via e-mail sent to the e-mail address registered by the CA. At the same time, the CA must also notify the authorised person of the expiry via e-mail or other electronic channels made

available to the authorised person. Alternatively, notification of the authorised person can be made by ordinary letter to the company's CVR postal address.

7.3.3 Certificate generation

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

OCES employee certificates must include:	***Solution***
Indication of the issuing CA identification and the country in which the certification authority is established	Issuer information contains the required information, i.e. as a minimum an unambiguous name and country code.
Subject name or a pseudonym; in the latter case it must appear that a pseudonym is used	CommonName contains name and/or pseudonym. If a pseudonym is used, the pseudonym is also placed in the Pseudonym field.
Specific information about the subject may be added, if relevant, depending on the purpose of the certificate	Subject serialNumber and other attributes contain information with suitable qualifiers. See further details in ETSI TS 101 862 and RFC 3039. The Subject SerialNumber format must follow the specifications for employee certificates in DS 844, section 4.3.
Signature verifying data corresponding to the signature generating data under the signer's control	X.509.v3.
Certificate commencement and expiry dates	X.509.v3 and RFC 3280.
Certificate identification code	The CA assigns the certificate a unique CA serial number. Together with the CA's identification, the number is completely unique. X.509.v3 and RFC 3280.
The issuing CA's advanced electronic signature	X.509.v3 and RFC 3280.
Limitations on the scope of use of the certificate, if applicable	KeyUsage, CertificatePolicies and Extended Key Usage.

The Subject certificate field

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

Attribute	**Requirements**	**Comment**
countryName	M	Country code

Attribute	Requirements	Comment
organizationName	M	The company's full name, including the CVR number where applicable
organizationalUnitName	O	Department
serialNumber	M	CVR:CVR number-RID:employeeId
postalAddress	O	The company's CVR address
givenName	O	The employee's first names
surname	O	The employee's surname
commonName	M	The employee's full name or registered pseudonym, including title where applicable
title	O	The employee's job title
emailAddress	O	The employee's e-mail address
pseudonym	O	The employee's pseudonym

Example:
countryName=DK,
organizationName= ABC // CVR:12345678,
emailAddress=tester@validdnsdomain.dk,
serialNumber=CVR:12345678-RID:employeeId,
commonName= Project Manager John Smith,
title=Project Manager

Rules:
CountryName=DK, organizationName, organizationalUnitName, serialNumber, givenName, surname, commonName and **pseudonym** must collectively and unambiguously point to the person who is the subject of the certificate. The CVR number must be contained in **serialNumber**. Fields not mentioned are optional.

Other fields (extensions)

The version number must be "v3".

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

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

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

digitalSignature (0)
contentCommitment (1)

The contentCommitment specification is set to inform recipients of certificates that the signature is binding on the subscriber in relation to the signed content.

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

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

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

In the tables below, the following codes are used:
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		
	1. Application	2. CA	3. End-user	4. Key Man.
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 signatures.

4. Generation of certificates to the end-user to be used for management/exchange of keys, e.g. in connection with the authentication/control of access rights.

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

7.3.4 Dissemination of terms and conditions

The CA must publish terms and conditions on its website for using certificates issued under this CP.

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

The CA must inform the subscriber that the private key must not be used until the OCES certificate has been received by the subject, apart from the use made during the certificate application process.

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

In addition, the CA must inform the subscriber that if the subscriber suspects that the private key has been compromised, the key must only be used for making a request for revocation. In case the private key is available to the subscriber, the private key may still be used for decrypting data which was encrypted using the associated public key.

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 associated private key.

The CA must inform the subscriber about the validity period of an OCES employee certificate and that an OCES employee certificate may be renewed if this is done 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 for issuing certificates under this CP.
- The CA must enable verification of the fingerprint of the root certificate via a different channel.
- Other certificates used for signing information between the CA, subscribers and verifiers (relying parties).
- This CP, as long as valid certificates issued under this CP exist, and as long as there are certificates on the revocation list of this CP.
- The CPS approved by the system auditor, except for specific trade secrets.
- List of all OCES employee certificates until at least two months after expiry of the validity period of the individual certificate. Excepted from this are the certificates to be kept secret.
- A revocation list for OCES employee certificates issued under this CP.

Revocation list information must be available without any kind of access control.

The CA must ensure that CA requirements imposed on the subscriber and verifier on the basis of this CP are summarised and documented, cf. sections 6.2 and 6.3.

7.3.6 Certificate revocation

Revocation of certificates, general

The CA must revoke an OCES certificate immediately if the CA becomes aware of one or more of the following conditions:

- The subscriber or subject wants to revoke the OCES certificate or terminate the use of this.
- The subject has lost access to the private key, e.g. as a result of losing the password.
- There is certainty or suspicion that the subject's private key has been compromised.
- The private key has been destroyed or lost in a different manner.
- The subject is no longer associated with the subscriber.
- Inaccuracy has been found in the content of the certificate or other information associated with the subscriber/subject, see also below regarding the subject's change of name.
- The subscriber's bankruptcy.
- The subscriber's business closes down.

If the subscriber changes its name, the CA must immediately notify the subscriber that the certificate is to be renewed within 30 days. If this is not made, the CA must revoke the certificate.

The CA's own violation of this CP shall not give the CA the right to revoke a certificate.

In case of a request for revocation, the CA must ensure that identification is made in a way that establishes the identity in the best possible manner, e.g. by a combination of subscriber/subject name, CVR number, CVR postal address and e-mail address.

A request for revocation can be made by the following:

- the subject;
- the authorised person;
- the CA, if the rules in this CP have not been met, or where warranted by the circumstances;
- persons authorised to sign for the company, upon showing proper documentation;
- a supervisor or liquidator, in case the subscriber has applied for a suspension of payments or has gone into liquidation;
- an administrator appointed by the probate court or heirs of the subscriber, in case the subscriber has passed away.

To the extent possible, the CA must ensure that the procedure for requesting revocation will not allow unauthorised revocation, while at the same time accepting authorised revocation by telephone, e-mail or online via the CA's website.

Requests for revocation

In case revocation is requested by telephone, the CA must ensure that the necessary information is submitted to ensure proper identification and that the reason for the requested revocation is stated.

Requests for revocation via online web forms or e-mail must contain the necessary information to ensure identification or be signed with the certificate desired to be revoked.

Further aspects regarding revocation

The CA must provide information about any revocation undertaken, via e-mail to the e-mail address stated in the certificate and to the authorised person's e-mail address or other electronic channels made available to the authorised person.

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 e-mail to the subject and to the authorised person's e-mail address.

In case of the subscriber's bankruptcy, the probate court or liquidator may request revocation. The above-mentioned methods may also be used. However, the CA must also send an acknowledgement of the revocation to the postal address stated by the probate court or liquidator.

Where a condition giving rise to revocation has been ascertained, the CA must ensure that revocation is made without undue delay.

An OCES employee certificate cannot be suspended.

Management of revocation lists

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

After a completed revocation, the CA must publish an updated revocation list. This must take place no later than 1 minute after revocation.

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

The CA must set the lifetime of the revocation list at 12 hours. The CA must publish a new revocation list each time a revocation is made, but no later than 6 hours before expiry of the current revocation list.

The CA must make revocation lists available for downloading via the following channels:

- LDAP
- HTTP

In addition, the CA must make revocation list information available via manual online lookup.

For revocation lists the CA must use a profile as stated in IETF RFC 3280. **thisUpdate** and **nextUpdate** must be stated in **UTCTime** format YYMMDDHHMMSSz.

The version number of the revocation list must be stated and set at "v2". There is no requirement to use CRL extensions.

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

For OCSP the CA must use a profile in accordance with IETF RFC 5019.

The OCSP response may be pregenerated, but it is required that if a certificate is revoked, then the associated OCSP response must be regenerated, and no later than 1 minute after the revocation has been registered the OCSP response must indicate that the certificate has been revoked.

OCSP responders must be provided with dedicated company certificates used exclusively for OCSP. Besides the formalities required for a company signature, the following requirements must be met by the contents:

- Key Usage: Digital Signature
- Extended Key Usage: OCSP Signing
- CRL Distribution Point: Not included
- AIA: Not included
- OCSP No Check: Included but empty

The lifetime of OCSP responder certificates must be 72 hours as a maximum, and the associated keys must be protected by cryptographic modules in line with other CA keys, as indicated in section 7.2.1.

The CA must make sure that revocation lists are not compromised, and that the revocation lists and OCSP services are available via the Internet 24 hours a day, 7 days a week. The services must have an average response time not exceeding 1 second measured at the server entry, i.e. from the time when the server has registered the request until it returns a response.

7.4 CA management and operation

The requirements in section 7.4 solely address the RA where this is explicitly mentioned.

7.4.1 Security management

The CA must ensure that its administrative and management procedures are adequate and conform to the basic requirements of Danish Standards' "Code of practice for information security management DS 484".

To the extent that the CA estimates that the special conditions regarding CA operation justify requirements for stricter security measures, i.e. compliance with stricter requirements as described in DS 484, these must be applied. In the annual CA report the CA must describe what requirements on stricter security measures have been implemented.

The CA must assume full responsibility for all services made available, directly or indirectly, for managing certificate issue and status information.

The CA must ensure that persons with auditing functions at the CA do not report to the same managers as operations officers and administrators.

7.4.2 Asset identification and classification

The CA must meet the basic and stricter requirements of DS 484 in accordance with the provisions of section 7.4.1.

7.4.3 Personnel security

Security classification procedures

The CA must check that managers and employees performing trusted assignments at or for the CA have not been convicted of a crime that makes them unsuitable for performing their job. This also applies to RA employees.

Check of subcontractors

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

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

RA personnel must receive training that will enable them to perform their work correctly and securely.

7.4.4 Physical security

General

The CA must clearly identify the localities at which 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.

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

In case of evacuation, the CA operation facilities must be capable of functioning via remote control without changes in operation. By remote control is understood the possibility of operating CA functions via a PC etc. from a facility physically separate from CA operations, e.g. where the CA has established a backup system.

Physical access
General
The CA must ensure that all facilities have perimeter protection conforming to DS 471 or better.

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 on video.

Storage and processing of data in other localities
If data is stored or processed at a different locality, the CA must ensure that this is subject to compliance with the same security requirements as those applying to the CA's main systems.

7.4.5 Management of the operation of IT systems and networks
The CA must meet the basic and stricter requirements of DS 484 in accordance with the provisions of section 7.4.1.

7.4.6 Management of access to systems, data and networks
The CA must meet the basic and stricter requirements of DS 484 in accordance with the provisions of section 7.4.1.

The CA must make RA systems available ensuring that only authorised RA personnel have access to operate such systems.

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

Prior to any system development (i.e. internal development or development by a third party), the CA must ensure that there is a management approved plan for integration of security in the systems.

7.4.8 Emergency preparedness planning
The following incidents must be considered serious:

- Compromise of the CA private key.
- Suspicion of compromise of the CA private key.
- Breakdown and critical errors on CA operating components (revocation lists etc.).
- Stoppage of the CA operating environment due to fire, power failure etc.

If the CA private key has been compromised, or if this is suspected, the CA must immediately inform all subscribers via the registered e-mail address. The CA must also inform the National IT and Telecom Agency immediately, with a detailed description of the situation that has arisen.

The CA must also inform verifiers (relying parties) immediately on its website, and to the extent found relevant in view of the situation arisen, via public media or by direct contact.

In case of serious incidents on data processing equipment, software and/or data, the CA must inform subscribers thereof to the extent that it is relevant to their use of the CA services. In view of the situation arisen, the verifiers (relying parties) must be informed via public media and announcements 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 after a breakdown.

7.4.9 CA termination

The CA must ensure that all issuing and renewal of certificates are stopped immediately when a CA function ceases to operate.

Prior to termination, the CA must inform subscribers and all other parties that have contractual relations to the CA.

The CA must ensure the continued maintenance of revocation lists and requests for revocation until all certificates issued by this CA have expired or have been transferred to another CA that meets the requirements of this CP.

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

7.4.10 Compliance with legislation

The CA and RA must ensure compliance with legal requirements, in particular the Act on Processing of Personal Data.

Special obligations regarding the protection of confidential information

Information included in certificates is considered non-confidential.

Person-related information not included in the certificate is considered private information.

Information included in certificates is considered non-private.

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

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

The CA and RA must ensure that statistical information about the use of OCES employee certificates cannot be related to the individual OCES certificate (cf. the Act on Processing of Personal Data).

If a dispute cannot be settled by conciliation, either of the parties may choose to bring the dispute before the ordinary courts. The venue is Copenhagen. The applicable law is Danish law.

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 secure operation of the CA in accordance with this CP. In addition, the CA must ensure that:

- all information is protected against unauthorised access;
- all security critical activities and activities requiring participation of more than one person are logged;
- all information about registration, including certificate renewals, is logged;
- all accesses and access attempts to areas that must be protected by access control are logged;
- all video monitoring is logged;
- there are written rules for regular review of all logs;
- all audit logs are signed electronically and are time stamped;
- audit logs are treated as confidential material;
- audit logs are backed up at regular intervals.

The CA must ensure that backup data is stored in accordance with the requirements of DS 484.

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 archived:

- all logs;
- certificate applications and associated communication;
- signed orders and written agreements;
- certificate renewals; and

- CPS and CP.

The CA must ensure that archived information can be made available in case of disputes, and that all archived material is kept for at least the current calendar year + five years. This also applies to any data from the RA's IT systems relevant to documenting the CA's activities.

The CA and RA must ensure that all material in archives is stored in accordance with the requirements of DS 484.

The CA and RA must ensure that backup copies are made of all electronic archive material at regular intervals.

The CA and RA must ensure that all electronic archive material is provided with an electronic time stamp 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 natural or legal person.

The CA must ensure equal access to all services within the scope of the OCES employee certificates. This means that terms and conditions for access to services must be non-discriminatory.

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 assumed as a CA, including the obligations in section 7.4.9, partly through insurance, and partly through equity capital.

The CA must at all times have at its disposal a sufficient number of trained personnel for operating, in an adequate manner, all services provided. The staff must at all times possess the skills prescribed for the trusted positions.

The CA must ensure that policies and procedures are in place for handling customer inquiries or inquiries from verifiers.

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

7.6 Data centre location

The requirements of this CP are applicable no matter whether the CA places all or parts of the operating environment abroad. Thus it must be possible to perform the ongoing check prescribed in the CP irrespective of the CA's geographic location.

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