COMMFIDES
Secure Communication & Online Identity Management

CERTIFICATE POLICY
CERTIFICATE PRACTICE STATEMENT

COMMFIDES SHA256 CLASS 3 PERSON STANDARD CERTIFICATES

For CA CPN PERSON STANDARD SHA256 CLASS 3

Version 1.0
Date 28.03.2011

Policy Identifier: 2.16.578.1.29.11.1.1.0

PUBLIC

Commfides Norge AS
Postal address: PO Box 1327 Lysaker
Visitor address: Fornebuveien 1, 1366 Lysaker
Tel.: +47 22 55 62 60
Fax: +47 22 55 62 76
E-mail: servicedesk@commfides.com
Business nr.: 988 312 495

History of change

Version	Date	Status	Description
1.0	28.03.2011	Approved	Initial version for the new SHA256 Root Structure for CPN. Approved by the Commfides (CN) Certificate Advisory Board (CAB).

Innholdsfortegnelse

Definitions

Term	*Definition*
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Administrator	Trusted Person within an organization which is a Managed Customer, RA or CA that performs validations and other CA or RA functions.
Agent	Any individual, organization or other entity that acts as Agent on behalf of a CTE Member to undertake their activities on their behalf in marketing, selling, supporting and servicing CTE Member's products and services.
Applicant	The Certificate Applicant
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a CA of the certificates which it has issued that is revoked prior to their stated expiration date. The list is periodically issued by and digitally signed by the CA.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs
CN Certificate Advisory Board (CAB)	Certificate Advisory Board is a part of Change Advisory Board that is responsible for changes made to the CP/CPS. All changes must be approved by the CAB
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked. CA Facility The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Management Authority (CMA)	The group within CN responsible for the promulgation of this CPS.
Certificate Operational Period	The period starting from the date and time a Certificate is issued and ending on the earlier date and time a Certificate expires or is otherwise earlier revoked.
Certificate Policy (CP)	A CP is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services). References to “the CPS” or “this CPS” refer to this document.
Class	A specified level of assurance as set-out in Section 1.1.1.
CN Trust Environment (CTE)	The Certificate-based Public Key Infrastructure governed by the CN Certificate Policies, which enables the worldwide deployment and use of Certificates by CN and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
CN UNID Service	CN have developed an UNID service in accordance with SEID leveranse nr 2 – Grensesnitt for tilgang til oppslagstjenester.
CN Professional Network (CPN)	The CN Hierarchy from root and trusting certificates
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
CTE Participant	An individual, organization or other entity with participation in the CTE including: CN, its Licensees, RAs, LRAs, Resellers, Agents, Customers, Subscribers and Relying Parties.
CTE Standards	The business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, Certificates within the CTE and providing associated trust services.
Customer	A person, organization or other entity that has contracted with a CTE Member of its affiliates, Resellers or Agents for Certification Services.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; “date of issue” and “date of next issue”.
Key Escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.
Local Registration Authority (LRA)	Carry out registration tasks on behalf of and is under the authority of a RA.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique

	alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Relying Party Agreement	An agreement used by a CA to set out the terms and conditions for acting as a Relying Party
Reseller	An entity that markets services on behalf of a CTE Member or its affiliates.
Root CA	The CA whose public key serves as the most trusted datum (i.e.,the beginning of trust paths) for a security domain.
Sub domain	The portion of the CTE under the control of a CTE Member and including all entities subordinate to it.
Subject	The holder of a Private Key corresponding to a Public Key. The term “Subject” can refer to a device or server that holds a Private Key.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions to be a Subscriber.
Subscriber	Legal entity or natural person that is issued a Certificate by CN
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
Trusted Persons	Persons, including employees, subcontractors or consultants of entities within the CTE who are responsible for managing infrastructure, an entities services, facilities and/or its practices.
Trusted Position	A position within the CTE that must be held by a Trusted Person.

ACRONYMS AND ABBREVIATIONS

AA	Authentication Authority
CA	Certification Authority
CARL	Certificate Authority Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
SOA	Statement of Applicability
CRL	Certificate Revocation List
CTEDN	CN Trust Environment Distinguished Name
ICC	International Chamber of Commerce
LRA	Local Registration Authorities
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RAA	Registration Authority Administrator
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA256	A family of two similar hash functions within SHA-2, with different block sizes, known as SHA-256 and SHA-512
S/MIME	Secure Multipurpose Internet Mail Extension
SSL/TSL	Secure Sockets Layer/Transport Security
U.S.C.	United States Code
WWW	World Wide Web

References

- Directive 1999/93/EC of 13. December 1999 on a Community Framework for Electronic Signatures.
- IETF RFC 2527 (1999): “Internet X.509 Public Key Infrastructure –Certificate Policy and Certification Practices Framework”, S. Chokhani, W.Ford.
- ITU-T X.509(03/00): Information technology – Open Systems Interconnection – The Directory : Public-key and attribute Certificate frameworks
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- The SEID Project - Publication: Task 1 – “Recommended certificate profiles for person certificates and enterprise certificates” Version 1.01
- The SEID Project Task 2 – ”Grensesnitt for tilgang til oppslagstjenester”
- ETSI TS 101 862: “Qualified Certificate profile”.
- ETSI TS 101 456: “Policy requirements for certification authorities issuing qualified certificates”.
- ETSI TS 102 042: “Policy requirements for certification authorities issuing public key certificates”.
- ETSI-102-176-1v2.0.0 “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures;
- ISO 27001 - ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements.
- Act on electronic signatures: LOV 2001-06-15 nr 81. http://www.lovdata.no/all/hl-20010615-081.html.
- RFC 3280 (2002): “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”
- NOU 2001:10, “Uten Penn og blekk”.
- Forskrift om frivillige selvdeklarasjonsordninger av 21. november 2005 nr. 1296
- Lov 14.april 2000 nr.31 om behandling av personopplysninger (personopplysningsloven)
- Forskrift 15.des 2000 nr.1265 om behandling av personopplysninger (personopplysningsforskriften)
- Kravspesifikasjon for PKI i offentlig sektor Versjon 2.0

1. Introduction

1.1 Overview

This document is structured according to RFC 2527 [RFC2527]. Not all sections of RFC 2527 are used. Sections that are not included have a default value of “No stipulation”

A **C**ertificate **P**olicy (CP) states the applicability of a certificate and defines the security requirements that are applied to the complete certificate lifecycle operated by the signing CA.

A **C**ertification **P**ractice **S**tatement (CPS) describes how the certificate policy is implemented in the context of the operating policies, system architecture, physical security, and computing environment of the CA organization. For example, a certificate policy might specify that end entity must be duly authenticated, so the CPS describes how this is accomplished by the PKI that is deployed.

CN Norge AS (CN) is a CA that offers products and services for the complete e-ID lifecycle by the use of PKI certificates. The CA is located physical in Lysaker Norway and is enhanced to fulfil the Norwegian Law “esignaturloven” and the specific requirements set by the Official PKI demands in Norway. The root and operating CA is fully managed and set up for the CN Trust Environment (CTE) by CN

This CP is aligned with the LCP as defined in ETSI 102-042

CPN Person Standard Certificates - provide a medium level of assurance within the CTE. CPN Professional Certificates are issued to individuals and Administrators for CAs and RAs. CPN Professional individual Certificates may be used for digital signatures, encryption, and access control, including as proof of identity, within the Subscriber's defined group of Professional users. CPN Professional individual Certificates provide assurances of the identity of the Subscriber based on their affiliation with the defined group of Professional users and on the verification by the Subscriber's Professional RA, based on, at a minimum, the Subscriber's Professional records or files.

1.2 Identification

This CP covers the Intermediate CA for:

- CN CPN Person-Standard SHA256 CA v.1.0
  Policy identifier=2.16.578.1.29.12.1.1.0

- OBJECT IDENTIFIER::= {joint-iso-itu-t(2) country(16) Norway(578) organisation(1) CN (29)

Commfides is following the QCP public + SSCD identifier:
Itu-t(0) identified-organization(4) etsi (0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd (1)

Certificate Policy Object Identifiers are used in accordance with Section 7.1.6.

The 'CPN RootCA SHA256 Class 3' CA is signing the following Intermediate CAs, identified as:

CPN Person-Standard SHA256 CA	v.1.0	Policy identifier=2.16.578.1.29.11.1.1.0
CPN Person-High SHA256 CA	v.1.0	Policy identifier=2.16.578.1.29.12.1.1.0
CPN Enterprise Norwegian SHA256 CA	v.1.0	Policy identifier=2.16.578.1.29.13.1.1.0
CPN ADMIN SHA256 CA	v.1.0	Policy identifier=2.16.578.1.29.101.1.1.0
CPN Miscellaneous SHA256 CA	v.1.0	Policy identifier=2.16.578.1.29.201.1.1.0

1.3 Community and Applicability

CTE applies to all CN Participants, including CN and its Licensees, RAs, LRAs, Resellers, Agents, Customers, Subscribers, End Entities, and Relying Parties.

1.3.1 Applicability

CPN Person-Standard SHA256 CA signed certificates may only be used for PKI based services between organizations as well as between organizations and private consumers. Organizations can be private or governmental.

CPN Person-Standard SHA256 CA can be used to:

- Authenticate the identity of an Person only alone or a Person and a Organization as the Subscriber
- Sign and verify signed data such as documents or e-mail

- Encrypt and decrypt data and exchange symmetric keys used for encryption

All organizations that are certificate subscribers must be registered in the Norwegian Central Coordinating Register for Legal Entities (one of the national computerized registers In the Brønnøysund Register Centre).

Subjects or End entities under this policy MUST be a Person

1.4 Contact Details

CN is responsible for all aspects of the CTE, CP and the CPS. Inquiries to CN should be addressed as follows:

CN Norge AS,
Fornebuveien 1,
PO-box 405
N-1327 Lysaker Norway
Attn: CN Practices Development – CPS

Telephone: +47 21 55 62 60 (voice)
Email: servicedesk@Commfides.com

2. General Provisions

2.1 Obligations

2.1.1 CA Obligations

CTE CAs performs the specific obligations appearing throughout the CPS including:

- Accept certification requests from entitled entities;
- Notify the RA of certification request and accept authentication results from the RA;
- Issue Certificates based on the requests from authenticated entities;

- Notify the Subscriber of the issuing of the Certificate;
- Publish the issued Certificate in accordance with the procedures outlined in the CPS;
- Accept revocation requests according to the procedures outlined in the CPS;
- Authenticate entities requesting the revocation of a certificate, (generally by delegating this task to a responsible RA);
- Issue a Certificate Revocation List (CRL);
- Publish the issued CRL; and
- Keep audit logs of the certificate issuance process.

As a condition of enrolment, a Subscriber must assent to a Subscriber Agreement. As a condition of receiving Certificate status information, similarly, RAs, LRAs, Resellers and Agents (where required by contract) must use Subscriber Agreements in accordance with the requirements imposed by the CPS. The Subscriber Agreements used by CTE Members, RAs, LRAs, Resellers and Agents must include the provisions required by Sections 2.2-2.4.

If a Licensee or other Business Partner has no Subscriber Agreement that has been approved by CN, the Subscriber Agreement of CN shall apply.

The community governed by the CPS is the CTE. This CP spans the Norwegian community for all legal persons with a verified F-nr or D-nr in the “Folkeregisteret” (DSF). For Person Standard certificates a person must be of the age of 14 years old or older.

2.1.2 RA Obligations

RAs assist a CA by performing validation and registration functions, approving or rejecting Certificate Applications, requesting revocation of Certificates, and approving renewal requests. RAs who perform such functions within the CTE shall comply with the CPS and the terms of any agreement between the RA and a CTE Member.

RA’s obligations include the following:

- Accept authentication requests from CTE CAs;
- Authenticate entity or person making the certification request according to procedures outlined in the CPS;
- Notify the CTE CA when authentication is completed for a certification or revocation

request;

- Accept revocation requests according to the procedures outlined in the CPS;
- Notify the CTE CA of all revocation requests; and
- Not approve a Certificate with a life time greater than that specified in this document

RAs must appoint one or more Trusted Persons as Administrators ("RAAs") who will be responsible for carrying out the RA functions using CN managed PKI systems.

The provisions of the CPS satisfy the obligations of each category of RA. Additional guidelines and requirements are described in the RAs operation agreement with a CTE Member

2.1.3 Subscriber Obligations

Subscriber obligations in the CPS apply to Subscribers within the CTE. Within the CTE, Subscriber Agreements require that Certificate Applicants provide complete and accurate information on their Certificate Applications and assent to the applicable Subscriber Agreement as a condition of obtaining a Certificate.

Subscriber Agreements require Subscribers to use their Certificates in accordance with Section x.x.x and to protect their private keys in accordance with Sections x.x-x.x. Under these Subscriber Agreements, if a Subscriber discovers or has reason to believe there has been a Compromise of the Subscriber's Private Key or the Activation Data protecting such Private Key, or the information within the Certificate is incorrect or has changed, that the Subscriber must promptly:

- Notify the entity that approved the Subscriber's Certificate Application, either a CA or an RA, in accordance with Section x.x.x.x and request revocation of the Certificate in accordance with Sections x.x, x.x.x.x, and
- Notify any person that may reasonably be expected by the Subscriber to rely on or to provide services in support of the Subscriber's Certificate or a digital signature verifiable with reference to the Subscriber's Certificate.

Subscriber Agreements require Subscribers to cease use of their private keys at the end of their key usage periods under Section x.x.x. Subscriber Agreements state that Subscribers shall not monitor, interfere with, or reverse engineer the technical implementation of CTE Members, except upon prior written approval from CN, and shall not otherwise intentionally compromise the security of the CTE.

2.1.4 Subcontractor Obligations

The CA shall have agreements with all parties that involve subcontracting, outsourcing or other third party arrangements.

2.1.5 Relying Party Obligations

Relying Parties must independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose. They state that CTE CAs and RAs are not responsible for assessing the appropriateness of the use of a Certificate. Relying Parties must not use Certificates beyond the limitations in Section 1.3.4.2 and for purposes prohibited in Section 1.3.4.3.

Relying Parties must utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. Under these Agreements, Relying Parties must not rely on a Certificate unless these verification procedures are successful.

Relying Parties is required to check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate Chain in accordance with Sections 4.4.10, 4.4.12. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party must not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain.

Relying Party Agreements state that assent to their terms is a condition of using or otherwise relying on Certificates. Relying Parties that are also Subscribers agree to be bound by Relying Party terms under this section, disclaimers of warranty, and limitations of liability when they agree to a Subscriber Agreement.

If all of the checks described above are successful, the Relying Party is entitled to rely on the Certificate, provided that reliance upon the Certificate is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Relying Party Agreements state that Relying Parties must not monitor, interfere with, or reverse engineer the technical implementation of the CTE, except upon prior written approval from CN, and shall not otherwise intentionally compromise the security of the CTE.

2.1.6 Repository Obligations

No Stipulations

2.2 Liability

For CPN Person-Standard SHA256 CA signed certificates CN pursues the liability for Certificates issued under this policy as specified in Article 6 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures."

CN limited liability:

NOK 5000, - pr. transaction

Certificate owner and Relying Parties may choose to enhance this limited liability by buying a higher coverage

2.3 Financial Responsibility

This CPS contains no limits on the use of any Certificates, issued by CN or by CTE CAs. Parties acting as Relying Parties shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction. This determination is entirely at the discretion of the Customer and Subscriber as Relying Party and is likely to depend upon several factors in addition to the certificate assurance level such as likelihood of fraud, other procedural controls, specific policy or statutorily imposed constraints.

2.3.1 Indemnification by Subscribers and Relying Parties

2.3.1.1 Indemnification by Subscribers

To the extent permitted by applicable law, CN' Subscriber Agreement requires, and other Subscriber Agreements shall require, Subscribers to indemnify CN, its Licensees and any non-CN CAs or RAs for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application;

- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party;
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key; or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

2.3.1.2 Indemnification by Relying Parties

To the extent permitted by applicable law, CN' Relying Party Agreements and other Relying Party Agreements require Relying Parties to indemnify CN and its Licensees and any non-CN CAs or RAs for:

- The Relying Party's failure to perform the obligations of a Relying Party;
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances; or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Subject to any limits appearing in applicable law, the laws of the Kingdom of Norway.

This governing law provision applies only to the CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that the Section 2.4.1 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

The CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

2.4.2 Severability, Survival, Merger, Notice

To the extent permitted by applicable law, CN' Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements and Relying Party Agreements shall contain, severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

2.4.3 Severability, Survival, Merger, Notice

To the extent permitted by applicable law, CN' Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements and Relying Party Agreements shall contain, severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

2.4.4 Dispute Resolution Procedures

No Stipulation

2.4.4.1 Disputes among CTE Members and Customers

Disputes between a CTE Member and one of its Customers shall be resolved pursuant to provisions in the applicable agreement between the parties.

2.4.4.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, CN' Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements and Relying Party Agreements shall

contain, a dispute resolution clause. The clause states that dispute resolution procedures require an initial negotiation period of sixty (60) days followed by litigation in the federal or provincial court encompassing the city of Oslo, Norway.

2.5 Fees

The fees for services provided by CN in respect to CN Certificates will be published on the CN web pages (www.commfides.com).

2.6 Publication and Repositories

2.6.1 Publication of CA information

CN is responsible for the repository function for its CAs and those of other CTE CAs. CN publishes certain CA information in the repository section of CN' web site at http://www.Commfides.com as described below. CN publishes the CPS and Subscriber Agreements in the repository section of CN' web site.

2.6.2 Frequency of Publication

Updates to the CPS are published in accordance with Section 8. Updates to Subscriber Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with Sections 4.4.9, 4.4.11.

2.6.3 Access Controls

Information published in the repository portion of the CN web site is publicly-accessible information. Read only access to such information is unrestricted. CN requires persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. CN has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

2.6.4 Repositories

No Stipulation

2.7 Compliance audit

CN has achieved ISO 27001 certification and the practices and procedures set forth in this CP and CPS will be part of the annual ISO 27001 audit.

2.8 Confidentiality

2.8.1 Types of Information to be kept confidential and private

The following records of Subscribers are, subject to Section 2.8.2, kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved;
- Certificate Application records (subject to Section 2.8.2);
- Transactional records and the audit trail of transactions;
- CTE Member's audit reports created by CN, another CTE Member or their respective auditors (whether internal or public);
- Contingency planning and disaster recovery plans; and
- Security measures controlling the operations of CN hardware and software and the administration of Certificate Services and designated enrollment services.

2.8.2 Types of Information Not Considered Confidential or Private

CTE Participants acknowledge that Certificates, Certificate revocation and other status information, CN' repository, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 2.8.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

See Section 2.8.2.

2.8.4 Release to Law Enforcement Officials

CTE Participants acknowledge that CTE Members shall be entitled to disclose Confidential/Private Information if, in good faith, CTE Members believe that disclosure is necessary in response to subpoenas and search warrants. This section is subject to applicable privacy laws.

2.8.5 Release as Part of Civil Discovery

CTE Participants acknowledge that CTE Members shall be entitled to disclose Confidential/Private Information if, in good faith, CTE Members believe that disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents. This section is subject to applicable privacy laws.

2.8.6 Disclosure upon Owner's Request

CTE Members' privacy policies contain provisions relating to the disclosure of Confidential/Private Information to the person disclosing it to a CTE Member. This section is subject to applicable privacy laws.

2.9 Intellectual Property Rights

The allocation of Intellectual Property Rights among CTE Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such CTE Participants. The following subsections of Section 2.9 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

2.9.1 Property Rights in Certificates and Revocation Information

CAs retains all Intellectual Property Rights in and to the Certificates and revocation information that they issue. CTE Members and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. CTE Members and Customers shall grant permission to use

revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

2.9.2 Property Rights in the CP

CTE Participants acknowledge that CN retains all Intellectual Property Rights in and to the CPS.

2.9.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

2.9.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates. Without limiting the generality of the foregoing, CTE Member's public keys and the Certificates containing them are the property of the respective CTE Member.

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

CN CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields. CN Issuer Distinguished Names consist of the components specified in the table below.

Attribute	***Value***
Country (C)	The CAs country or origin.
Organization (O)	Indicates the controlling Organization of the CA
Organizational Unit (OU)	CN CA Certificates contain several OU attributes which specify the CA's position in the CTE hierarchy and type of Certificate issued.
State or Province (S)	Indicates the CAs state or province.
Locality (L)	Indicates the CAs city.
Common Name (CN)	This attribute is the common name of the CA.

End-user Subscriber Certificates contain an X.501 Distinguished Name in the Subject name field and consist of the components specified in Table 5 below.

Attribute	***Value***
Country (C)	Indicates the Subscriber's Country or not used.
Organization (O)	Subscriber's organizational or company name for Subscriber's personal certificate or not used.
Organizational Unit (OU)	CN end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: Subscriber organizational unit. An indication of which CA issued the Certificates. "Authenticated by CN" or other entity in Certificates whose applications were authenticated by CN or other entity. "Persona Not Validated" for CPN International Class 3 Certificates Text to describe the type of Certificate.
State or Province (S)	Indicates the Subscriber's state or province or not used.
Locality (L)	Indicates the Subscriber's locality or not used.
Common Name (CN)	This attribute includes the name of the individual or device (hostname in the case of server Certificates).

The Common Name (CN=) component of the Subject Distinguished Name of end-user Subscriber Certificates is authenticated in the case of Person Standard and Person High Class Certificates. The Common Name value included in the Subject Distinguished Name of individual Certificates represents the individual's generally accepted personal name. For Person-Standard certificates, Subject name e.g. subscriber name, system name, application name, or Domain name owned by the Company can be included.

3.1.2 Name Meanings

Person Standard and Person High Class end-user Subscriber Certificates contains names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate. For such Certificates, pseudonyms of end-user Subscribers (names other than a Subscriber's true personal or organizational name) are not permitted.

For Person-Standard certificates the full name as stated in the national registry of persons and legal status of the Subscriber as defined in the Central Coordinating Register for Legal Entities must be used and it must be able to identify both Certificate Applicants and Subject Sponsors as Authorized Subscriber Representatives.
CTE CA Certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

For use of email address, the address must be meaningful

3.1.3 Uniqueness of Names

CTE Members ensure that Subject Distinguished Names are unique within the domain of each CTE CA.

3.1.4 Method to Prove Possession of Private Key

CTE Members verify the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS #10, another cryptographically-equivalent demonstration, or another CN-approved method.

Where a key pair is generated by CTE Members on behalf of a Subscriber such as where pre-generated keys are placed on smart cards, this requirement is not applicable.

3.1.5 Authentication of Organization Identity

The following information about the Subscriber must be presented to the CTE Members during registration:

- Full name and legal status of the Subscriber as defined in Brønnøysundregistrene
- The Subscribers' Organization Number as defined in the Brønnøysundregistrene.
- A Subscriber Certificate that identifies the person who is by the Subscriber organization given the signature right for the Subscriber organization or per procurator.
- Physical address, or other means, which give information on how the Subscriber can be contacted.
- CTE CA Certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.
- The Serial Number must be included. Serial Number maps to "Fødselsnummer". Relying Parties who are authorized may obtain the "Fødselsnummer" from CA, through the Commfides "UNID service" as defined in "The SEID Project Task 2 – Grensesnitt for tilgang til oppslagstjenester".

3.1.6 Authentication of Individual Identity

For all Classes of Individual and Enterprise Certificates, CTE Members confirm that:

- The Certificate Applicant is the person identified in the Certificate Application
- In case of a electronic application, the Certificate Applicant rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with Section 3.1.7; and
- The information to be included in the Certificate is accurate, except for Non-Verified Subscriber Information.

In addition, CTE Members perform more detailed procedures described below (3.1.10, 3.1.11) for each Class of Certificate.

3.1.7 Identification and Authorization of Subscriber Representatives

CTE Members must be able to identify the Certificate Applicants as Authorized Subscriber Representatives.

a) A person that has signature rights for the Subscriber organization or a procurator as identified by a formal Subscriber Certificate must be considered an Authorized Subscriber Representative.
b) Proof of holding the rights for signing on the behalf of the Subscriber organization for a Certificate Applicant that is not covered by a) must be given through a Subscriber

Authorization Statement which

1. Identifies the person by first name, middle and last name and social security number as registered in the National Registry of Persons (DSF) or equally International registry.

2. Is signed by one of the persons that by the Subscriber organization have a right to sign or per procurator as identified by the Subscriber Certificate.

A certificate must not be issued if any of these requirements are not met.

If the information in the Certificate Application is supported by verification by the Authentication Authority, CTE Members may approve the Certificate Application.

The record is subsequently archived for 10 years.

3.1.8 Authentication of Authorized Subscriber Representatives

Before a Certificate can be distributed to a Subscriber, Subject or any Relying Party at least one Authorized Subscriber Representative involved in the certification process (Certificate Applicant) must be authenticated, in person or electronically;

A formal Subscriber Certificate may not be mandatory if the CA can obtain the required information directly from a trusted source, e.g. the Brønnøysundregistrene.

a) In person: The Authorized Subscriber Representative must authenticate himself/herself in person towards a CTE Member representative by presenting a nationally recognized identity document. Identity documents accepted is stated in the”Hvitvaskingsforskriften, §4”. The CTE Member representative must verify that the documents are acceptable and valid.

b) Electronically: The Authorized Subscriber Representative must authenticate himself/herself electronically towards the CTE Members system using an electronic “Person-Standard Class” certificate issued by a CA registered in the Norwegian Post and Telecommunications website as a issuer of qualified certificates.

Additional requirements for the use of electronic authentication are:

a) The electronic credential issuance to the Authorized Subscriber Representative must be according to section 3.1.7.

3.2 Routine Rekey

Subscriber Certificates, which have not been revoked, may be renewed.

3.3 Rekey after Revocation

Re-key after revocation is not be permitted if:

- Revocation occurred because the Certificate was issued to a person other than the one named as the Subject of the Certificate;
- The Certificate was issued without the authorization of the person named as the Subject of such Certificate; or
- The entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.

Subject to the foregoing paragraph, Subscriber Certificates, which have been revoked, may be replaced (i.e., re-keyed) in accordance with the table below.

Timing	***Requirement***
Prior to Certificate expiration	For replacement of a Certificate following revocation of the Certificate, CN verifies that the person seeking certificate replacement is, in fact, the Subscriber (for individuals) or an authorized organizational representative (for devices), as described in Sections 3.1.8, 3.1.9. In addition the requirements for the validation of an original Certificate Application in the subsections of Section 3.1.8, 3.1.9 are used for placing a Certificate following revocation. Such Certificate contains the same Subject Distinguished Name as the Subject Distinguished Name of the Certificate being replaced.
After Certificate expiration	The requirements specified in Sections 3.1.8, 3.1.9 for the authentication of an original Certificate Application shall be used for replacing an end-user Subscriber Certificate.

3.4 Revocation Request

4. Operational Requirements

4.1 Certificate Application

A certificate application is the process where administrators on behalf of a subscriber request a certificate issuance from the RA, LRA or CA.

For CTE Certificates, all Certificate Applicants shall undergo an enrolment process consisting of:

- completing a Certificate Application and providing the required information;
- assenting to the relevant service(s) agreement; and
- assenting to the relevant Subscriber Agreement.

CA shall control the application records for completeness and consistency and verify that there is a match in the National Register of Persons (Det Sentrale Folkeregisteret – DSF) for the application record.

4.1.1 Subscriber Agreement

A subscriber MUST have a signed a written subscriber agreement with CN before any certificate application can be processed. The subscriber agreement can be a part of the certificate application. The subscriber agreement must be signed by the persons holding the signature right or procurement right as stated in the Norwegian national business register. The holder of the signature right or procurement MAY delegate with a power of attorney the right to sign the subscriber agreement on the behalf of the subscriber.

4.1.2 Validation

All persons signing a subscriber agreement according to section 4.1.1 above and persons signing Certificate applications shall authenticate themselves according to section 3.1. In case of a power of attorney, this must also be validated with the holder of the signature right or procurement.
CA controls the subscriber agreement and certificate application records for completeness and

consistency and verifies that there is a match in the National Register of Persons (DSF) for the application record.

If an email address is recorded in the application, a check if the domain name is a valid domain name must be verified.

Certificate Applications are submitted to CTE Members or other RAs for evaluation and either accepted or denied. Once a Certificate Application has been accepted by a CTE Member or other RA ("RA Approved Certificate Application") a request to issue a Certificate is then submitted to the applicable CTE CA. CTE CAs evaluates the requests they receive for Certificate issuance and either approve and process the request or denied it.

4.2 Certificate Issuance

After a Certificate Applicant submits a Certificate Application, the CTE Member or other RA (see Section 4.1.1) attempts to confirm the information in the Certificate Application (other than Non Verified Subscriber Information) pursuant to Sections 3.1.8, 3.1.9. Upon successful performance of all required authentication procedures pursuant to Section 3.1, The CTE CA or other RA approves the Certificate Application. If authentication is unsuccessful, The CTE CA or other RA denies the Certificate Application.

A CTE CA confirms the RA approved Certificate Application contained in the request to issue a Certificate for its adherence to CN Standards and either denies the request or completes processing and creates and issues a Certificate to the Certificate Applicant. CTE CAs create and issue a Certificate to a Certificate Applicant based on the verified information in a Certificate Application

4.3 Certificate Acceptance

Upon Certificate creation, CTE Members notify Subscribers that their Certificate is available and

notifies them of the means for obtaining such Certificate.
Upon issuance, Certificates are made available to end-user Subscribers on hardware tokens or Smart Cards, and on CD/DVD for machine based certificates.
End-user Subscriber key pairs are pre-generated by CTE Members on hardware tokens or smart cards and such devices are distributed to the end-user Subscriber, acceptance of these devices and their corresponding PIN numbers on the part of Subscriber constitutes the Subscriber's acceptance of the Certificate.

4.4 Certificate Suspension and Revocation

CA shall on authorized requests revoke or suspend certificates 24 hours a day, 7 days a week within 1 hour after CA received the request.
Revocation status shall be made available through online certificate status protocol (OCSP) immediately after revocation and no longer than 24 hour through certification revocation lists (CRL)

4.4.1 Circumstances for Revocation

4.4.1.1 Circumstances for Revoking End-User Subscriber Certificates

An end-user Subscriber Certificate is revoked if:

- A CTE Member, a RA, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key;
- A CTE Member, a RA, or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement;
- The Subscriber Agreement with the Subscriber has been terminated;
- A CTE Member, a RA or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to a person or entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person or entity named as the Subject of such Certificate;
- A CTE Member, a RA or a Customer has reason to believe that a material fact in the Certificate Application is false;
- A CTE Member, a RA or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived;
- The information within the Certificate, other than Non-Verified Subscriber Information, is incorrect or has changed; or

- The Subscriber requests revocation of the Certificate in accordance with Section 3.4.

CN Subscriber Agreements require end-user Subscribers to immediately notify CN of a known or suspected compromise of its private key in accordance with the procedures in Section 4.4.3.1

4.4.1.2 Circumstances for Revoking CA or RA Certificate

CN will revoke CA or RA Certificates if:

- CN discovers or has reason to believe that there has been a compromise of the CA or RA private key;
- The agreement between the RA and CN has been terminated;
- CN discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the Subject of such Certificate;
- CN determines that a material prerequisite to Certificate issuance was neither satisfied nor waived; or
- CA or RA requests revocation of the Certificate
- Organization/business is filed under bankruptcy according to the Norwegian Business Registry.

4.4.2 Who Can Request Revocation

4.4.2.1 Who Can Request Revocation of an End-User Subscriber Certificate?

The following entities may request revocation of an end-user Subscriber Certificate:

- CN or the RA or Customer that approved the Subscriber's Certificate Application may request the revocation of any end-user Subscriber or Administrator Certificates in accordance with Section 4.4.1.1.
- Individual Subscribers may request revocation of their own individual Certificates.
- In the case of device, server Certificates, only a duly authorized representative of the organization is entitled to request the revocation of Certificates issued for such device or server.

4.4.2.2 Who Can Request Revocation of a CA or RA Certificate?

The following entities may request revocation of a CA or RA Certificate:

- Only CN is entitled to request or initiate the revocation of the Certificates issued to its own CAs, RAs, or infrastructure components.
- CN may initiate the revocation of any CA, or RA in accordance with Section 4.4.1.2.

4.4.3 Procedure for Revocation Request

4.4.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation must communicate the request to the CTE Member or the RA who approved the Subscriber's Certificate Application and who will in turn initiate revocation of the Certificate promptly

4.4.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to CN. CN will then revoke the Certificate. CN may also initiate CA or RA Certificate revocation

4.4.4 Revocation Grace Period

Revocation requests must be submitted as promptly as possible within a commercially reasonable period of time.

4.4.5 Circumstances for Suspension

Only RA can request a certificate suspension

4.4.6 Who Can Request Suspension

Only RA can request a certificate suspension

Not applicable see Section 4.4.5.

4.4.7 Procedure for Suspension Request

Not applicable see Section 4.4.5.

4.4.8 Limits on Suspension Period

Not applicable see Section 4.4.5.

4.4.9 CRL Issuance Frequency

CN publishes CRLs showing the revocation of CTE Certificates and offers status checking services. CRLs for CAs that issue end-user Subscriber Certificates are published daily. CRLs for CAs that only issue CA Certificates are published quarterly and also whenever a CA Certificate is revoked. Expired Certificates are removed from the CRL starting thirty (30) days after the Certificate's expiration.

4.4.9.1 Certificate Revocation List Checking Requirements

Relying Parties must check the status of Certificates on which they wish to rely. Relying Parties may check Certificate status by consulting the most recent CRL published by the CA that issued the Certificate on which the Relying Party wishes to rely.

- For CN CAs and Test and CPN Class Certification Authorities, CRLs are posted in the CN repository at http://crl1.Commfides.com/.

- For Managed Custom Customer CAs CRLs are posted in the CN repository at http://crl1.Commfides.com Customer-specific repositories, the location of which is communicated to the Managed Custom Customer, can be provided for by CTE CAs.

4.4.9.2 On-Line Revocation/Status Checking Availability

In addition to publishing CRLs, CN provides Certificate status information through query functions available though web-based query functions accessible through Certificate Authority Manager and CN OCSP service.

4.4.9.3 On-Line Revocation Checking Requirements

If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party must check Certificate status using the applicable methods specified in Section 4.4.11.

4.4.9.4 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.9.5 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.9.6 Special Requirements Regarding Key Compromise

In addition to the procedures described in Sections 4.4.9 – 4.4.14, CN uses commercially reasonable efforts to notify potential Relying Parties if CN discovers, or has reason to believe, that there has been a Compromise of the private key of a CTE CA.

4.5 Security Audit Procedures

Security auditing of the CN PKI is currently provided for. CN and other CTE CAs may support and are encouraged to support a formal security auditing plan.

4.5.1 Types of Events Recorded

CN manually or automatically logs the following significant events:
CA key life cycle management events, including:

- Key generation, backup, storage, recovery, archival, and destruction; and
- Cryptographic device life cycle management events.

- CA and Subscriber Certificate life cycle management events, including:
- Certificate Applications, renewal, re-key, and revocation:
- Successful or unsuccessful processing of requests: and
- Generation and issuance of Certificates and CRLs.

- Security-related events including:
- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed by CN personnel;
- Security sensitive files or records read, written or deleted;
- Security profile changes;
- System crashes, hardware failures and other anomalies;
- Firewall and router activity; and

- CA facility visitor entry/exit.
- Log entries include the following elements:
- Date and time of the entry;
- Serial or sequence number of entry, for automatic journal entries;
- Identity of the entity making the journal entry; and
- Kind of entry.

4.5.2 Frequency of Processing Log

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, CN reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within CN CA and RA systems.
Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also be documented.

4.5.3 Retention Period for Audit Log

Audit logs are retained onsite at least two (2) months after processing and thereafter archived in accordance with Section 4.6.2.

4.5.4 Protection of Audit Log

Electronic and manual audit log files are protected from unauthorized viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

4.5.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

4.5.6 Audit Collection System

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by CN personnel.

4.5.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessment

CN has certified its ISO 27001 Security Management Framework by The Norske Veritas.

4.6 Records Archival

4.6.1 Types of Events Recorded

In addition to the audit logs specified in Section 4.5, CN maintains records that include documentation of:

- CN' compliance with the CPS and other obligations under its agreements with their Subscribers, and
- actions and information that are material to each Certificate Application and to the creation, issuance, use, revocation, expiration, and re-key or renewal of all Certificates it issues from the CN CAs.

CN records of Certificate life cycle events include:

- The identity of the Subscriber named in each Certificate (except for Test and CPN Basic Class Certificates, for which only a record of the Subscriber's unambiguous name is maintained);
- The identity of persons requesting Certificate revocation (except for Test and CPN Basic Class Certificates, for which only a record of the Subscriber's unambiguous name is maintained);
- Other facts represented in the Certificate;
- Time stamps; and

may be maintained electronically or in hard copy, provided that such records are accurately and completely indexed, stored, preserved, and reproduced.

4.6.2 Retention Period for Archive

Records associated with a Certificate are retained for at least the time periods set forth below following the date the Certificate expires or is revoked:

- Ten (10) years for Person Standard, Person High and Person-Standard Class Certificates;

If necessary, CN may implement longer retention periods in order to comply with applicable laws.

4.6.3 Protection of Archive

CN protects its archived records compiled under Section 4.6.1 so that only authorized Trusted Persons are permitted to access archived data. Electronically archived data is protected against unauthorized viewing, modification, deletion, or other tampering through the implementation of appropriate physical and logical access controls. The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archived data can be accessed for the time period set forth in Section 4.6.2.

4.6.4 Archive Backup Procedures

CN incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records compiled under Section 4.6.1 are maintained in an off-site disaster recovery facility in accordance with Section 4.8.

4.6.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information. Such time information is not cryptographic-based.

4.6.6 Procedures to Obtain and Verify Archive Information

See Section 4.6.3.

4.7 Key Changeover

CN CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in Section 6.3.2. CN CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services in accordance with Section 6.1.

4.8 Disaster Recovery and Key Compromise

CN uses and adheres to CN robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key Compromise or disaster. In addition, CN has implemented disaster recovery procedures described in Section 4.8.2 and Key Compromise response procedures described in Section 4.8.3. CN Compromise and disaster recovery procedures have been developed to minimize the potential impact of such an occurrence and restore CN' operations within a commercially reasonable period of time.

4.8.1 Corruption of Computing Resources, Software, and/or Data

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to CN and CN' incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, CN' key compromise or disaster recovery procedures will be enacted.

4.8.2 Disaster Recovery

CN has implemented a disaster recovery site. CN has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. CN' disaster recovery site has implemented the physical security protections and operational controls to provide for a secure and sound backup operational setup.

CN has the capability to restore or recover operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance;
- Certificate revocation; and
- Publication of revocation information.

A disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at CN' primary site. For High availability services like OCSP and CRL, the disaster site is online redundant. CN tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for audit and planning purposes. Where possible, operations are resumed at CN' primary site as soon as possible following a major disaster.

CN maintains offsite backups of important CA information for CN CAs. Such information

includes, but is not limited to: application logs, Certificate Application data, audit data (per Section 4.5), and database records for all Certificates issued.

4.8.3 Key Compromise

Upon the suspected or known Compromise of a CTE CA or CTE infrastructure, CN' Key Compromise Response procedures are enacted. CN assesses the situation, develops an action plan, and implements the action plan.
If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status in communicated to Relying Parties through the CN repository in accordance with Section 4.4.5;
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected CTE Participants; and
- The CA will generate a new key pair in accordance with Section 4.7, except where the CA is being terminated in accordance with Section 4.9.

4.9 CA Termination

In the event that it is necessary for a CTE CA to cease operation, CN makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, CN will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA;
- Handling the cost of such notice;
- The revocation of the Certificate issued to the CA by CN;
- The preservation of the CA's archives and records for the time periods required in Section 4.6;
- The continuation of Subscriber and Customer support services;
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services;
- The revocation of unexpired un-revoked Certificates of end-user Subscribers and subordinate CAs, if necessary;
- The payment of compensation (if necessary) to Subscribers whose unexpired un-revoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA;

- Disposition of the CA's private key and the hardware tokens containing such private key; and
- Provisions needed for the transition of the CA's services to a successor CA.

All CTE partners shall receive advance notification. CA shall

- inform Subscribers, Relying Parties and other CAs about its intention to end operation, with no less than 6 months notice,
- make publicly available information about its intention to end operations, with no less than 3 months notice,
- keep all relevant databases, archives, records and documents, for these to be made available on request for a commercial reasonable period of time, not less than 10 years after CA termination.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

CN' CA and RA operations are conducted within CN primary facilities in OSLO, Norway. All CN CA and RA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

CN' primary facilities have physical security tiers as described in Section 5.1.2

5.1.2 Physical Access

CN' CA systems are protected by several tiers of physical security, with access to the lower tier required before gaining access to the higher tier. All access to the servers is limited to CN managers and system support staff in compliance with Section 5.2. In addition, the physical security system includes additional tiers for key management security. Dual control is implemented for relevant security zones.

5.1.3 Electrical (Power and Air Conditioning)

CN has taken reasonable precautions to provide adequate power and air conditioning. A Generator, UPS and redundant air conditioning is installed.

5.1.4 Water Exposures

CN has taken reasonable precautions to minimize the impact of water exposure to the CN systems.

5.1.5 Fire Prevention and Protection

CN has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. CN fire prevention and protection measures have been designed to comply with local fire safety regulations. Automatic fire alarms connected to local fire station is installed.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within CN facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal.

5.1.8 Off-Site Backup

CN performs routine backups of critical system data, audit log data, and other sensitive information of the CN system and data. Offsite backup media are stored in a physically secure manner.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- The validation of information in Certificate Applications;
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrolment information;
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository; or
- The handling of Subscriber information or requests.

CN considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements of Section 5.3.

5.2.2 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing CN HR or security functions and a check of well-recognized forms of identification such as passports and driver's licenses. Identity is further confirmed through the procedures in Section 5.3.

CN ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- granted access to the required facilities; and
- issued electronic credentials to access and perform specific functions on CN CA, RA, or other IT systems.

5.3 Personnel Controls

All access to the servers and applications that comprise the CTE is limited to CN Trusted Persons.

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.2 Background Check Procedures

Background check procedures shall be described in the CPS and shall demonstrate that CN requirements set forth in Section 5.3.1 are met.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of CN or a CTE CA shall receive training in the following areas:

- CA/RA security principals and mechanisms;
- All PKI software used in the CA system;
- All PKI duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

CN provides refresher training and updates to its personnel to the extent and frequency required

to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. Periodic security awareness training is provided on an ongoing basis.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

CN or CTE Members shall take appropriate administrative and disciplinary actions against personnel who perform actions not authorized in the CPS, or other CN Standards.

5.3.7 Contracting Personnel Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to CN employees in a comparable position.

Independent contractors and consultants who have not completed the procedures specified in Section 5.3.1 are permitted access to CN secure facilities only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

CN provides and makes available to its CA and RA personnel, the relevant sections of the CPS, CN Standards and any applicable statutes.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys.

Generation of end-user Subscriber key pairs is generally performed by Commfides.

6.1.2 Private Key Delivery to Entity

End-user Subscriber key pairs are typically generated by Commfides. Delivery of the private key to a Subscriber is accomplished by the Subscriber. The activation data required to activate the encrypted file may be communicated to the end-user Subscriber using an out of band process. The distribution of such private key is logged by Commfides.

End-user Subscriber key pairs are pre-generated by Commfides on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the end-user Subscriber using an out of band process. The distribution of such devices is logged by Commfides.

6.1.3 Public Key Delivery to Certificate Issuer

This requirement is not applicable as Commfides generates CA, RA, or end-user Subscriber key pairs.

6.1.4 CA Public Key Delivery to Users

CN's root CAs may be downloaded by Subscribers and Relying Parties from Commfides web site, or can be distributed via alternative channels (e-mail messages, media, etc.).

Commfides generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance.

6.1.5 Key Sizes

Commfides Intermediate CA key pairs are 2048 bit RSA. Commfides end-user Subscribers key

pairs are 2048 bit RSA. Commfides Professional Network Root CA is 2048 bit RSA.

6.1.6 Public Key Parameter Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

Commfides generates its CA pair's keys in accordance with Section 6.2.1. RA and end-user Subscriber key pairs may be generated in hardware or software.

6.1.9 Key Usage Purposes

See Section 7.1.2.1.

6.2 Private Key Protections

Commfides has implemented a combination of physical, logical, and procedural controls to ensure the security of Commfides CA private keys. Logical and procedural controls are described in Section 6.2. Physical access controls are described in Section 5.1.2.

6.2.1 Standards for Cryptographic Modules

Commfides uses hardware cryptographic modules that meet industry standards for its Principal CAs, Root and Issuing CAs. Currently Commfides HSM is granted FIPS 140-2 security validation at level 2 and level 3.

6.2.2 Private Key (n out of m) Multi Person Control

Not stipulated.

6.2.3 Private Key Escrow

Commfides does not escrow CA, RA or end-user Subscriber private keys with any third party for purposes of access by law enforcement.

Commfides may backup/escrow Subscriber private keys for encryption certificates only based on subscriber's written agreement.

6.2.4 Private Key Backup

Commfides creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form. Cryptographic modules used for CA private key storage meet the requirements of Section 6.2.1.

Modules containing onsite backup copies of CA private keys are subject to the requirements of Sections 5.1, 6.2.1. Modules containing disaster recovery copies of CA private keys are subject to the requirements of Section 4.8.2.

For the backup of end-user Subscriber private keys, see Section 6.2.3.

6.2.5 Private Key Archival

When Commfides CA key pairs reach the end of their validity period, such CA key pairs will be archived for a period of at least 5 years. Procedural controls prevent archived CA key pairs from being returned to production use. Upon the end of the archive period, archived CA private keys will be securely destroyed in accordance with Section 6.2.9.

Commfides does not archive copies of Subscriber private keys, except for separate encryption keys, see Section 6.2.3.

6.2.6 Private Key Entry into Cryptographic Module

Commfides generates CA key pairs on the hardware cryptographic modules in which the keys will be used. Commfides additionally makes copies of such CA key pairs for routine recovery and disaster recovery purposes. In such cases where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Method of Activating Private Key

All Commfides Participants are required to protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.7.1 End-User Subscriber Private Keys

This section applies the CTE Standards for protecting activation data for end-user Subscribers' private keys to all CTE Member's Subdomains. In addition, Subscribers have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys. The use of two factor authentication mechanisms is strongly encouraged.

6.2.7.2 Person Standard Certificates

The CN Person Standard Certificate private key protection is for Subscribers to:

- Use a password or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, a password to operate the private key, a machine logon or screen saver password or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

Commfides recommends that Person-Standard Class Subscribers use enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8 Method of Deactivating Private Key

Commfides CA private keys are deactivated when removed from the token reader. RA private keys are deactivated upon system log-off. Administrators and end-user Subscribers private keys may be deactivated after each operation, upon logging off their system or upon removal of their token or card from the authentication mechanism. In all cases end-User Subscribers have an obligation to protect their private key(s) in accordance with Sections 2.1.3, 6.4.1.

6.2.9 Method of Destroying Private Key

At the conclusion of a CN' CA's operational lifetime, one or more copies of the CA private key are archived in accordance with Section 6.2.5. Remaining copies of the CA private key are securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CN CA, RA and end-user Subscriber Certificates are backed up and archived as part of CN' routine backup procedures.

6.3.2 Usage Periods for the Public and Private Keys

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that private keys may continue to be used for decryption and public keys may continue to be used for signature verification. The maximum Operational Periods for CTE Certificates for Certificates issued on or after the effective date of the CPS are set forth in Table 7 below.

In addition, CN CAs stop issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Certificate Issued By	***Norwegian Enterprise CA***	***Person Standard CA***	***Person High CA***
CN Professional Network ROOT self-signed 2048 bit SHA256RSA	N/A	N/A	N/A
Intermediate CA signed by CPN ROOT 2048 bit SHA256RSA	Valid to 31.12.2024	Valid to 31.12.2024	Valid to 31.12.2024
Intermediate CA to end-user Subscriber 2048 bit SHA256RSA	Normally up to 3 years, but up to 12 years under the conditions described below	Normally up to 3 years, but up to 12 years under the conditions described below	Normally up to 3 years, but up to 12 years under the conditions described below

Table 7 – Certificate Operational Periods based on ETSI-102-176-1v2.0.0 Table 11/clause 9.

Except as noted in this section, CN Participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to twelve years, but no longer that remaining lifetime of signing CA, if the following requirements are met:

- The Certificates are encryption Certificates;
- Subscribers' key pairs reside on a hardware token, such as a smart card;
- Subscribers are required to undergo re authentication procedures when Signing and Authentication key is rekeyed under Section 3.1.8;
- If a Subscriber is unable to complete re authentication procedures under Sections 3.1.8 successfully or is unable to prove possession of such private key when required by the Foregoing, the CA shall automatically revoke the Subscriber's Certificate.

6.4 Activation Data

CN CA Private Key generation is carried out according to CN Key Ceremony with Security Officer, Security Centre Director, Chief Executive Officer, two System Administrators and Internal Auditor present. Key was randomly generator and installed using FIPS140-2 HSM.

6.4.1 Activation Data Protection

CN CA Private Key Activation Data is protected in a physically secured environment under dual control with at least one Security Officer.

6.5 Computer Security Controls

6.6 Life Cycle Security Controls

CN conforms to the requirements put down in the Normalized Certificate Policy (NCP) requirements of ETSI 102 042

6.7 Network Security Controls

CN performs all its CA and RA functions using networks secured in accordance with the ISO/IEC 27002 controls as defined in CN SOA to prevent unauthorized access and other malicious activity. CN protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Cryptographic Module Engineering Controls

Cryptographic modules used by CN meet the requirements specified in Section 6.2.1.

7. Certificates and CRL Profile

7.1 Certificate Profile

CPS § 7.1 defines CN' Certificate Profile and Certificate content requirements for CTE Certificates issued under the CPS.

At a minimum, CN X.509 contain the basic X.509 Version 3 fields and indicated prescribed values or value constraints in the document *CN-CPS_CN Certificate Profiles* available: https://www.Commfides.com/e-ID/Certificate-Policy-CP-og-Certification-Practice-Statement-CPS.html

7.1.1 Version Number

CN CA and end-user Subscriber Certificates are X.509 class 3 Certificates.

7.1.2 Certificate Extensions

When X.509 class 3 Certificates are used, CN populates Certificates with the extensions required by sections 7.1.2.1 - 7.1.2.8. Private extensions are permissible as long as their use is consistent with the CPS.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The Key Usage extensions in X.509 class 3 Certificates are generally configured so as to set and clear bits and the criticality field in accordance with CN-CPS_CN Certificate Profiles available:

https://www.Commfides.com/e-ID/Certificate-Policy-CP-og-Certification-Practice-Statement-CPS.html

7.1.2.2 Certificate Policies Extension

Certificate criteria (non critical x.509 extension)	Certificate Policy: Policyidentifier=2.16.578.1.29.11.1.1.0 OBJECT IDENTIFIER::= {joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) CN (29) CPN Person-Standard SHA256 CA (3) certificatepolicy (1) version 1.0}		Y

7.1.2.3 Subject Alternative Name

CN X.509 Version 3 end-user Subscribers Certificates use the RFC 822 name which is populated with the Subscriber's e-mail address.

7.1.2.4 Basic Constraints

CN populates X.509 Version 3 CA Certificates with a BasicConstraints extension with the Subject Type set to CA. End-user Subscriber Certificates are also populated with a BasicConstraints extension with the Subject Type equal to End Entity. The criticality of the BasicConstraints extension is generally set to FALSE. The criticality of this extension may be set to TRUE for other Certificates in the future.

CN X.509 Version 3 CA Certificates issued to have a "pathLenConstraint" field of the BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. CA Certificates issued to the online CAs of Managed Customers and CN CAs, issuing end-user Subscriber Certificates have a "pathLenConstraint" field set to a value of "0" indicating that only an end- user Subscriber Certificate may follow in the certification path.

7.1.2.5 Extended Key Usage

		Critical	Mandatory
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Smartcard logon (1.3.6.1.4.1.311.20.2.2)		Y

7.1.2.6 CRL Distribution Points

CN X.509 Person-Standard Class Individual end-user Subscriber Certificates use the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status.

Address is: http://crl1.Commfides.com/ and http://crl2.Commfides.com/

7.1.3 Algorithm Object Identifiers

CN X.509 Certificates are signed with sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) in accordance with RFC 3280.

7.1.4 Name Forms

CN populates CTE Certificates with an Issuer and Subject

Distinguished Name in accordance with Section 3.1.1. In addition, CN includes within end-user Subscriber Certificates two additional Organizational Unit fields that indicate the Certificate type, and name of the CA that generated it. Exceptions to the foregoing requirement are permitted only when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended.

7.1.5 Name Constraints

No Stipulations

7.1.6 Certificate Policy Object Identifier

This CP covers CN Person High IDs. The OID's are:

For CN Person Standard IDs:
Policyidentifier=2.16.578.1.29.11.1.1.0
OBJECT IDENTIFIER::= **{joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) CN (29) CPN Person-Standard SHA256 CA (13) certificatepolicy (1.0) version 1.0}**
The identifiers are made available to Certificate Holders and to Relying Parties.
Certificate Policy Object Identifiers are used in accordance with Section 1.2.

7.1.7 Usage of Policy Constraints Extensions

No Stipulations

7.1.8 Policy Qualifier Syntax and Semantics

No Stipulations

7.2 CRL Profile

CN issues CRLs that conform to RFC 3280. At a minimum, CN CRLs contain the basic fields and contents specified in Table 10 below:

Field	***Value or Value constraint***
Version	See Section 7.2.1.
Signature	Algorithm used to sign the CRL. CN CRLs are signed using

Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) in accordance with RFC 3280.
Issuer	Entity that has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in Section 7.1.4.
Effective Date	Issue date of the CRL. CN CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. The Next Update date for CN CRLs is set as follows: 24 hours from the Effective Date for all CN CAs. CRL issuance frequency is in accordance with the requirements of Section 4.4.5.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 10 – CRL Profile Basic Fields

7.2.1 Version

CN currently issues X.509 Version 3.

7.2.2 CRL and CRL Entry Extensions

No stipulation

8. SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

Amendments to the CPS shall be made by the CN Practices Development Professional. CN reserves the right to amend the CPS without notification to end users. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

8.2 Publication and Notification Policies

8.2.1 Items Not Published in the CPS

Security documents considered confidential by CN are not disclosed to the public. Confidential security documents include the documents identified in Section 2.8.1 as documents that are not available to the public.

8.2.2 Distribution of the CPS

The CPS is published in electronic form within the CN Repository at

https://www.Commfides.com/e-ID/Certificate-Policy-CP-og-Certification-Practice-Statement-CPS.html

website.

The CPS is available in the CN' Repository in Adobe Acrobat pdf.

8.2.3 CPS Approval Procedures

The CN Certificate Advisory Board (CAB) is responsible for the CPS. All changes must be approved by the CAB. .

8.2.4 Waivers

No stipulation.