CERTIFICATE PRACTICE STATEMENT

COMMFIDES CLASS 3 CERTIFICATES

CPS and CP for Qualified Certificates: "PERSON HIGH"

V 1.2
OID: 2.16.578.1.29.2.1.2

COMMFIDES

Secure Communication & Online Identity Management

Table of contents:

1 INTRODUCTION

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

This document is the Commfides Certification Practice Statement ("CPS"), and includes both the Certificate Policy ("CP") and the Certificate Practice Statement for the Commfides Trust Environment ("CTE")

It states the practices that CTE Certification Authorities ("CTE CAs") employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates within the CTE. Each Registration Authority ("RA") is responsible for the vetting of user identities within their community according to their authorization for "Person High" certificates.

The CPS is the principal statement of policy governing the CTE. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital or electronic certificates ("Certificates") within the CTE and providing associated trust services. These requirements, called the "CTE Standards", protect the security and integrity of the CTE, apply to all CTE Participants, including Commfides, its Licensees, Sub-Licensees, RAs, LRAs, Resellers, Agents, Customers, Subscribers and Relying Parties, and thereby provide assurances of uniform trust throughout the CTE.

Commfides has a CPS that governs its Sub domain within the CTE. While the CP sets forth requirements that CTE participants must meet, the CPS describes how Commfides and its Licensees ("CTE Members") meet these requirements within their respective Sub domains of the CTE. More specifically, the CPS describes the practices that CTE Members employ for:

. • Securely managing the CTE infrastructure; and
. • Issuing, managing, revoking and renewing Certificates within the CTE ("CTE Certificates").

CTE Members have authority over a portion of the CTE. The portion of the CTE controlled by a CTE Member is called its "Sub domain" of the CTE. A CTE Member's Sub domain includes entities subordinate to it such as its CAs, RAs, LRAs, Agents, Resellers, Customers, Subscribers, and Relying Parties. Activities conducted by CTE Members outside the CTE are not governed by the CPS. If a "Sub domain" wishes to issue qualified certificates under a different name than Commfides (license Commfides CA), the subjected part in the "Sub domain" must achieve status as a supplier of qualified certificates given by the Norwegian Post and Telecommunications.

1.1 Overview

Commfides Norge AS is a Company that offers digital certificates – products and services for wired and wireless solutions. The CA is located physical In Oslo Norway and is enhanced to fulfil the Norwegian Law "esignaturloven" and meets the specific requirements set by the SEID standard and the Official PKI demands in Norway. Our root and operating CA is fully managed and set up for CTE by Commfides Norge AS.

The CP describes at a general level the overall business, legal, and technical infrastructure of the CTE. The CPS then applies CTE Standards from the CP to CTE Members. The CPS describes how CTE Members meet these requirements within their Sub domains. CTE Members are also subject to additional obligations and standards relevant to their operations by virtue of their CTE Member Agreement.

The practices specified in the CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards related to the operation of CAs in the EU, Norway, Canada and the USA.

The structure of the CPS generally corresponds to the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, known as RFC 2527 of the Internet Engineering Task Force, an Internet standards body. The RFC 2527 framework has become a standard in the PKI industry.

1.1.1 Certificate Policy

This section summarizes the types of Certificates offered by CTE Members within the CTE. The CTE is a PKI that accommodates a public community of users. Applications include digitally signing and authenticating identities and other attributes for e-mail, web forms, web sites, and encrypting/decrypting information.

Within the CTE, CTE Members offer four distinct types ("Classes") of certification services, for both the wired and wireless Internet and other networks. Classes provided are "International Class 3", "Person Standard", "Person High" and "Norwegian Enterprise". Each Class of Certificate provides specific functionality and security features and corresponds to a specific level of trust. Commfides Participants choose which Classes of Certificates they need. This document is a statement for the "Person High" class.

Person High Certificates - provide the highest level of assurances within the CTE. Person High Certificates are issued to individuals in Norway with an F-nr or a D-nr and Administrators for CAs and RAs. Person High individual Certificates may be used for digital signatures, encryption, and access control, including as proof of identity, in high-value transactions. Person High individual Certificates provide assurances of the identity of the Subscriber based on the personal (physical) presence of the Subscriber before an independent third party that confirms the identity of the Subscriber using, at a minimum, a well-recognized and approved form of government-issued identification and one other identification credential.

1.1.2 CTE Certification Services

1.1.2.1 Certification Services Description

Commfides operates firstly as a Trust Service Provider to deliver Trust Services to user communities, directly or through Licensees, RAs, LRAs, Agents and Resellers and also as a network of CTE Members sharing Commfides procedures and brands to issue high quality Certificates which inherit trust that is vested with Commfides top root and brand name.

CTE Certification Services offered by CTE Members support secure electronic commerce and communication and on-line business services through the provision of general-purpose Certificates that can be used for non-repudiation, authentication, encryption and access control.

CTE Members offer a full range of services to assist in deployment, management and uses of Certificates. Services offered by CTE Members to their Customers are subject to the provisions of specific sales and service agreements between CTE Members and their Customers ("Customer Agreements") Schedule I.

A CTE Secure Processing Center ("CSPC") operates a secure facility that houses among other things, CA systems, including the cryptographic modules holding the private keys used for the issuance of Certificates. CSPCs provide the "back-end" infrastructure and support for a CA. Commfides and other CTE Members may operate a CSPC or outsource in whole or in part, certain aspects of the delivery of their services to others, provided such service provider has agreed to provide services in accordance with the CPS and is under the control and direction of a CTE Member.

1.1.2.2 CTE Business Partners

To meet the diverse certification needs of users and their organizations, CTE Members work with selected business partners to deliver PKI services including certification and registration to customers in Norway, EU and throughout the world. Partners include Licensees, RAs, LRAs, Agents and Resellers that operate under agreement with Commfides. Regardless of the form or format of the relationship with CTE Participants, Commfides is ultimately responsible for the integrity and compliance with the CPS.

CTE Members, RAs, LRAs, Agents and Resellers sell direct to individuals and to corporate and other Professionals and to organizations incorporating CTE Certificates into their products. RAs, LRAs, Agents and Resellers must comply with the CPS and the additional obligations set out in their respective agreements with CTE Members.

1.1.2.3 Certificate Service Forms

CTE Members and their business partners offer Certificate Services under the terms:

(a) Retail Services -CTE Members in conjunction with their business partners, sell Certificates to individuals and organizations one by one through the Commfides Web Site or through other Commfides systems.
(b) Managed Services -CTE Members provide various forms of managed services to meet customer needs. CTE Members and Customers undertake varying portions of the application and issuance process depending on the agreement governing their operation. Managed Solutions include provisions for branded and co-branded solutions.

Within the categories titled "Retail" and "Managed" Services, CTE Members may provide varying levels of service and support, which are detailed in the specific Customer Agreements covering such service engagements.

1.1.2.4 Retail Services

CTE Members offer a full range of Certificate Services directly to the public. Retail Services are often delivered directly to Subscribers through CTE Member's Web sites or by their business partners. Retail Services are subject to Customer Agreements between CTE Members and their Customers and compliance with the CPS.

1.1.2.5 Managed Services

Managed Services offered by CTE Members are fully integrated, managed PKI services that allow organizations to provide Certificates to individuals, such as employees, sub-contractors, partners, suppliers, and customers ("Affiliated Individuals"). Customers obtaining Managed Services ("Managed Service Customers") fall into two principal categories:

(i) Managed Custom Customers ("Managed Custom Customers") provide Certificates by becoming a CA within the CTE. Managed Custom Customers perform the RA "front-end" functions of approving or denying Certificate Applications, and initiating the revocation or renewal of Certificates using Managed PKI functionality. The Managed Custom Customer uses the secure PKI backbone of the CTE by outsourcing all "back-end" functions of Certificate issuing, management, revocation, and renewal functions to CTE Members.

(ii) Managed Customers ("Managed Customers") use Managed Services, which provides security for enterprises and organizations not requiring Custom Services. Managed Customers become RAs associated with a CTE CA, which is shared among a CTE Member’s Customers of the same specific Class of Certificates. Managed Customers approve or deny Certificate Applications using Managed PKI functionality, and request the revocation or renewal of Certificates. CTE Members perform all the back-end functions of Certificate issuance, management, revocation, and renewal functions.

Managed Customers may only approve Certificate Applications of individuals who are affiliated with their organization and may not approve Certificate Applications from the general public. Managed Services are subject to Managed Service Agreements between CTE Members and their Customers and compliance with the CPS.

1.1.2.6 Electronic Certificates

Electronic ID (e-ID), electronic signature (e-Signature), digital certificates, certificates or digital IDs (“Certificates”), allow entities that participate in an electronic or digital transaction to prove their identify relative to other participants. Certificates are used as the digital equivalent of an identity card. By means of a Certificate, CTE Members provide confirmation of the relationship between a Subscriber and its public key. The CTE provides various types of Certificates to meet end user needs for non-repudiation, authentication, encryption and access control.

1.1.2 General Definitions

Capitalized terms within the CPS are defined terms with specific meanings. The following table sets out the term and definition of some of the more general terms within the CPS. Terms not defined here are set-out in Section 11.

Term	***Definition***
Authentication Authority (AA)	Portion of the responsibilities of the RA, the Authentication Agent provides outside third party validation or individuals and organizations.
Certification Authority (CA)	The entity/system that issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA).
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber’s public key, identifies the Certificate’s Operational Period, contains a Certificate serial number (UNID), and is digitally signed by the CA. It states also that it is a “Qualified Certificate” for Person High usage and states its Warranty limits.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Authority Manager (CAM)	The CAM is a front-end Web server for CTE CAs that provides a Web user interface for RAs and certain Customers. The CAM forwards certificate-signing requests to the actual CTE CA to issue X.509 certificates.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which

	terminates in a root Certificate.
CTE CA	A CA that issues Certificates within the CTE.
CTE Certificates	Certificates issued by a CTE CA.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Non-Verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (an RA performs or is delegated certain tasks on behalf of a CA).
Relying Party	A recipient of a Certificate who acts in reliance on that Certificate and/or digital signatures verified using that Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of a device Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate. Subscriber and end-user Subscriber are used interchangeably.

Table 1: General Definitions

1.2 Identification

This CP covers Commfides Person High IDs. The OID’s are:

For Commfides Person High IDs:

Smartcards

OBJECT IDENTIFIER::= **{joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) Commfides (29) person-high(2) certificatepolicy (1) 2}**

The identifiers are made available to Certificate Holders and to Relying Parties.

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

1.3 Community and Applicability

The community governed by the CPS is the CTE. The CTE is a PKI that accommodates widely distributed community of wired and wireless users with diverse needs for communication and information security. This CP spans the Norwegian community for all legal persons with a verified F-nr or D-nr in the “Folkeregisteret” (DSF). For Person High certificates a person must be of legal age of 18 years old or be accompanied with an official registered guardianship.

1.3.1 Certification Authority

The term Certification Authority or CA is a general term that refers to an entity that issues Certificates. A CA may also be generally described by the term Issuing Authority. CAs that issue Certificates within the CTE are referred to as CTE CAs. Commfides is responsible for drafting all policy related to the issuing of Certificates within the CTE and is referred to in this capacity as the Policy Authority. All policy related to the issuing of Certificates within the CTE shall meet the structure of RFC 2527.

1.3.1.1 CTE Principal Certification Authorities

The CTE root CAs act as root for all CTE Certificates.

Subordinate to the CTE CPN (Commfides Professional Network) Root CA is the CPN Class CAs which are entities within the CTE that have been designated to interoperate directly with the CTE CPN Root CA (I.E., through the exchange of cross-certificates), and which issues certificates or cross-certificates (or other means of interoperation) to other CTE CAs. There is one CTE CPN Class Subordinate CA for each Class of CPN Certificates within the CTE.

1.3.1.2 Other CTE Certification Authorities

Subordinate to the CPN Class Subordinate CAs, Other CTE CAs are entities within the CTE that have been designated to interoperate directly with the CTE CPN Class Subordinate CAs (I.E., through the exchange of cross-certificates), and which issues either end-entity certificates or certificates or cross-certificates (or other means of interoperation) to other CTE Members, their Customers, or both.

CPN CAs may be referred to as CAs that is "subordinate" to the CTE Principal CAs. The use of this term shall encompass any CA under the control of a CTE Member that has a Certificate issued to it by a CTE Principal CA or any CA subordinate to a CTE Principal CA, whether or not the CTE Member employs a hierarchical or other PKI architecture.

1.3.2 Registration Authority

Registration Authorities ("RAs") assist a CA by performing front-end functions of confirming identity, approving or denying Certificate Applications, requesting revocation of Certificates, and approving or denying renewal requests. Local Registration Authorities ("LRAs"), carry out registration tasks on behalf of a RA. A RA supervises a LRA. LRAs may have a geographical, industry or business connotation and they operate within the framework of the CTE and in accordance with the CPS. RAs may support several LRAs. There is no limitation on the number of RAs or LRAs that may be associated with Commfides.

The requirements for RAs and LRAs within the CTE are set out below:

- Accept, evaluate, approve or reject Certificate Applications;
- Register Subscribers for CTE Certification Services;
- Attend all stages of the identification of Subscribers as assigned by Commfides according to the type of Certificate they issue;
- Use official, notarized or otherwise indicated document to evaluate a Subscriber Application;
- Follow approval of a Certificate Application with notification to the applicable CTE Member; and
- Initiate and approve the process to request the renewal and revocation of a Certificate.

Within the CTE RAs can be classified under three categories:

. • CTE Members,
. • Managed Custom Customers, and
. • Managed Customers.

CTE Members provide a full range of certification services including RA services. CTE Members provide RA functions when they sell retail services to Customers.

Managed Customers and Managed Custom Customers become RAs assisting a CTE CA to issue client Certificates to end-user subscribers. CTE Members perform all the "back-end" functions including issuing, managing, revoking and renewing Certificates on their behalf.

CTE Members reach their Subscribers both directly and through a network of RAs and LRAs. RAs and LRAs interact with both the Subscriber and a CTE Member to deliver public PKI services to the end-user.

Other RA's are provided for within the CTE with written notice from Commfides. Other RAs must meet the obligations placed on Managed Customers, subject to modifications necessary for differences between technologies used.

1.3.2.1 Authentication Authorities

Authentication Authorities ("AAs") are independent third party authentication agencies who assist RAs by performing identification of Subscribers. AAs must meet the applicable obligations placed on Managed Customer RAs and the CPS and are subject to the terms of Authentication Authority Agreements approved by Commfides.

1.3.2.2 Administrators

Administrators are Trusted Persons who perform Certificate Services management functions on behalf of CAs and RAs. Each RA has one or more Administrators who perform the management functions on behalf of that RA.

1.3.3 End Entities

1.3.3.1 Subscribers.

A Subscriber is the entity or person whose name appears as the subject in a Certificate, who asserts that it uses it's key and Certificate in accordance with the CP, and who does not itself issue certificates. CAs is sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.3.2 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the Certificate by checking the appropriate certificate status information. The Relying Party can use the Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the Certificate (such as OU fields, or Issuer DN) to determine the suitability of the Certificate for a particular use.

1.3.4 Applicability

The CPS applies to all Commfides Participants, including Commfides and its Licensees, RAs, LRAs, Resellers, Agents, Customers, Subscribers, and Relying Parties. The CPS applies to CTE Members and Commfides core infrastructure supporting the CTE. The CPS describes the practices governing the use of Certificates within the CTE. Each Class of Certificate is generally appropriate for use with the applications set forth in Section 1.1.1. Nonetheless, by contract or within specific environments, CTE Participants are permitted to use Certificates for higher security applications than the ones described in Sections 1.1.1, 1.3.4.1. Any such usage, however, shall be limited to such entities and subject to Sections 2.2.1.2, 2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.3.4.1 Factors in Determining Usage

The Relying Party must first determine the level of assurance required for an application, and then select the Class of Certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by Commfides or other CTE Members. Relying Parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates)

For guidance, suitable applications are set out at Section 1.1.1. These listings are not intended to be exhaustive.

Individual Certificates and some organizational Certificates permit Relying Parties to verify digital signatures. CTE Participants acknowledge and agree, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to a CTE Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Subject to applicable law, a digital signature or transaction entered into with reference to a CTE Certificate shall be effective regardless of the geographic location where the CTE Certificate is issued or the digital signature created or used, and regardless of the geographic location of the place of business of the CA or Subscriber.

1.3.4.2 Restricted Applications

In general, CTE Certificates are general-purpose Certificates. CTE Certificates may be used globally and to interoperate with diverse Relying Parties worldwide. Usage of CTE Certificates is not generally restricted to a specific business environment. Nonetheless, such use is permitted and Customers using Certificates within their own environment may place further restrictions on Certificate use within these environments. Commfides and other Participants, however, are not responsible for monitoring or enforcing any such restrictions in these environments.

Also, with respect to X.509 Version 3 CTE Certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the public key in a Certificate may be used within the CTE. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

More generally, CTE Certificates shall be used only to the extent use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

1.3.4.3 Prohibited Applications

CTE Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance, where failure could lead directly to death, personal injury, or severe environmental damage. Also, subject to Section 1.3.4, Test Class and CPN Basic Class Certificates shall not be used as proof of identity or as support of non-repudiation of identity or authority.

1.4 Contact Details

1.4.1 Specification Administration Organization

Commfides Norge AS is responsible for all aspects of the Commfides Trust Environment CP and the CPS. Inquiries to Commfides Norge AS should be addressed as follows:

Commfides Norge AS, Fornebuveien 1, PO-box 405 N-1327 Lysaker Norway Attn: Commfides Practices Development – CPS +47 64 00 77 51 (voice) practices@commfides.com

Commfides Norge AS is responsible for all applicable aspects of the Commfides Trust Environment CP and the CPS as it's promoted and practiced in Norway or for Norwegian users contracted or in agreement with Confides Norge AS or one of it's reseller or sub-licensees. Inquiries to Commfides Norge AS should be addressed as follows:

Commfides Norge AS, Fornebuveien 1, PO-box 405, 1327 Lysaker, Norway: Attn: Commfides Practices Development – CPS + 47 64 00 77 51 practices@commfides.com

1.4.2 Contact Person

Questions regarding the CPS may be directed to: practices@commfides.com or to the following address:

Commfides Norge AS, Fornebuveien 1, PO-box 405, 1327 Lysaker, Norway: Attn: Commfides Practices Development – CPS + 64 00 77 51 practices@commfides.com

1.4.3 Person Determining CPS Suitability for the Policy

The organization identified in Section 1.4.1 is responsible for determining whether the CPS and other documents in the nature of certification practice statements that supplement or are subordinate to the CPS are suitable under the CP and the CPS.

2 GENERAL CONSIDERATIONS/PROVISIONS

2.1 Obligations

The obligations described below pertain to CAs within the CTE. The obligations of CA's operating within the CTE pertain to their activities as issuers of Certificates within the CTE.

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.

CTE CAs must also comply fully with the requirements set out in the Commfides License or CTE Member Agreement.

Commfides uses commercially reasonable efforts to ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within the CTE. As a condition of enrolment, a Subscriber must assent to a Subscriber Agreement. As a condition of receiving Certificate status information, Relying Parties must assent to a Relying Party Agreement. Similarly, RAs, LRAs, Resellers and Agents (where required by contract) must use Subscriber Agreements and Relying Party Agreements in accordance with the requirements imposed by the CPS. The Subscriber Agreements and Relying Party 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 or Relying Party Agreement that has been approved by Commfides, the Subscriber Agreement and Relying Party Agreement of Commfides shall apply.

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 then that specified at Section 6.3.2.

RAs must appoint one or more Trusted Persons as Administrators ("RAAs") who will be responsible for carrying out the RA functions using Commfides 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, by way of Subscriber Agreements approved by Commfides. 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 apply the specific obligations appearing in the CPS to Subscribers in the CTE. Subscriber Agreements require Subscribers to use their Certificates in accordance with Section 1.3.4 and to protect their private keys in accordance with Sections 6.1-6.2. 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 4.4.1.1 and request revocation of the Certificate in accordance with Sections 3.4, 4.4.3.1, 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 6.3.2. 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 Commfides, and shall not otherwise intentionally compromise the security of the CTE.

2.1.4 Relying Party Obligations

Relying Party obligations in the CPS apply to Relying Parties within the CTE, by way of Relying Party Agreements approved by Commfides.

Relying Party Agreements within the CTE state that before any act of reliance, 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 Party Agreements specifically state that 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 Party Agreements further state that 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 Party Agreements also require Relying Parties 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, according to Relying Party Agreements, 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.

Relying Party Agreements state that 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 Commfides, and shall not otherwise intentionally compromise the security of the CTE.

2.1.5 Repository Obligations

Commfides is responsible for the repository functions for its own CAs and other CTE CAs. CTE Members issuing Certificates to end-user Subscribers publish Certificates they issue in the Commfides part of the Commfides repository in accordance with Section 2.6.

Upon revocation of an end-user Subscriber’s Certificate, Commfides publishes notice of such revocation in the repository. CTE Members issue CRLs for their own CAs pursuant to Sections 2.6, 4.4.9, and 4.4.11.

2.2 Liability

Commfides accepts 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.”

Commfides limited liability: (Person High)

NOK 50000, - pr. transaction

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

2.2.1 Certification Authority Liability

The warranties, disclaimers of warranty, and limitations of liability of CTE Members and their respective Customers within the CTE are set forth and governed by the agreements among them. This Section 2.2.1 relates only to the warranties that the CTE CA must make to end-user Subscribers receiving Certificates from it and to Relying Parties, the disclaimers of warranties they shall make to such Subscribers and Relying Parties, and the limitations of liability they shall place on such Subscribers and Relying Parties.

CTE Members use, and (where required) other Business Partners shall use, Subscriber Agreements and Relying Party Agreements in accordance with Section 2.1.1. These Subscriber Agreements shall meet the requirements imposed by Commfides. Requirements that Subscriber Agreements contain warranties, disclaimers, and limitations of liability below apply to all Business Partners that use Subscriber Agreements. CTE Members adhere to such requirements in their

Subscriber Agreements. Commfides' practices concerning warranties, disclaimers, and limitations in Relying Party Agreements apply to CTE Members. Terms applicable to Relying Parties shall also be included in Subscriber Agreements, in addition to Relying Party Agreements.

2.2.1.1 Certification Authority Warranties to Subscribers and Relying Parties

Commfides' Subscriber Agreements include, and other Subscriber Agreements shall include, a warranty to Subscribers that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate;
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate;
- Their Certificates meet all material requirements of the CPS; and
- Revocation services and use of a repository conform to the CPS in all material aspects.

Commfides' Relying Party Agreements contain, and other Relying Party Agreements shall contain a warranty to Relying Parties who reasonably rely on a Certificate that:

- All information in or incorporated by reference in such Certificate, except Non-Verified Subscriber Information, is accurate;
- In the case of Certificates appearing in the Commfides repository, that the Certificate has been issued to the individual or organization named in the Certificate as the Subscriber, and that the Subscriber has accepted the Certificate in accordance with Section 4.3; and
- The entities approving the Certificate Application and issuing the Certificate have substantially complied with the CPS when issuing the Certificate.

2.2.1.2 Certification Authority Disclaimers of Warranties

To the extent permitted by applicable law, Commfides' Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements and Relying Party Agreements shall disclaim, CTE Members' possible warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of the CPS.

2.2.1.3 Certification Authority Limitations of Liability

To the extent permitted by applicable law, Commfides' Subscriber Agreements and Relying Party Agreements limit, and other Subscriber Agreements and Relying Party Agreements shall limit CTE Members' liability outside the context of the CPS. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the following liability cap limiting CTE Members' damages concerning a specific Certificate to the extent permitted by applicable law to two times the amount paid for the Certificate. The liability limitations provided in Section 2.2.1.3 shall be the same regardless of the number of digital signatures, transactions, or claims related to such Certificate and CTE Members shall not be obligated to pay more than the total liability limitation for each Certificate.

Class	***Liability Caps***
International Class 1	See section 5 of Certificate Subscription And Use Agreement for International Class 1
International Class 3	See section 5 of Certificate Subscription And Use Agreement for International Class 3
International Enterprise	See section 5 of Certificate Subscription And Use Agreement for International Enterprise Class
Norwegian Enterprise	See section 5 of Certificate Subscription And Use Agreement for Norwegian Enterprise
Person Standard Class	See section 5 of Certificate Subscription And Use Agreement for Person Standard
Person High Class	See section 5 of Certificate Subscription And Use Agreement

Table 2: Liability Caps for Internationa class 1 and 3, International Enterprise, Norwegian Enterprise, Person Standard and Person High Certificate Classes

2.2.1.4 Force Majeure

To the extent permitted by applicable law, Commfides' Subscriber Agreements and Relying Party Agreements include, and other Subscriber Agreements and Relying Party Agreements shall include, a force majeure clause protecting CTE Members.

2.2.2 Registration Authority Liability

The warranties, disclaimers of warranty, and limitations of liability between an RA and the CA it is assisting to issue Certificates, are set forth and governed by the agreements between them. CTE Members, in their role as RA, uses Subscriber Agreements and Relying Party Agreements in accordance with Sections 2.1.1-2.1.2, which has their own warranties, disclaimers, and limitations.

2.2.3 Subscriber Liability

2.2.3.1 Subscriber Warranties

Commfides Subscriber Agreements require Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
- No unauthorized person has ever had access to the Subscriber's private key;
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;
- All information supplied by the Subscriber and contained in the Certificate is true;
- The Certificate is being used exclusively for authorized and legal purposes, consistent with the CPS; and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Other Subscriber Agreements shall also contain these requirements.

2.2.3.2 Private Key Compromise

The CPS sets forth Commfides' standards for the protection of the private keys of Subscribers, which are included by virtue of Section 6.2.7 in Subscriber Agreements. Subscriber Agreements state that Subscribers failing to meet these standards are solely responsible for any loss or damage resulting from such failure.

2.2.4 Relying Party Liability

Subscriber Agreements and Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in Section 2.1.4.

2.3 Financial Responsibility

This CPS contains no limits on the use of any Certificates, issued by Commfides 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, Commfides' Subscriber Agreement requires, and other Subscriber Agreements shall require, Subscribers to indemnify Commfides, its Licensees and any non-Commfides 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, Commfides' Relying Party Agreements and other Relying Party Agreements require Relying Parties to indemnify Commfides and its Licensees and any non-Commfides 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, Commfides' 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 Dispute Resolution Procedures

2.4.3.1 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.

2.4.3.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Commfides' 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

2.5.1 Certificate Issuance or Renewal Fees

CTE Members and Business Partners are entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

2.5.2 Certificate Access Fees

CTE Members, Business Partners and Customers do not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

2.5.3 Revocation or Status Information Access Fees

CTE Members do not charge a fee as a condition of making the CRLs required by Section 4.4.9 available in a repository or otherwise available to Relying Parties. CTE Members do, however, charge a fee for providing customized or other value-added revocation and status information services. Commfides does not permit access to revocation information, Certificate status information, or time stamping in its repository by third parties that provide products or services that utilize such Certificate status information without Commfides' prior express written consent.

2.5.4 Refund Policy

CTE Members adhere to, and stand behind, rigorous practices and policies in undertaking certification operations and in issuing Certificates. If for any reason a Subscriber is not completely satisfied with the Certificate issued to him, her, or it, the Subscriber may request that the CTE Member revoke the Certificate within thirty (30) days of issuance and provide the Subscriber with a refund. After the initial thirty (30) day period, a Subscriber may request that the CTE Member revoke the certificate and provide a refund if the CTE Member has breached a warranty or other material obligation under the CPS relating to the Subscriber or the Subscriber's Certificate. After the CTE Member revokes the Subscriber's Certificate, the CTE Member will promptly credit the Subscriber's account or credit card (if the Certificate was paid by the Subscriber's credit card) or otherwise reimburse the Subscriber, for the full amount of the applicable fees paid for the Certificate. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to Subscribers.

2.6 Publication and Repository

2.6.1 Publication of CA Information

Commfides is responsible for the repository function for its CAs and those of other CTE CAs.

Commfides publishes certain CA information in the repository section of Commfides' web site at http://www.commfides.com as described below. Commfides publishes the CPS, Subscriber Agreements, and Relying Party Agreements in the repository section of Commfides' web site.

Commfides publishes Certificates in accordance with Table 3.

Certificate Type	***Publication Requirements***
Commfides Issuing Root CA Certificates	Available to Relying Parties through add-on to a browser software and as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
End-User Subscriber	Not generally made available.

Certificates Available to Administrators for Managed Service Customers and RAs through Commfides Certificate Authority Manager.

Table 3 – Certificate Publication Requirements

Commfides publishes Certificate status information in accordance with Section 4.4.11.

2.6.2 Frequency of Publication

Updates to the CPS are published in accordance with Section 8. Updates to Subscriber Agreements and Relying Party 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 Commfides web site is publicly-accessible information. Read only access to such information is unrestricted. Commfides requires persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. Commfides has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

2.6.4 Repositories

See Section 2.1.5.

2.7 Compliance audit

The Commfides PKI is not currently audited by an outside party. CA operations may be reviewed by any cross certifying organization or potential relying organization if approved by Commfides. As a regulatory authority of qualified certificates in Norway, the Norwegian Post and Telecommunications may appoint an outside audit party.

2.8 Confidentiality and Privacy

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 Commfides, an other CTE Member or their respective auditors (whether internal or public);
- Contingency planning and disaster recovery plans; and
- Security measures controlling the operations of Commfides 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, Commfides' 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.

2.8.7 Other Information Release Circumstances

No stipulation.

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 Commfides 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

Commfides CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields. Commfides Issuer Distinguished Names consist of the components specified in Table 4 below.

Attribute	***Value***
Country (C)	The CAs country or origin..
Organization (O)	Indicates the controlling Organization of the CA
Organizational Unit (OU)	Commfides 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.

Table 4 – Distinguished Name Attributes in CA Certificate

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)	Commfides 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 Commfides" or other entity in Certificates whose applications were authenticated by Commfides or other entity. "Persona Not Validated" for CPN Basic Individual 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).

Table 5 – Distinguished Name Attributes in End User Subscriber 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.

3.1.2 Need for Names to be Meaningful

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.

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".

For use of email address, the address must be meaningful

3.1.3 Rules for Interpreting Various Name Forms

No stipulation.

3.1.4 Uniqueness of Names

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

3.1.5 Name Claim Dispute Resolution Procedure

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. CTE Members, however, do not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. CTE Members are entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.1.6 Recognition, Authentication, and Role of Trademarks

See Section 3.1.5.

3.1.7 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 Commfides-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.

3.1.8 Authentication of Organization Identity

CTE Members confirm the identity of Person High Class end-user Subscribers and other enrollment information provided by Certificate Applicants (except for Non-Verified Subscriber Information) in accordance with the procedures set forth in the subsections that follow. In addition to the procedures below, the Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with Section 3.1.7.

3.1.9 Authentication of Individual Identity

For all Classes of individual Certificates, CTE Members confirm that:

- The Certificate Applicant is the person identified in the Certificate 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 for each Class of Certificate.

3.1.9.1 Person High Class Individual Certificates

Person High Class Certificates are authenticated based on the personal presence of the Certificate Applicant before an independent third party Authentication Authority. The Authentication Authority checks the identity of the Certificate Application by reference to recognized forms of valid legal government issued documentation such as passport, driver's license issued after spring of 1989, ID card of the armed forces, travel license for refugees, all issued by Norwegian Authorities.

Proxy or power of attorney is not accepted. Subscriber must sign a form where date, authentication type (type of identity card) and "fødselsnummer" is stated. The Subscribers identity card with photo that matches subscribers face must be photocopied for storage together with information stated above.

Subscriber must not receive certificate 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.

3.2 Routine Re-key and Renewal

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. Commfides generally provides for the Subscriber to renew the expiring key pair (technically defined as "renewal"). Renewal of all end-user Certificates with the exception of non-repudiation Certificates, will be renewed whenever possible.

Generally speaking, "Re-key" is commonly described as "Certificate Renewal," focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Classes of Commfides Certificates, this distinction is not important as a new key pair is not generated as part of Commfides' end-user Subscriber Certificate replacement process.

3.2.1 Routine Re-key and Renewal for End-User Subscriber Certificates

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

3.3 Re-key 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 Table 6 below.

Timing	***Requirement***
Prior to Certificate expiration	For replacement of a Certificate following revocation of the Certificate, Commfides 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.

Table 6 – Requirements for Certificate Replacement After Revocation

3.4 Revocation Request

Prior to the revocation of a Certificate, CTE Members verify that the revocation has been requested by the Certificate's Subscriber or the entity that approved the Certificate Application. Acceptable procedures for authenticating Subscriber revocation requests include:

- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber.

Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

Administrators are entitled to request the revocation of end-user Subscriber Certificates within the CTE. CTE Members authenticate the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Certificate Applications for End-User Subscriber Certificates

For CTE Certificates, all end-user 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.

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.

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.

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

4.2 Certificate Issuance

4.2.1 Issuance of End-User Subscriber Certificates

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 Commfides 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 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.

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

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 (other than a CPN Basic Class Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a CPN Basic Class Certificate) was issued without the authorization of the person 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.

Commfides Subscriber Agreements require end-user Subscribers to immediately notify Commfides 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 Certificates

Commfides will revoke CA or RA Certificates if:

- Commfides 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 Commfides has been terminated;
- Commfides 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;
- Commfides determines that a material prerequisite to Certificate issuance was neither satisfied nor waived; or
- CA or RA requests revocation of the Certificate.

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:

- Commfides 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 Commfides is entitled to request or initiate the revocation of the Certificates issued to its own CAs, RAs, or infrastructure components.
- Commfides 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 Commfides. Commfides will then revoke the Certificate. Commfides may also initiate CA or RA Certificate revocation.

4.4.4 Revocation Request Grace Period

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

4.4.5 Circumstances for Suspension

Commfides does not support suspension of Certificates.

4.4.6 Who Can Request 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

Commfides 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.

4.4.10 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 Commfides CAs and Test and CPN Class Certification Authorities, CRLs are posted in the Commfides repository at http://www.commfides.com/crl.
- For Managed Custom Customer CAs CRLs are posted in the Commfides repository at http://www.commfides.com/crl. Customer-specific repositories, the location of which is communicated to the Managed Custom Customer, can be provided for by CTE CAs.

4.4.11 On-Line Revocation/Status Checking Availability

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

4.4.12 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.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Regarding Key Compromise

In addition to the procedures described in Sections 4.4.9 – 4.4.14, Commfides uses commercially reasonable efforts to notify potential Relying Parties if Commfides 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 Commfides PKI is currently provided for. Commfides and other CTE CAs may support and are encouraged to support a formal security auditing plan.

4.5.1 Types of Events Recorded

Commfides 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 Commfides 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, Commfides reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within Commfides 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 Commfides 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

Commfides is pursuing ISO 27001 Security Management Framework. The review is done in ISO 17799:2005 style, which allows Commfides to do its own security audit as long as is it compatible with the standard.

Commfides follows NIST standards (NIST 800-26 for self assessment and NIST 800-30 for external assessment).

4.6 Records Archival

4.6.1 Types of Events Recorded

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

- Commfides' 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 Commfides CAs.

Commfides 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:

- Five (5) years for Test and CPN Basic Class Certificates;
- Ten (10) years for Person Standard and Person High Class Certificates; and

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

4.6.3 Protection of Archive

Commfides 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

Commfides 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

Commfides CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in Section 6.3.2. Commfides 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

Commfides uses and adheres to Commfides robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key Compromise or disaster. In addition, Commfides has implemented disaster recovery procedures described in Section 4.8.2 and Key Compromise response procedures described in Section 4.8.3. Commfides Compromise and disaster recovery procedures have been developed to minimize the potential impact of such an occurrence and restore Commfides' 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 Commfides and Commfides' incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Commfides' key compromise or disaster recovery procedures will be enacted.

4.8.2 Disaster Recovery

Commfides has implemented a disaster recovery site. Commfides 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. Commfides' disaster recovery site has implemented the physical security protections and operational controls to provide for a secure and sound backup operational setup.

Commfides 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.

Commfides' disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at Commfides' primary site. Commfides 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 Commfides' primary site as soon as possible following a major disaster.

Commfides maintains offsite backups of important CA information for Commfides 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, Commfides' Key Compromise Response procedures are enacted. Commfides 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 Commfides 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, Commfides 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, Commfides 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 Commfides;
- 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

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

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

5.1.2 Physical Access

Commfides' 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 Commfides managers and system support staff in compliance with Section 5.2. In addition, the physical security system includes additional tiers for key management security.

5.1.3 Electrical (Power and Air Conditioning)

Commfides has taken reasonable precautions to provide adequate power and air conditioning.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

Commfides has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Commfides fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within Commfides 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

Commfides performs routine backups of critical system data, audit log data, and other sensitive information of the Commfides 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.

Commfides 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 Commfides 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.

Commfides 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 Commfides CA, RA, or other IT systems.

5.3 Personnel Controls

All access to the servers and applications that comprise the CTE is limited to Commfides 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 Commfides 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 Commfides 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

Commfides 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

Commfides or CTE Members shall take appropriate administrative and disciplinary actions against personnel who perform actions not authorized in the CPS, or other Commfides 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 Commfides 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 Commfides secure facilities only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

Commfides provides and makes available to its CA and RA personnel, the relevant sections of the CPS, Commfides 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

Commfides'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 minimum 1024 bit RSA. Commfides Professional Network Root CA is 4096 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.

6.2.7.1.1 Person High Certificates

The Commfides Standard for Person High 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 High Certificate 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 Commfides' 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

Commfides CA, RA and end-user Subscriber Certificates are backed up and archived as part of

Commfides' 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, Commfides 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	***Int. Class 1***	***Int. Class 3***	***International Enterprise***	***Norwegian Enterprise***	***Person Standard***	***Person High***
Commfides Professional Network ROOT self-signed 4096 bit RSA	Valid to 31.12.2019	Valid to 31.12.2019	Valid to 31.12.2019	Valid to 31.12.2019	Valid to 31.12.2019	Valid to 31.12.2019
Intermediate CA signed by CPN ROOT 4096 bit RSA	Valid to 31.12.2019	Valid to 31.12.2019	Valid to 31.12.2019	Valid to 31.12.2019	Valid to 31.12.2019	Valid to 31.12.2019
Intermediate CA to end-user Subscriber 2048 bit RSA	Up to 5 Years	Up to 5 Years	Up to 5 Years	Normally up to 3 years, but up to 5 years under the conditions described below	Normally up to 3 years, but up to 5 years under the conditions described below	Normally up to 3 years, but up to 5 years under the conditions described below

Table 7 – Certificate Operational Periods based on ETSI-102-176-1v1.2.1 Liberal view

Except as noted in this section, Commfides 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 five years, if the following requirements are met:

- The Certificates are individual Certificates;
- Subscribers' key pairs reside on a hardware token, such as a smart card;
- Subscribers are annually required to undergo re authentication procedures under Section 3.1.8;
- Subscribers shall annually prove possession of the private key corresponding to the public key within the Certificate; and
- 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

6.4.1 Activation Data Generation and Installation

The activation data used to unlock Commfides Primary CA or other CA or end -user Subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Commfides recommends the use of smart cards, biometric access devices, and other hardware tokens for high level assurance. If activation data is to be transmitted, it shall be via an appropriately protected channel, and distinct in time form the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be protected biometrically or by other hardware token and not memorized or written down.

6.4.3 Other Aspects of Activation Data

No Stipulation.

6.5 Computer Security Controls

Commfides performs all CA and RA functions using Trustworthy Systems that meet the requirements of Commfides' Security and Audit Requirements Guide.

6.5.1 Specific Computer Security Technical Requirements

Commfides ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, Commfides limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

Commfides production network is logically separated from other components. This separation prevents network access except through defined application processes. Commfides use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

Commfides requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. Commfides requires that passwords be changed on a periodic basis.

Direct access to Commfides databases supporting the Commfides repository is limited to Trusted Persons in Commfides operations Professional having a valid business reason for such access.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by Commfides in accordance with Commfides systems development and change management standards.

6.6.2 Security Management Controls

Commfides follows NIST standards (NIST 800-26 for self assessment and NIST 800-30 for external assessment).

6.6.3 Life Cycle Security Ratings

No Stipulation.

6.7 Network Security Controls

Commfides performs all its CA and RA functions using networks secured in accordance with the best industry practices to prevent unauthorized access and other malicious activity. Commfides protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Cryptographic Module Engineering Controls

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

7 CERTIFICATE AND CRL PROFILE

The profile is based on ETSI TS 102 280 as again is based on ETSI TS 101 862 for qualified certificates especially and on Internet standards RFC 3280 and RFC 3739 for generic profile of X.509v3 certificates generally. In the matter the profile differs from one or several of the above mentioned standards, this is explicit describe.

7.1 Certificate Profile

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

At a minimum, Commfides X.509 contain the basic X.509 Version 3 fields and indicated prescribed values or value constraints in Table 8 below:

Field	***Value or Value constraint***
Version	See Section 7.1.1.
Serial Number	Unique value per Issuer DN
Signature Algorithm	Name of the algorithm used to sign the certificate (See Section 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Encoded in accordance with RFC 2459.
Valid To	Universal Coordinate Time base. Encoded in accordance with RFC 2459. The validity period will be set in accordance with the constraints specified in Section 6.3.2.
Subject DN	See Section 7.1.4
Subject Public Key	Encoded in accordance with RFC 2459 using algorithms specified in Section 7.1.3 and key lengths specified in Section 6.1.5.
Signature	Generated and encoded in accordance with RFC 2459

Table 8 – Certificate Profile Basic Fields

Basic fields for Person High certificates

Issuer:

`countryName(c);`	NO
`organizationName(o);`	COMMFIDES NORGE AS - 988 312 495

Subject:

`countryName(c);`	NO
`serialNumber;`	9578-4502-UNID**
`commonName(cn);`	syntax="Name Middlename Surname" ***
organisationName(o);	Companyname of (cn) if employee

** UNID algorithm 0-9 A-Z

7.1.1 Version Number(s)

Commfides CA and end-user Subscriber Certificates are X.509 Version 3 Certificates.

7.1.2 Certificate Extensions

Where X.509 Version 3 Certificates are used, Commfides 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.

Smartcard sertificates for Person High certificate are based on tree certificates, one for encryption, one for signing and one for authentication.

Key Usage:	**Set as critical**
Signature Certificate (first Cert):	nonRepudiation
Authentication (second Cert)	digitalSignature
Encryption Certificate (Third cert):	Key Encipherment, Data Encipherment, Key Agreement

Extended Key Usage:

Signing and Encryption:	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Authentication	Client Authentication (1.3.6.1.5.5.7.3.2)

Subject alternative name:	as normal with email address
CRL Distribution point:	http://crl.commfides.com/CommfidesPerson-High.crl
Authority information access:	http://ocsp.commfides.com/ocsp
Subject information access :	not necessary
Qualifed Certificate Statement:	QUALIFIED CERTIFICATE
qCStatements extension	Includes a OID as described in ETSI TS 101 862 point 5.2.1 Includes an OID for Transaction limit on 50000 NOK is specified as ETSI TS 101 862 point 5.2.2

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 KeyUsage extensions in X.509 Version 3 Certificates are generally configured so as to set and clear bits and the criticality field in accordance with Table 9 below. The criticality field of the KeyUsage extension is generally set to FALSE.

		CAs	***International Class 3***	***Norwegian Enterprise Class***	***Person Standard Class***	***Person High Class***
Criticality		FALSE	Set	Set	Set	Set
0	digitalSignature	Clear	Set	Set	Set	Set
1	nonRepudiation	Clear	Set	Set	Set	Set
2	keyEncipherment	Clear	Set	Set	Set	Set
3	dataEncipherment	Clear	Set	Set	Set	Set
4	keyAgreement	Clear	Set	Set	Set	Set
5	keyCertSign	Set	Clear	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Clear	Clear
8	decipherOnly	Clear	Clear	Clear	Clear	Clear

Table 9 – Key Usage settings

Key usage for Person High certificates:

Field Set as critical
nonRepudiation, digitalSignature
Key Encipherment, Data Encipherment, Key Agreement

7.1.2.2 Certificate Policies Extension

No stipulation.

7.1.2.3 Subject Alternative Name

Commfides 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

Commfides 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.

Commfides 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 Commfides 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

Client Authentication (1.3.6.1.5.5.7.3.2)

Secure Email (1.3.6.1.5.5.7.3.4)

7.1.2.6 CRL Distribution Points

Commfides X.509 Person High 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.

Adress is: crl.commfides.com

7.1.2.7 Authority Key Identifier

Commfides populates the Authority Key Identifier extension of X.509 Version 3 end-user Subscriber Certificates. The use of Authority Key Identifier is composed of the 160-bit- SHA-1 hash of the public key of the CA issuing the Certificate. The criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Where Commfides populates X.509 Version 3 CTE Certificates with a subjectKeyIdentifier extension, the keyIdentifier based on the public key of the Subject of the Certificate is generated. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.3 Algorithm Object Identifiers

Commfides X.509 Certificates are signed with sha1RSA (OID: 1.2.840.113549.1.1.5) in accordance with RFC 3280.

7.1.4 Name Forms

Commfides populates CTE Certificates with an Issuer and Subject Distinguished Name in accordance with Section 3.1.1. In addition, Commfides 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 stipulation.

7.1.6 Certificate Policy Object Identifier

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

For Commfides Person High IDs:

Smartcards

OBJECT IDENTIFIER::= **{joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) Commfides (29) person-high(2) certificatepolicy (1) 2}**

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 Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

Commfides issues CRLs that conform to RFC 3280. At a minimum, Commfides 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	Algorithm used to sign the CRL. Commfides CRLs are signed using sha1RSA (OID: 1.2.840.113549.1.1.5) 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. Commfides CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. The Next Update date for Commfides CRLs is set as follows: 24 hours from the Effective Date for all Commfides 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 Number(s)

Commfides currently issues X.509 Version 3.

7.2.2 CARL and CRL Entry Extensions

No stipulation.

8 SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

Amendments to the CPS shall be made by the Commfides Practices Development Professional. Commfides 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 Commfides 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 Commfides Repository at https://www.commfides.com/cps/CPN-Person-High.pdf website. The CPS is available in the Commfides' Repository in Adobe Acrobat pdf, and HTML.

8.3 CPS Approval Procedures

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

8.4 Waivers

No stipulation.

9 BIBLIOGRAPHY

- 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-102-176-1v1.2.1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures;

- ISO/IEC 15408(1999): "Information technology Security techniques – Evaluation criteria for IT security (parts 1 to 3)".

- 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" R. Housley RSA Laboratories, W. olk NIST, W. Ford VeriSign, D. Solo Citigroup

- NOU 2001:10, "Uten Penn og blekk".

10 ACRONYMS AND ABBREVIATIONS

AA	Authentication Authority
CA	Certification Authority
CARL	Certificate Authority Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CTEDN	Commfides 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)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
U.S.C.	United States Code
WWW	World Wide Web

11 Glossary

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 subscribers 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 are 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
Commfides Certifcate 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 Commfides 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.
Commfides Trust Environment (CTE)	The Certificate-based Public Key Infrastructure governed by the Commfides Certificate Policies, which enables the worldwide deployment and use of Certificates by Commfides and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
Commfides UNID Service	Commfides have developed an UNID service in accordance with SEID leveranse nr 2 – Grensesnitt for tilgang til oppslagstjenester.
Commfides Professional Network (CPN)	The Commfides 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: Commfides, 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	An 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.
Subdomain	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.
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.

Table 11: Glossary of terms