COMFACT

Comfact CPS

Certification Practice Statement

Version date	**2022-02-16**
Classification	**Unclassified**
OID	**1.2.752.253.8.3**

Revision history of this document

This document Comfact CPS is valid from the date of its publication in Comfact Repository until a new version of the document is made available in the Comfact Repository with a new version date.

Version date	Description	Approval by
2022-02-16	First public version of new release of this document.	Comfact Certificate Service's Management Team

Table of contents

1 Scope

The present document outlines a) the CA Policy, describing the requirements and obligations for issuing digital certificates, and b) the Certification Practice Statement (CPS) of Comfact Certificate Service, describing the premises, procedures, and processes in fulfilling the CA Policy. Any references made herein to 'CP' refer to the present version of this document.

The CPS gives the reader insight into how the requirement and obligations are enforced in order to securely issue and manage digital certificates. Note, however, that the following CPS may reference additional, internal documentation that are not elaborated on in detail herein nor made public elsewhere (e.g., in-depth technical description, security testing, and blueprints of floor plans).

The CPS presented in this document describes the certificate practices employed in issuing digital certificates to:

- A natural, private person as part of an independent signature service,
- Digital certificates issued to or in affiliation with other entities such as employees, organizations for Timestamp or Seal signatures, and
- Digital certificates issued for internal services owned by Comfact AB.

2 References

The following documents contain provisions relevant to this document:

Reference	Description
ETSI 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI 319 412-3	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
ETSI 119 431-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
ETSI 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
ISO 27001	ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 6489	Certification Authority (CA) Key Rollover in the Resource Public Key Infrastructure (RPKI)
DIGG Policy	Normativa specifikationen för fristående underskriftstjänst, Policy fristående underskriftstjänst, version 1.4

3 Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

4 Introduction

4.1 Overview

The CPS presented in this document describe the content, issuance, revocation, and usage of digital certificates. This CPS is structured to align with IETF RFC 3647 and to conform with the requirements of extended Normalized Certificate Policy (NCP+) as outlined in ETSI 319 411-1, as well as to national policy requirements as stated in DIGG Policy.

The present document is aligned with IETF RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

4.2 Document name and identification

The CPS specified in this document is titled “Comfact CPS” and holds the object-identifier (OID): 1.2.752.253.8.3

It (this CPS) abides by the Normalized Certificate Policy: {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2}.

Note: this CPS is common for all Comfact NCP+ certificates, meaning other CPS documents may refer to this document while issued certificates will refer to the OID related to those (other) specific CPS documents.

4.3 PKI participants

Comfact issues digital certificate to Comfact’s own services, its employees, and its customers. All CAs issued under this CPS must comply with the practices specified herein. However, Comfact Certificate Services retain overall responsibility for conformance with the procedures prescribed in this CPS.

The following describes the identity or types of entities that fill the roles of participants relevant for Comfact Certificate Service’s PKI, namely: CA, RA, Subscribers, and Relying Parties.

4.3.1 Certification Authorities

Certificate authorities, or CAs, are entities such as Comfact Certificate Services that is authorized to issue (i.e., create, sign, and distribute) and revoke public key certificates. However, in the present document, the term CA is used to reference a certificate used to sign other certificates (CA and end-entity), certificate revocation lists (CRL), and Online Certificate Status Protocol (OCSP) responses, whilst the administrative instrument to operate such operations is referred to as the CA system (e.g., EJBCA). As such, Comfact Certificate Service act as the Trusted Service Provider (TSP) and is responsible for managing the life cycle of CAs and end-entity certificates signed by those CAs, as well as providing status information of the issued certificates throughout their lifetime. This includes:

- Issue and sign digital certificates for Subscribers, CA, and RA operators (see section 7.1-7.8),
- Publish CRLs on a regular basis and provide OCSP responses for supported enteties (see section 7.9) as well as maintain distribution points, and
- Distribute issued end-entity digital certificates (see section 9.1.2).

4.3.2 Registration Authorities

The registration authority (RA) is a module (internal or external to the CA system) authorized to perform registration functions, i.e., identification, authentication, and approval of certificate applicants (see section 6 and 7 for further details on the enrollment process), for end-entity certificates on behalf of Comfact Certificate Service.

The RA modules are responsible for the following activities:

- Identify and authenticate submitted certificate requests from Subscribers (see section 6),
- Handle revocation requests for certificates (see section 7.9), and
- Manage applications for renewal or re-keying of certificates (see sections 7.6-7.7).

4.3.3 Subscriber

A subscriber to Comfact Certificate Services is an entity, natural or legal person, that 1) holds a service agreement with Comfact AB, 2) have agreed to its terms and conditions, and 3) fulfils the obligations defined in this CPS relevant to that entity. That is to say, obligations of an individual or entity that has been issued a certificate and is authorized to use the corresponding private key for a particular usage.

When the Subscriber is a legal person, that entity is responsible for the activities of their associated end-user and Relying Parties, and are expected to inform them of appropriate usage of certificates issued by Comfact Certificate Services according to the agreed terms and conditions, as stated in the aforementioned service agreement with Comfact AB.

When the subscriber is a natural person, that individual will be held directly responsible if its obligations are not correctly fulfilled according to the service agreement with Comfact AB.

4.3.4 Relying Parties

A Relying Party is an entity or individual that relies on a certificate, or digital signature associated with a certificate, issued by Comfact Certificate Services under the CSP presented in this document. As such, a relying party may be any other organization, individual, application, or device. A Relying Party may or may not be a Subscriber.

4.3.5 Other participants

No other participants are currently defined.

4.4 Certificate usage

Certificates issued by Comfact Certificate Services under the CSP presented in this document can be used in a variety of applications to establish integrity, authenticity, and confidentiality.

4.4.1 Appropriate certificate usage

Certificates issued under this CPS are intended for the following applications:

- *Root certificates*: used to create intermediate CAs,
    - *Intermediate CAs*: used to issue short-lived, end-entity certificates
        - *Signing Certificates*: short-lived certificates intended for natural persons used for digital document signing.
        - *Seal Certificates*: short-lived certificates intended for legal persons used for digital document signing or timestamping.
        - *Service Certificates*: short-lived certificates intended for Comfact AB owned services used to authenticate computer-to-computer communication.

An overview of the appropriate certificate usage is outlined in the table below.

Certificate Authority Certificate	Appropriate Usage
Comfact Root CA G1	Root certificates used to issue intermediate CAs and sign certificate revocation lists (CRL).
Comfact Signature CA G1	This intermediate CA sign certificate revocation lists (CRL), online certificate status protocol (OCSP) responses, and issues short-lived, end-entity certificates for natural individuals that are intended to be used for signing digital documents (e.g., PDF and XML).
Comfact Seal CA G1	This intermediate CA sign certificate revocation lists (CRL) and issues short-lived, end-entity certificates for legal entities that are intended to be used for signing digital documents (e.g., PDF and XML) or data (e.g., timestamps).

Comfact Services CA G1	This intermediate CA issues short-lived, end-entity certificates used by Comfact AB owned services for authenticating computer-to-computer communications.

Note: see section 9.1.7 and the Certificate Profiles in section 10 for further specification of the intended key usage for each type of certificate.

4.4.2 Prohibited certificate usage

Certificates issued under this CPS are not intended for electronic communication and transactions (e.g., computer-to-computer communication and authentication). However, certificates issued to Comfact AB owned services, i.e., issued by the Comfact Services CA (see section 10.1.4), are intended to be used for computer-to-computer authentication, but is limited to the Key Usage of digital signature, and key encipherment or key agreement. The Extended Key Usage is prohibited, except for certain end-entity certificates which allows for timestamping or Microsoft document signing. See section 10.1 for more information.

In addition to the specified key usage, certificates issued under this CPS shall not be used in any circumstance that may breach law or regulation, this CP, or other relevant Subscriber agreements with Comfact AB.

4.5 Policy Administration

4.5.1 Organization administering the document

Comfact Certificate Service's Policy Management Team is responsible for authoring, reviewing, and approving changes to this CPS. Proposals on changes shall be submitted in written and signed form to the contact as described in section 4.5.2 below. Any decisions on changes are at the sole discretion of the Comfact Certificate Service's Management Team.

Contact information
Comfact AB Certificate Services Stora Badhusgatan 18 SE-411 21 Gothenburg, Sweden +46 (0)31 13 53 15 support@comfact.com

4.5.2 Contact person

Contact details on matters related to this CPS
Comfact AB Certificate Services Stora Badhusgatan 18 SE-411 21 Gothenburg, Sweden +46 (0)31 13 53 15 support@comfact.com

4.5.3 Person determining CPS suitability for the policy

Comfact Certificate Service's Management Team is the management body with overall responsibility for Comfact Certificate Services and has final authority for approving the CPS and determining its suitability to the applicable policies.

4.5.4 CPS approval procedures

Comfact Certificate Service's Management Team reviews any proposed changes to and modifications of this CPS to determine if any additions or deletions are necessary, acceptable, and conforms with the security standards and policies as outlined herein.

4.6 Definitions and acronyms

For the purposes of this document, the following definitions apply:

Term	Definition
CA system	Composition of IT products and components organized to support the provision of certificate authority related services
Certification Practice Statement	Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
Comfact Certificate Service	Comfact service for issuing certificates
Comfact CPS	The present document
Comfact or Comfact AB	Comfact AB with registered office Stora Badhusgatan 18, SE-411 21 Gothenburg, Sweden
Comfact Repository	Documents are currently available at request to: info@comfact.com or at https://www.comfact.se/en-us/resources/repository
Comfact Service Agreement	Agreement between Comfact and a subscriber or customer on the conditions to use the service
Coordinated Universal Time	Time scale based on the second as defined in Recommendation ITU-R
Relying party	Recipient of a time-stamp who relies on that time-stamp
Subscriber	Legal or natural person who is bound to obligations included in a Comfact Service Agreement
Timestamp	Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time
Trust service	Electronic service that enhances trust and confidence in electronic transactions
Trust Service Provider	Entity which provides one or more trust services

The following abbreviations are relevant in this document:

Abbreviation	Meaning
CA	Certification Authority
CPS	Certification Practice Statement
ISMS	Information Security Management System according to ISO 27001
OID	Object Identifier
RA	Registration Authority

TSP	Trust Service Provider
UTC	Coordinated Universal Time
CRL	Certificate Revocation List
CARL	Certification Authority Revocation List
OCSP	Online Certificate Status Protocol

5 Publication and repository responsibilities

5.1 Repositories

Information related to Comfact Certificate Services can be found at Comfact Repository: https://www.comfact.se/en-us/resources/repository

5.2 Publication of certification information

A full version of this CPS, alongside the listed items below, are published at Comfact Repository—publicly available 24 hours per day, 7 days per week, excluding scheduled maintenance or other planned breaks.

Upon system failure, maintenance, service, or factors which are not under the control of Comfact AB, Comfact Certificate Services shall, to the best endeavor and commercially reasonable effort, ensure that the information service is not unavailable for longer than a maximum of one (1) business day.

Additional public items published:

- Comfact Certificate Service's issued CA certificates, i.e., root and intermediate,
- Current versions of certificate revocation lists (CRL), listing all hitherto revoked certificates at the time of its publication, and
- Earlier versions of this CP/CPS.

5.2.1 Publication of CRL

CA	URL
Comfact Root CA G1	http://pki.comfact.com/crls/comfact-root-ca-g1.crl
Comfact Signature CA G1	http://pki.comfact.com/crls/comfact-signature-ca-g1.crl
Comfact Seal CA G1	http://pki.comfact.com/crls/comfact-seal-ca-g1.crl
Comfact Services CA G1	http://pki.comfact.com/crls/comfact-services-ca-g1.crl

5.2.2 Publication of OCSP

CA	URL
Comfact Signature CA G1	http://pki.comfact.com/ocsp/comfact-signature-ca-g1

5.3 Time or frequency of publication

This CPS is reviewed, updated and modified (see defined review process for the practices including responsibilities for maintaining the CPS in section 12.1.12) at least once per year. CRLs are published at a frequency as described in 7.9.7.

Publications and planned changes, including termination of services, are communicated to employees, subscribers, and relying parties as relevant.

5.4 Access controls on repositories

This CPS, all CRLs and CA certificates are publicly available, and no access control is required to gain access and download material published on the repository, as referenced in section 5.2. Only authorized Comfact Certificate Service personnel have written access to the repository.

6 Identification and authentication

This component describes the procedures used to authenticate the identity and other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance.

6.1 Naming

6.1.1 Types of names

All X.509 certificates must use Distinguished Name (DN) attributes as specified in recommended in ITU-T X.520 for unambiguous name of the Subject in the “Subject” field of the certificate. Certificate names shall not be misleading but must specify meaningful names in accordance with the X.509 conventions following the requirements for naming as recommended in IETF RFC 5280.

For certificates issued to natural persons, the certificate profile correlates to the recommendations in ETSI EN 319 412-2. For certificates issued to legal entities, the certificate profile correlates to the recommendations in ETSI EN 319 412-3. For a more detailed overview of the resulting certificate profile, see section 10.

6.1.1.1 Root CA

The following relative distinguished names are used for the root CA certificate issued by Comfact Certificate Services.

Attribute	OID	Description of Value
commonName (CN)	2.5.4.3	The name of the CA. The attribute specifies the name by which the CA is commonly known by in a particular context, e.g., Comfact Services CA G1.
organizationalName (O)	2.5.4.10	The name of the CA organization, e.g., Comfact AB.
organizationUnitName (OU)	2.5.4.11	A name that identifies the organizational unit with which the named entity is affiliated, e.g., Certification Services.
Country (C)	2.5.4.6	The country code, chosen from ISO 3166, describing where the CA organization is incorporated, e.g., SE.

6.1.1.2 Intermediate CA

The following relative distinguished names are used for intermediate CA certificate issued by Comfact Certificate Services.

Attribute	OID	Description of Value
commonName (CN)	2.5.4.3	The name of the subordinate CA. The attribute specifies the name by which the CA is commonly known by in a particular context within the organization, e.g., Comfact Signature CA G1.

organizationalName (O)	2.5.4.10	The name of the CA organization, e.g., Comfact AB
organizationUnitName (OU)	2.5.4.11	A name that identifies the organizational unit with which the named entity is affiliated, e.g., Certification Services.
organizationIdentifier (OI)	2.5.4.97	An identification of an organization different from the organization name, e.g., 5563426666.
Country (C)	2.5.4.6	The country code, chosen from ISO 3166, describing where the CA organization is incorporated, e.g., SE

6.1.1.3 End-entities

When the end entity is a natural person, the following attribute may be used:

Attribute	OID	Description of Value
commonName (CN)	2.5.4.3	The name of the subject.
Country (C)	2.5.4.6	The country code, chosen from ISO 3166, describing where the subject is citizen.
serialNumber	2.5.4.5	A unique identifier for the subject (see ETSI EN 319 412 section 5.1.3), e.g., based on personal number.
surame (SN)	2.5.4.4	The surname of the subject by which the individual is commonly known.
givenName	2.5.4.42	The name of the subject by which the individual is commonly known.
dateOfBirth	1.3.6.1.5.5.7.9.1	The name of the subject by which the individual is commonly known.

When the end entity is a legal person, or a Comfact AB service, the following attribute may be used:

Attribute	OID	Description of Value
commonName (CN)	2.5.4.3	The name of the subject. The attribute specifies the name by which the subject is commonly known by in a particular context.
organizationalName (O)	2.5.4.10	The name of the subject organization, e.g., “Comfact AB”.
Country (C)	2.5.4.6	The country code, chosen from ISO 3166, describing where the subject organization is incorporated.
organizationIdentifier (OI)	2.5.4.97	A unique identifier for the subject (see ETSI EN 319 412 section 5.1.3), e.g., based tax identification number.

Note that additional DN, Subject Alternative Name, and Subject Directory attributes may be used as necessary (e.g., as required by national standards) but is verified and granted by Comfact Certificate Services personnel.

6.1.2 Need for names to be meaningful

Names shall be meaningful, as stated in section 6.1.1.

6.1.3 Anonymity or pseudonymity of subscribers

For a natural person, no Subscribers shall be anonymous or pseudonymous. For a legal person, the commonName attribute can include the name or pseudonym of the subject, but shall always contain the organizationName attribute that accurately identifies the Subscriber.

6.1.4 Rules for interpreting various name forms

The commonName (CN) attributes contains the name of the subject in the following forms:

Issuing CA	commonNamea Form
Comfact Root CA G1	The commonName for subordinate CAs issued by “Comfact Root CA G1” should be the name of the related function and context or organizational unit.
Comfact Signature CA G1	The commonName for end-entities issued by “Comfact Signature CA G1” to a natural person is composed of the given name and surname obtained from trusted identity providers, such as e.g., Swedish BankID.
Comfact Seal CA G1	The commonName for end-entities issued by “Comfact Seal CA G1” to a legal entity may contain a name commonly used by the subject to represent itself that does not need to be an exact match of the fully registered organization name.
Comfact Services CA G1	The commonName for end-entities issued by “Comfact Services CA G1” to a Comfact AB owned service may contain a name commonly used by the service to represent itself and is set by the development team of said service.

Country codes used in the Distinguished Name (DN) shall conform with ISO 3166.

In addition to the name forms for legal entities, the organization (O) attributes shall identify the Subject organization in relation to the subject being identified. This attribute (O), shall contain the registered name of the organization, without abbreviations. The organizationIdentifier (OI) shall contain an identification of the Subject organization that is different from the organization name, e.g., the organizational number.

6.1.5 Uniqueness of names

All X.509 certificates issued by Comfact Certificate Services shall contain a Distinguished Name (DN) that can uniquely identify a single subscriber. Subject name uniqueness in this document means that the issuing CA shall not issue certificates with identical DN to different entities. For example, in cases of natural or legal persons, a Subscriber may hold several different certificates with the same DN, but different entities cannot not share a common DN issued by the same CA.

If necessary, Comfact Certificate Services may append additional numbers or letters to subject names in order to ensure uniqueness.

6.1.6 Recognition, authentication, and role of trademarks

Comfact Certificate Services does not make any specific checks to avoid infringement of intellectual property rights (IPR). The subject organization is responsible for ensure that their names do not infringe upon any IRP of any other company, organization, or agency. However, Comfact Certificate Services require each subject organization to provide legal documentation that is confirms their claimed identity before a certificate is issued in their name. See section 6.2.2 for more information.

6.2 Initial identity validation

This section describes the procedure for Comfact Certificate Service’s initial registration for each subject type. Comfact Certificate Service’s verifies that the identity of the Subscriber and Subject, and any certificate request, are correct based on the collected identity claims (e.g., name).

6.2.1 Method to prove possession of private key

All CA private keys are generated by Comfact Certificate Services and stored in Hardware Security Modules (HSM) certified to at least NIST FIPS 140-2 level 3.

If the Subject wants to generate and host their own key-pair, Comfact Certificate Services shall 1) verify the electronic signature of the PKCS#10 Certificate Sigining Request (CSR), 2) make sure it corresponds to the public key within the CSR and thereby verify the integrity of the signed data, and 3) that the private key has been generated within a security module which meets the same requirement as if generated and hosted by Comfact Certificate Services. Alternatively, a Smart Card that meets the same security requirement can be provided by Comfact to the Subject, if physically present.

6.2.2 Authentication of organization identity

Comfact Certificate Services verifies third-party identities through provided legal documentation that is confirmed through official business registration before entering into agreement with Comfact. In particular, claims regarding full name, dates, and legal status of the associated legal person (e.g., natural person associated with the Subscriber), as well as affiliation and relevant existing registration information (e.g., company registration) of the associated legal person is checked.

6.2.3 Authentication of individual identity

Comfact Signature CA G1 issues end-entity certificates for natural persons. The process is based on an autoenrollment RA, which verifies submitted Subject information from trusted identity providers (IdP, e.g., BankID, that reaches a level of assurance equal or greater than 3, in accordance with DIGG Policy). Only after a request from a Subscriber has been verified, along with the identity of the intended certificate Subject, does Comfact Certificate Services proceed with generating a new key-pair for a short-lived, end-entity certificate. See certificate profile in section 10.1.4 for details on what information is required and included in the Subject end-entity certificate.

6.2.4 Non-verified subscriber information

No key pair and certificate shall be generated to subscribers that are unable to prove their identity.

6.2.5 Validation of authority

Comfact verifies that the Subscriber is currently in agreement with Comfact Certificate Services and verifies the authority of that same agreement.

Physical and logical access controls are used to restrict access to and management of Comfact Certificate Services, and is only accessible to a limited set of authorized, trusted personnel. Multiple authorized, trusted personnel is required to create new CAs.

6.2.6 Criteria for Interoperation

Not applicable.

6.3 Identification and authentication for re-key requests

Re-keying may be performed when certificates are about to expire or if existing key pairs are no longer retrievable or in use, e.g., when the private key has been compromised and revoked. For more information, see section 7.7.3. The process for re-keying requests is outlined in section 7.7.

6.3.1 Identification and authentication for routine re-key

Re-keying for intermediate CAs is handled in the same manner as when creating a new intermediate CA request, see section 7.1. If any changes are made in the subject or certificate distribution, the request shall be validated in the same way as the initial registration.

Re-keying of short-term, individual certificates the initial certificate process shall be used.

6.3.2 Identification and authentication for re-key after revocation

In accordance with 6.3.1.

6.4 Identification and authentication for revocation requests

The following table outlines the handling of revocation request based on its issuing CA.

Issuing CA	Revocation routine
Comfact Root CA G1	Key-pairs for subordinate CA certificates issued by "Comfact Root CA G1" are generated and stored by Comfact Certificate Services and can only be requested for revocation by authorized personnel. Such a request must be submitted by creating the internal incident report form "Comfact Incident Report DATE+TIME.docx. Upon such a request, multiple (n-out-of-m, where n=2) trusted personnel of Comfact Certificate Services are required to peruse the incident report and reach a unanimous decision if the incident is cause for revocation, and for what reason. Upon reaching a decision to revoke, multiple (n=2) personnel of Comfact Certification Services are required to enable the root key in order to revoke the CA. The procedure is outlined in greater detail under section 7.9.
Comfact Signature CA G1	For short-term, end-entity certificates issued to a natural person, the key-pairs are either generated and stored by Comfact Certificate Services or on a secure cryptographic module by the Subject. – In case where the Subject's keys are generated and stored by Comfact, the keys cannot be reported as compromised by the Subscriber or Subject, and can only be revoked through an incident report if a) the secure facility of Comfact Certificate Services has been (or is suspected to have been) compromised, or b) the issued certificate was the result of identity theft (in accordance with national law) on behalf of the subscriber. – In case where the Subject generate and store the key on their own secure cryptographic module (e.g., a Smart Card) a revocation request can be submitted through e-mail or post (contact details are outlined in section 4.5.2). The request must include the following information: o The certificate Subject identifier, o The reason for the revocation, o The Subject's phone number or e-mail address.
Comfact Seal CA G1	For short-term, end-entity certificates issued to a legal person, a revocation request can be submitted through e-mail or post (contact details are outlined in section 4.5.2). The request must include the following information: – The certificate Subject identifier, – The reason for the revocation, – The Subscriber's phone number or e-mail address.
Comfact Services CA G1	Key-pairs for short-term, end-entity certificates issued by "Comfact Services CA G1" are generated and stored by Comfact Certificate Services and can only be requested for

	revocation by authorized personnel. Such a request must be submitted by creating the internal incident report form "Comfact Incident Report DATE+TIME.docx."

Requests for revocation, or reports of events relating to revocation, is processed on receipt. Meaning, the maximum delay between receiving a revocation request, or report of event relating to revocation, and reaching a decision as to change the status or not of a particular certificate is 24 hours—thereby making the new status information available to all relying parties through updated CRLs, and in the case of short-lived, end-entity certificates issued to a natural person (see section 10.1.5), also upon OCSP requests.

If the authenticity of or reason for the revocation request or reports of event relating to revocation cannot be confirmed within 24 hours, the status will not be changed.

Future dates (i.e., to have the revocation status scheduled to change at a later date) may be accepted after having been considered by Comfact Certificate Services.

7 Certificate life cycle operational requirements

7.1 Certificate application

In the present document, certificate application refers to the initial registration, re-keying, or modification of subordinate CAs, as well as the issuance of end-entity certificates.

7.1.1 Who can submit a certificate application?

The following table outlines a list of people and systems who can submit a certificate application:

Issuing CA	Certificate Application
Comfact Root CA G1	Applications for subordinate CAs can be submitted by an authorized Comfact Certificate Services employee, or, an authorized Subscriber that is in agreement with Comfact to host their CA at Comfact Certificate Services.
Comfact Signature CA G1	Any natural person who has been successfully identified by a trusted IdP by Comfact Signature Services and is in agreement with an approved Subscribed is able to obtain an end-entity certificate.
Comfact Seal CA G1	A legal person who has been successfully identified by Comfact Signature Services and is in agreement with Comfact.
Comfact Services CA G1	Applications for end-entity certificates can be submitted by an authorized Comfact Certificate Services employee.

7.1.2 Enrollment process and responsibilities

The following table outlines a list of processes and responsibilities for enrollment:

Issuing CA	Enrollment Process / Responsibilities
Comfact Root CA G1	The enrollment process of the root CA-certificate itself follows a specific key ceremony. The generation of a new root key-pair, and subsequently the certificate, is followed by the generation of a shared secret (n-out-of-m) to manage/enable it. The key ceremony script details the procedure for creating the key-pair and is further described in section 9.1. The ceremony results in a report that is signed by everyone present during the ceremony. During the enrollment of a new subordinate CA, a new CPS is prepared for that CA. However, an existing CPS may be used if appropriate, upon which the existing CPS shall be reviewed and updated accordingly.

	A Subscriber that is in agreement with Comfact to have their CA hosted by Comfact Certificate Services shall abide by this CPS, the new CPS (if any) of the subordinate Subscriber CA being enrolled, and other terms and conditions as relevant. Before the enrollment, authorized Comfact Certificate Service personnel must record the request information, subject, CPS, Subscriber using a root key ceremony specification before approving the certificate application. Multiple trusted personnel (n=2) of Comfact Certificate Services are required to review the root key ceremony specification, activate the root, and enroll a new CA certificate. The entire enrollment process is outlined in Comfact Certification operations key ceremony documentation.
Comfact Signature CA G1	This CA can only issue end-entity certificates to a natural person. This issuing process is the responsibility of the auto RA function, where a Subject's personal information will be provided by the Subscriber and verified against a trusted IdP (e.g., Swedish BankID, see section 6.2.3). As such, the trusted IdP used in the auto RA function is responsible for end-entity verification, while Comfact Certificate Service is responsible for verifying the IdP response. Once the identity is successfully verified, the new key-pairs can either be generated on Comfact HSMs or on the Subject's secure cryptographic module (e.g., a Smart Card). In cases where the key-pairs are generated by Comfact HSMs, the private key is short lived, meaning it is used in a signing operation and deleted immediately afterwards.
Comfact Seal CA G1	This CA can only issue end-entity certificates to a legal person. This issuing process is the responsibility of Comfact Signature Service, where a Subject's personal information will be provided by the Subscriber, as described in section 6.2.2.
Comfact Services CA G1	This CA can only issue end-entity certificates to a Comfact AB owned service. This issuing process is the sole responsibility of authorized personnel at Comfact AB.

7.2 Certificate application processing

7.2.1 Performing identification and authentication functions

The identification and authentication of Subject and Subscriber information is performed in accordance with section 6.2, and with the responsibilities as described in section 7.1.2.

7.2.2 Approval or rejection of certificate applications

Comfact Certificate Services shall approve a certificate application by an entity that is in agreement with Comfact, or with a Subscriber that is in agreement with Comfact, to use its Certificate Services and meets the requirements of validation and identification. All other certificate applications will be rejected.

Rejected certificate applications submitted by a Subscriber shall be informed of the rejection, and how to proceed to be approved by Comfact Certificate Services.

7.2.3 Time to process certificate applications

Comfact Certificate Services shall begin to process received certificate applications within a reasonable time frame. When a certificate is applied directly through Comfact Signature Service, the certificate request is processed automatically by the auto RA function (as described in section 7.1.2) immediately after the request is submitted.

There are no specific processing time requirements, unless otherwise specifically agreed with the Subscriber.

7.3 Certificate issuance

7.3.1 CA actions during certificate issuance

The following actions apply for the different certificate issuances:

- **CA Certificates**: In the case of issued CA certificates, the new key-pair and certificate is generated after the certificate application is approved by Comfact Certificate Services personnel, and in accordance with the key-ceremony (see section 9.1). Key-pairs are generated inside an HSM hosted by Comfact Certificate Services and remains hosted by Comfact Certificate Services to guarantee the private keys confidentiality during this process.
- **Natural Person Certificate**: In the case of short-lived, end-entity certificates issued to a natural person, Comfact Certificate Service's CA system verifies that the certificate request has been approved by the auto RA by validating the signature on the request sent from the auto RA function. The key-pair is then generated either inside a) an HSM hosted by Comfact Certificate Services, where it remains until it has been used, whereupon it is deleted, to guarantee the private keys confidentiality during this process. Or b) generated inside a security module (e.g., HSM or Smart Card that meets the security requirements expressed under section 9.2.1) maintained by the Subject.
- **Legal Person Certificate**: In the case of short-lived, end-entity certificates issued to a legal person, Comfact Certificate Service's personnel verifies the certificate request and the identity of the legal person (see section 6.2.2). The key-pair is then generated inside a security module (e.g., HSM or Smart Card that meets the security requirements expressed under section 9.2.1) maintained either by the Subscriber or Comfact Certificate Services.
- **Comfact Services Certificate**: In the case of short-lived, end-entity certificates issued to a Comfact AB owned service, Comfact Certificate Service's personnel verifies the certificate request and the identity of the authorized Comfact AB personnel. The key-pair is then generated inside a security module (e.g., HSM or Smart Card that meets the security requirements expressed under section 9.2.1) maintained by Comfact Certificate Services.

The issuance of a certificate only occurs if Comfact Certificate Service's accepts the certificate application and the submitted Subject information. However, the Comfact Certificate Services may overwrite or append some certificate Subject information as described in section 6.1.5.

7.3.2 Notification to subscribers by the CA of issuance of certificate

The following table outlines a list of notifications based on certificate type issuance:

Issuing CA	Certificate Issuance
Comfact Root CA G1	After an approved certificate application, the CA generates a new subordinate CA key-pair and certificate. Multiple (n=2) trusted personnel of Comfact Certificate Services are required to enable the root key in order to sign the new CA certificate. The Subscriber is then notified over e-mail of the creation of the certificate, where it can be obtained, and instructions for revocation—as outlined in section 6.4.
Comfact Signature CA G1	Subscribers will not receive any notification about the issuance of the certificate, instead, they are provided with the document signed using the newly generated, short-lived key-pair, including the embedded certificate.

Comfact Seal CA G1	After an approved certificate application, the Subscriber is notified over e-mail of the creation of the certificate, where it can be obtained, and instructions for revocation—as outlined in section 6.4.
Comfact Services CA G1	After an approved certificate application, the public certificate is rolled out to the intended Comfact AB owned service.

7.4 Certificate acceptance

7.4.1 Conduct constituting certificate acceptance

The Subscriber shall read and accepted the terms and conditions regarding the use of certificates before it being issued by Comfact Certificate Services. The agreement is recorded (e.g., in electronic form) in a contractual relationship between the Subscriber and Comfact.

Acceptance of the certificate is then assumed when the Subject:

- Starts using the certificate's key-pair, or
- When no authorized applicant has objected to the certificate within two business days.

7.4.2 Publication of the certificate by the CA

Comfact Certificate Services will publish CA certificates to Comfact PKI repository, in accordance with section 5. However, Comfact Certificate Services will not publish Subscriber end-entity certificates to a publicly available repository—unless otherwise agreed upon with the particular Subscriber.

7.4.3 Notification of certificate issuance by the CA to other entities

No notifications are sent to other entities.

7.5 Key-pair and certificate usage

7.5.1 Subscriber private key and certificate usage

In cases where the private key is hosted by the Subscriber, the Subscriber shall protect the private key from unauthorized use. The private-key must reside in a secure cryptographical module (typically a smart card provided by Comfact) that meets the security requirements expressed under section 9.2.1. Should the Subscriber notice that unauthorized entities have, or have had, access to their private key(s), the Subscriber shall notify Comfact Certificate Services immediately and request for revocation of the certificate.

For information regarding appropriate Subscriber key usage, see the keyUsage field extension in the certificate profiles, sections 9.1.7 and 10. Unauthorized use of the Subject's key, or use outside of the limitations notified to the Subscriber and Subject, is prohibited.

In cases where the private key is hosted by Comfact Certificate Services, and its intended use is for signing digital content (e.g., documents, agreements and/or transactions), sole control of the private key is ensured to the Subject in conformance to ETSI TS 119 431-1.

7.5.2 Relying party public key and certificate usage

It is the responsibility of the Relying Party to verify that the certificate issued to / used by a Subscriber is appropriate for the intended usage and in accordance with the keyUsage field extension included in the certificate.

Relying Parties that use certificates issued under this CPS to identify Subscribers shall independently ensure that the certificate was valid at the time of use (e.g., check the certificate validity date and verify from a valid CRL that the certificate, including its certificate chain, has not been revoked).

If these verifications cannot be satisfied (e.g., due to system failure or otherwise) the certificate shall not be accepted.

7.6 Certificate renewal

Certificate renewal is the process of re-issuing a certificate using the same public key and corresponding private key as before, but with a new validity date (see RFC 3647).

7.6.1 Circumstance for certificate renewal

No stipulation, certificate renewal is not allowed.

7.6.2 Who may request renewal?

No stipulation, certificate renewal is not allowed.

7.6.3 Processing certificate renewal requests

No stipulation, certificate renewal is not allowed.

7.6.4 Notification of new certificate issuance to Subscriber

No stipulation, certificate renewal is not allowed.

7.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation, certificate renewal is not allowed.

7.6.6 Publication of the renewal certificate by the CA

No stipulation, certificate renewal is not allowed.

7.6.7 Notification of certificate issuance by the CA to other entities

No stipulation, certificate renewal is not allowed.

7.7 Certificate re-key

Certificate re-keying is the process of re-issuing a certificate with a new public key and corresponding private key, but with the same subject and SAN values as before (see RFC 3647).

7.7.1 Circumstance for certificate re-key

Certificate re-keying might be an option when a certificate is about to expire, or has been revoked.

Short-lived, end-entity certificates issued to a natural person and hosted by Comfact Certificate Services HSMs, shall not be re-keyed as they are issued per request by the auto RA and the private key destroyed immediately after usage.

7.7.2 Who may request certification of a new public key?

Only authorized entities of a valid Subscriber may request a certificate re-keying, e.g., the same person who requested the initial certificate application—as described in section 7.1.1.

7.7.3 Processing certificate re-keying requests

The re-keying process is the same as the initial certificate application, as described in section 7.1-7.2.

7.7.4 Notification of new certificate issuance to Subscriber

Subscribers are notified in the same way as the initial certificate application, as described in section 7.3.2.

7.7.5 Conduct constituting acceptance of a re-keyed certificate

The conduct constituting acceptance of a re-keyed certificate is as described in section 7.4.1.

7.7.6 Publication of the re-keyed certificate by the CA

The publication of the re-keyed certificate is in accordance with the description in section 7.4.2.

7.7.7 Notification of certificate issuance by the CA to other entities

Since re-keyed certificates are processed in the same way as the initial certificate application, notifications of certificate issuance are in accordance with section 7.4.3.

7.8 Certificate modification

Certificate modification is the process of re-issuing a certificate with changes to its information (other than extension of its validity—see certificate renewal—or key-pair—see certificate re-keying) (see RFC 3647).

7.8.1 Circumstance for certificate modification

Certificate modification can occur when Subscriber's or Subject's changes e.g., name, affiliation, or role. However, short-lived, end-entity certificates issued to a natural person (with the keys generated by Comfact Certificate Services HSMs) shall not be modified as they are issued per request by the auto RA and used only for a particular instance.

7.8.2 Who may request certification modification?

Only authorized entities of a valid Subscriber may request a certificate modification, e.g., the same person who requested the initial certificate application—as described in section 7.1.1.

7.8.3 Processing certificate modification requests

The modification process is the same as the initial certificate application, as described in section 7.1-7.2.

7.8.4 Notification of new certificate issuance to Subscriber

Subscribers are notified in the same way as the initial certificate application, as described in section 7.3.2.

7.8.5 Conduct constituting acceptance of a modified certificate

The conduct constituting acceptance of a modified certificate is as described in section 7.4.1.

7.8.6 Publication of the modified certificate by the CA

The publication of the modified certificate is in accordance with the description in section 7.4.2.

7.8.7 Notification of certificate issuance by the CA to other entities

Since modified certificates are processed in the same way as the initial certificate application, notifications of certificate issuance are in accordance with section 7.4.3.

7.9 Certificate revocation and suspension

Revocation of certificates is supported by Comfact Certificate Services. Certificate suspension, however, is not supported.

Upon a certificate revocation, the certificates serial number is added to the CRL as well as the status of revoked along with a revocation reason, as defined in RFC 5280. If the revoked certificate is a short-lived, end-entity certificate issued to a natural person (see section 10.1.5), the revoked status will also be the response of any OCSP request. Once a certificate is revoked, the status is permanent and the certificate shall not be reinstated.

7.9.1 Circumstance for revocation

In cases where Comfact Certificate Services receive a certificate revocation request, Comfact Certificate Services personnel shall verify that the request was made in accordance with section 6.4.

The following table outlines a list of circumstances for revocation based on certificate type issuance:

Issuing CA	Circumstances for Revocation
Comfact Root CA G1 Comfact Certificate Services shall revoke a Subordinate CA certificate within the timeframe of five (5) days if one or more of the following circumstances occur.	• If the certificate is re-keyed, renewed, or modified, the original certificate shall be revoked, • If a certificate request is received, recorded, and agreed to in accordance with section 6.4 of this CPS, • If the original certificate request was not authorized, • If Comfact Certificate Services obtains evidence that the certificate is misused, • If Comfact Certificate Services suspect that the private-key has been compromised, • If Comfact Certificate Services is made aware that an issued subordinate CA does/has not complied with this CPS or other contractual agreements, terms, and conditions, • If Comfact Certificate Services determines that the information within an issued certificate is inaccurate, misleading, or otherwise no longer accurate or representative of the facts, • If the smart card or equivalent cryptographic module holding the private key is no longer in use or in possession of the Subscriber, • If a Subscribers contract with Comfact is terminated, • If the Subscriber terminates its relationship with Comfact, all of its issued certificates shall be revoked unless Comfact has agreed to continue maintaining the CRL repository.
Comfact Signature CA G1, **Comfact Seal CA G1,** **Comfact Services CA G1** Comfact Certificate Services shall revoke a Subscriber's certificate within the timeframe of five (5) days if one or more of the following circumstances occur.	• If a used CA-key is suspected of compromise, • If Comfact Certificate Services obtains evidence that the issued certificate was unauthorized, e.g., the result of identity theft (in accordance with national law), • If Comfact Certificate Services obtains evidence that the issuer's private key has been compromised, • If Comfact Certificate Services obtains evidence that the information within the certificate is inaccurate.

7.9.2 Who can request revocation?

Revocation requests can be made by:

- Authorized entities of a valid Subscriber—e.g., the same natural / legal person who requested the initial certificate application—or RA acting as a Subscriber that made the initial certificate application on behalf of a Subscriber or Subject,
- Authorized Comfact Certificate Services personnel upon receiving requests or sufficient evidence about one or more of the reasons listed in section 7.9.1,
- A Subject, to whom the certificate is issued to.

7.9.3 Procedure for revocation requests

All entities requesting certificate revocation shall be identified as described in section 6.4.

Subscribers and Subjects are required to promptly request for a certificate to be revoked if they are involved in a security incident that may have compromised the private key or its usage.

For revoking a certificate, Comfact Certificate Services shall first identify and authenticate the requester as described in section 6.4. Only authorized Comfact Certificate Services personnel can then approve the certificate revocation requests. Upon approval, the certificate shall be permanently revoked. The revocation process shall take proceed within reasonable time in accordance with section 6.4.

7.9.4 Revocation request grace period

Revocation of certificates can be submitted to Comfact Certificate Services 24 hours per day, 7 days per week.

Subscribers, or RAs acting on behalf of Subscribers, are required to report any suspected compromise of their private keys and make a certificate revocation request to Comfact Certificate Services. The certificate revocation request shall be made within 24 hours after the discovering the suspected compromise. Authorized Comfact Certificate Services personnel shall then decide on and carry out the certificate revocation within 24-hours. The delay is set to give reasonable time to gather enough information to make an accurate decision (e.g., verify the identity of the requester).

Comfact shall not be held responsible for any damage caused by wrongful usage of the Subject's private key, but shall be responsible for the publication of the revocation status in the form of CRL and, in the case of short-lived end-entity certificates issued to a natural person (see section 10.1.5), also OCSP.

7.9.5 Time within which CA must process the revocation request

The publication of updated revocation status for a particular certificate shall be made within one (1) hour after a certificate revocation request has been processed and the certificate marked for revocation.

7.9.6 Revocation checking requirement for Relying Parties

The responsibility of checking and verifying certificate revocation status lies solely with the Relying Party. The Relying Party shall verify the revocation status by consulting the most recent CRL identified from each certificate in the chain of the certificate the relying party which to check.

As such, it is up to the Relying Party to verify that:

- The CRL used to check the certificates revocation status is the most recent,
- The signature of the CRL is valid, and that
- The CRL is still valid.

If the Relying Party is verifying a short-lived, end-entity certificate, the status can also be checked though OCSP.

7.9.7 CRL issuance frequency

Each subordinate, issuing CA hosted by Comfact Certificate Services shall produce an updated version of their respective CRL on a 24-hour basis. That is to say, the nextUpdate field of the CRL shall refer to a point in time 24-hours after thisUpdate. However, CRL overlap period specified for this CPS is half of the nextUpdate time, which means that the nextPublishTime shall refer to a point in time 12-hours after thisUpdate. This is done to allow for a margin of error issuing the updated CRLs.

Upon reaching the end of a CA's life, the last issued CRL shall set the nextUpdate field to "99991231235959Z", as defined in RFC 5280.

Root certificates are maintained in an offline state, and will issue a new Certification Authority Revocation List (CARL) every year (i.e., the nextUpdate field is set to one (1) year after the issuing date). Upon a subordinate CA being revoked, a new CARL shall be generated.

7.9.8 Maximum latency for CRLs

CRL are submitted to the repository within one (1) hour after generation (however, this is typically done automatically, as soon as they are generated, and therefore within minutes).

7.9.9 On-line revocation/status checking availability

Comfact Certificate Services offer access to an online repository where updated CRLs are published. Online certificate status protocol (OCSP) responses are available only for short-lived, end-entity certificates issued to a natural person (see section 10.1.5), which is signed by its issuer.

7.9.10 On-line revocation checking requirements

Relying Parties must confirm the revocation status of a certificate by consulting the most recent CRL in accordance with section 7.9.6, prior to trusting the certificate.

7.9.11 Other forms of revocation advertisements available

No other forms of revocation information are published or advertised elsewhere.

7.9.12 Special requirements regarding key compromise

Comfact Certificate Services shall use commercially reasonable efforts to notify potential Relying Parties if it is discovered, or if there is reason to believe, that a private key has been compromised. Upon which the certificate with the corresponding public key is revoked with reason code keyCompromise, as defined in RFC 5280.

In cases of a private key being compromised that is hosted by Comfact Certificate Services, the procedure as outlined in section 8.7.3 shall be followed.

In cases of a private key being compromised that is not hosted by Comfact Certificate Services, the incident shall be reported to Comfact instantly by the Subscriber, as described in section 7.9.3.

7.9.13 Circumstances for suspension

Not applicable.

7.9.14 Who can request suspension?

Not applicable.

7.9.15 Procedure for suspension request

Not applicable.

7.9.16 Limits on suspension period

Not applicable.

7.10 Certificate status services

7.10.1 Operational characteristics

All CRLs are published on Comfact website, as specified under section 5.2.

7.10.2 Service availability

Comfact Certificate Service's certification status service is publicly available 24 hours per day, 7 days per week—excluding scheduled maintenance or other planned breaks.

Upon system failure, maintenance, service, or factors which are not under the control of Comfact, Comfact Certificate Services shall to the best of endeavor ensure that the information service is not unavailable for longer than a maximum of one business day.

7.10.3 Optional features

No revocation status information shall be removed before the expiry date of the revoked certificate.

7.11 End of subscription

End of subscription as the result of no longer requiring Comfact Certificate Services, being in breach of- or otherwise compromising the contract between the Subscriber and Comfact will result in termination of the CA as described in section 8.8.

If the Subscriber terminates its relationship with Comfact, or termination of employment (voluntary or imposed), all issued certificates under that Subscriber's CA shall be revoked, unless Comfact has agreed to continue maintaining the repository and revocation information till the Subscriber's CA expires, as described in section 7.9.1.

7.12 Key escrow and recovery

7.12.1 Key escrow and recovery policy and practices

Key escrow and recovery are not supported.

However, backups of Subscribers private keys that are hosted by Comfact Certificate Services may be kept, but will not be escrowed. The number of backups shall not exceed the minimum needed to ensure continuity of the service. The backups are only kept for continuity purposes, and are protected in an encrypted form (e.g., Smart Card or other cryptographic modules) with no lower security than the original subject's private key. The decryption mechanism for restoring the key backups is fractioned onto several (n-out-of-m) Smart Cards entrusted to trusted persons of Comfact Certificate Services personnel. Restoration of the backups onto a cryptographic module can only proceed if at least two (2) of said personnel participate in the restoration with their entrusted smart card.

For short-lived, end-entity certificates issued to a natural person (where the key-pairs are generated by Comfact Certificate Service's HSMs), there is no key-escrow or recovery, since the private key is immediately deleted after being used.

7.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

8 Facility, management, and operational controls

Physical, logical, and administrative controls are the result of a risk assessment carried out over Comfact Certificate Service's systems, facilities, and operation. The risk assessment is part of a wider information security management system, under the current ISO 27001 certification. As such, an inventory of information assets is retained and kept up to date, where each asset is classified and valued according to Comfact classification scheme, as part of the risk assessment, and handled according to Comfact data handling scheme.

Trusted personnel of Comfact Certificate Services must accept or reject the residual risk. The risk assessment is regularly reviewed and revised.

8.1 Physical controls

Physical security controls are put in place to protect against various types of threats. For example, the data centers used are geographically separate from Comfact office space, and various protective measures are put in place against unauthorized access, such as breaking and entering, but also natural disasters, fire, and power failure, as well as other, external threats. For example, maintaining a stable Internet connection, should disruption that lays beyond the premise of the data center (e.g., a severed cable), by multiple Internet connections maintained by separate Internet service providers.

8.1.1 Site location and construction

Comfact Certificate Service's CA operations are provided in a secure data center. The data center is protected by multiple tiers of physical security, e.g., access control systems, alarms, and camera monitoring on 24 hours a day 7 days a week basis, designed to deter, prevent, and detect covert or overt penetration, in order to only allow access for authorized individual.

8.1.2 Physical access

The physical location is independently monitored by a third-party, as well as surveillance equipment maintained by Comfact in the security area. Each request to enter the facility is logged (time marked for entrance and exit). Upon entry, each person has to register and identify themselves, whereupon they are checked against a white-list, and accompanied by a security escort during the stay. Finally, Comfact CA related hardware and software (e.g., for certificate generation and revocation management services) is locked in a separate high security area, where only a limited number of trusted roles have access.

Similarly, root CA keys are held offline in a physically isolated form, with the same level of security as its normal location of operation, that only designated, trusted Comfact Certificate Service personnel have access to.

8.1.3 Power and air conditioning

There are two power supplies, primary and secondary, to ensure continuous and uninterrupted power supply. Redundancy is provided in the form of battery uninterrupted power supplies (UPS) and diesel generators.

Air condition, heating, and ventilation is provided and dimensioned to control temperature and relative humidity for a commercial data processing facility.

8.1.4 Water exposures

Measures to protect against water exposure is taken in order to ensure high level of availability of Comfact Certificate Services, including revocation management. Prevention of water exposure is, for example, prevented with structural solutions, e.g., no pipes traverse the controlled, high security area allocated by Comfact.

8.1.5 Fire prevention and protection

Measures to protect against fire is taken in order to ensure high level of availability of Comfact Certificate Services, including revocation management. The facility used is, for example, equipped with fire suppression in accordance with local fire safety regulations.

8.1.6 Media storage

All media holding data relation to the production environment (e.g., software, audit information, backups, archive, etc.) are stored within Comfact facilities, secured with appropriate physical, logical, and administrative controls, not only to limit access to authorized personnel, but to ensure confidentiality, integrity, and availability.

8.1.7 Waste disposal

All sensitive data and information are shredded before disposal, and physical media (e.g., cryptographic devices) are physically destroyed and / or wiped in a secure manner prior to disposal.

8.1.8 Off-site backup

Comfact provides routine backups of its critical systems, its data, audit logs, software, and other critical and/or sensitive information. Office backup is constructed in a mirrored environment, and holds similar security as the primary environment site. Due to security reasons, the full scope of the backup routines is not disclosed publicly.

8.2 Procedural controls

The following section outlines administrative controls in terms of operating procedures enacted by Comfact Certificate Services. Note that Comfact Certificate Services retain overall responsibility for conformance and operational functionality, including third-party and outsourced components. The liability is defined in the contract with these parties and considered as part of the risk assessment.

8.2.1 Trusted roles

Personnel (e.g., employees, consultants, and contractors) that manage Comfact infrastructure shall be considered as trusted. People who obtain a role managing Comfact infrastructure must undergo and meet the required security screening, see section 8.3. Ceased, terminated, or modified roles are updated or removed within a reasonably timely manner.

Trusted personnel include those roles that have access to secure facilities, control authentication, and/or oversee cryptographic operations that may affect:

- Manage Subscriber requests and information,
- Review and conclude Certificate Applications,
- Review and conclude revocation, renewal, re-keying, or modification requests, and
- Processing, rejection, and issuance of Certificates.

All personnel in trusted roles must be free from conflict of interest that might bias or prejudice the impartiality of Comfact Certificate Service's CA or RA operations.

Trusted personnel define separation of trusted roles and access to information and application system functions. Note that all trusted personnel shall be identified and authenticated before access and use to critical applications related to Comfact Certificate Services. These roles include:

- **Security Officers**: Overall responsibility for planning and overseeing implementation and governance of security practices. This includes planning and reviewing logical, physical, and administrative security controls as well as review logs and archives for incidents, anomalies, attempted compromise, and so on.
- **System Administrators**: Authorized to install, configure, and maintain Comfact Certificate Service CA systems, e.g., to generate new end-entity key-pairs, issue and revoke certificates, generating revocation lists, manage CA system accounts and audit certificate issue logs.
- **System Operators**: Responsible for operating Comfact Certificate Services systems and hardware on a day-to-day basis, including servers, network configuration of firewalls and routers, and maintain systems updated, patched, and backed up for stability and recoverability.
- **System Auditor**: Responsible for accessing archives and audit logs of Comfact Certificate Services CA systems, e.g., to control and review system operation, assess past or present anomalies, and suggest enhancements in controls, polices, and procedures.
- **HSM Administrator**: Authorized to install, configure, and maintain the hardware security modules, e.g., securely setup or dispose of HSMs, and perform backups of private keys.
- **Systems Developer**: Authorized to develop, configure, and maintain Comfact Certificate Service's custom software and applications, e.g., auto-RA and electronic signature functionality.
- **Secret Share Holder**: Responsible to ensure the confidentiality, integrity, and availability of a secret assigned (e.g., part of an m-or-of-n secret to enable a certain private CA key).

Further details of trusted roles within Comfact are specified in a classified document, and shall therefore not be detailed publicly.

8.2.2 Number of persons required per task

The number of persons required to carry out manual, sensitive CA tasks are at least two (2) people. All participants shall hold a trusted role as defined in section 8.2.1, where at least one shall be an administrator. Example of sensitive tasks include CA key generation, certificate issuance by the root CA, decisions regarding revocation of certificates, and HSM related operations (e.g., backups and recovery). For some sensitive tasks, like key-ceremony, many more people are required for security reasons. The objective is to limit the possibility of malicious activities being carried out by one actor.

The following activities are examples which shall only be allowed with multiple-person control (n-out-of-m):

- Access to the hosting area of the CA, where HSM containing private keys as well as servers with CA system and related material are stored and operate,
- Changes to the HSM, e.g., creating, removing, activation, or backing up of private keys, and
- Access to backups of private keys.

The following activities are examples which shall only be allowed after a person has been successfully identified with strong authentication or multi-person control (n-out-of-m):

- Access to and administration of application servers of Comfact Certificate Services,
- Access to and administration of Comfact Certificate Services PKI repository,
- Access to and administration and issuance of end-entity certificates, and
- Access to and administration of databases related to PKI services.

8.2.3 Identification and authentication for each role

Trusted personnel interacting with the CA systems must first authenticate themselves before they are allowed access to the system. Access to the CA system is limited to predefined user accounts and can only on the specific local network (e.g., over VPN that requires valid user credentials to access). Physical access to HSMs is only possible through physical visits to the secure facilities, and only by specific whitelisted, trusted personnel, logical access to particular keys is limited to multiple trusted Secret Share Holders.

8.2.4 Roles requiring separation of duties

Comfact maintains a policy outlining the rigorous control procedure and separation of duty criteria. The complete, detailed documentation of all roles and what duties are separated can be found in Comfact CA Operational Policy.

Examples of duties requiring separation includes, but are not limited to:

- HSM operations affecting private keys (e.g., creation, deletion, and backups) are separated from the HSM Administrator role to include a Systems Administrator role.
- Approving new access control is separated from the Systems Administration role, and auditing is separated from the System operation role.

8.3 Personnel controls

Personnel controls are outlined in the relevant information security policy which is communicated with all employees impacted by it. However, considering the classified nature of the information security policy, only the following excerpts are elaborated on.

8.3.1 Qualifications, experience, and clearance requirements

All employees holding a trusted role (see section 8.2.1) at Comfact shall sign a confidentiality (non-disclosure) agreement. Personnel that hold or is employed for a trusted role shall possess qualification, expert knowledge and experience obtained through training and/or attained from practice for the particular role. Upon applying for a trusted role, the person must present proof of the requisite qualifications and experiences needed to perform the tasks. Note that the assignment of a trusted role falls upon Management Team.

The job description of trusted roles (both temporary and permanent) and their responsibilities are clearly defined in which must first be accepted and signed by the person being assigned a trusted role. The job description includes the required skills and experiences, but also specific functions on segregation of duties and policies on least privilege, access levels, procedure on background screening, as well as training and awareness.

8.3.2 Background check procedures

Prior to being employed under a trusted role, Comfact conducts a background interview. The background interview can be repeated for personnel holding a trusted role. The background interview includes the following:

- Check previous employment and other professional references,
- Check of criminal records, and
- Check of credit and financial records.

Background interviews are reviewed by human resources (HR) and security personnel, who will determine the appropriateness of the employment. Background interviews containing undesirable reports (e.g., certain criminal records, indications of financial problems, and unfavorable or misrepresented references) maybe lead to cancellation of employment offers, termination of existing trusted roles or employment.

8.3.3 Training requirements

Upon employment, Comfact provides all personnel with training that cover awareness and skills on the following topics:

- Security policies and procedures, and data protection rules
- Incident handling, disaster recovery, business continuity procedures
- Basic Public Key Infrastructure (PKI)
- Basic security threat identification, e.g., phishing and social engineering
- For managerial personnel and personnel with security responsibilities, basic risk assessment sufficient to carry out management functions

In addition, training is given for responsibilities and duties the person is expected to perform, and personnel is expected to keep up to date with industry-relevant best practice by attending e.g., conferences and seminar on work related topics and practices. Information on security updates, relevant threats, and vulnerabilities are discussed and reviewed on a biweekly basis, and security updates on training and practices at least every year (12 months).

8.3.4 Retaining frequency and requirements

Retraining is frequented to the extent that ensures personnel maintains proficiency to perform their job duties and responsibilities.

8.3.5 Job rotation frequency and sequence

No stipulation.

8.3.6 Sanctions for unauthorized actions

Failure to comply with this CPS, security policies and practices, by any personnel holding a trusted role, will result in appropriate disciplinary and administrative actions by HR. The trusted role will be suspended whilst pending management review.

8.3.7 Independent contractor requirements

Independent contractors may, in certain circumstances, be used to fill trusted positions, abiding the same criteria and security requirements as would any other employee holding a trusted role.

Independent contractor or consultant that have yet to complete the background check (as outlined in section 8.3.2) may only enter Comfact secure facilities if escorted and directly supervised by personnel already holding a trusted role.

8.3.8 Documentation supplied to personnel

Personnel involved in any capacity with Comfact Certificate Services CA operations shall be made aware of the requirements of applicable CP and CPS, as well as any other relevant documentation,

such as policies, processes, and procedures, needed to maintain the integrity of Comfact Certificate Services CA and perform their duties satisfactorily.

8.4 Audit logging procedures

Audit logs are automatically created on Comfact Certificate Service's systems relating to their security and services. Where possible, these logs are collected electronically, otherwise kept in digital form on respective system or physically, on paper (e.g., logbooks).

8.4.1 Types of events recorded

Comfact Certificate Services automatically, or manually, logs the following events relating to critical systems:

System	Information logged

CA related systems (i.e., certificate lifecycle operations)	• Attempts to access the system,
	• Revocation requests made to the system,
	• Registration information, including:
	  ○ Types of documents present,
	  ○ Unique identification data (e.g., application or persons identity)
	  ○ Information about related documents (e.g., agreements)
	  ○ Identity of the entity accepting the application, and
	  ○ Means of identity validation.
	• Reocation information, including:
	  ○ Information about the certificate requested to be revoked,
	  ○ Identity of the entity requesting revocation,
	  ○ Means of identity validation.
	• All events relating to the life cycle of keys, including: issuance, usage, and removal.
	• Certificate applications, renewal, re-keying, and revocation,
	• Successful and failed processing of requests,
	• Changes to certificate issuance policies
	• Generated CRLs and OCSP responses, and
	• Issued certificates, including date and time of issuance.

Logical controls (i.e., software related security systems)	• System events (e.g., crashes or errors), • System start-up, shutdown, and crashes (software or hardware related), • Clock synchronization events • Firewall activities, • Router activities, and • Backups and archival.
Physical controls	• Entries and exists to/from the CA facility.

8.4.2 Frequency of processing log

Security logs are reviewed upon alerts based on anomalies, warnings, and errors within respective system. Reviews of audit logs are conducted by trusted Comfact Certificate Services System Administrators, as described in section 8.2.1. During an audit log review, all recorded critical events (e.g., anomalies, warnings, and errors) shall be investigated and their cause reported. All actions taken in response to the audit log review shall be documented. Archival of logs are carried out on a biweekly basis.

8.4.3 Retention period for audit log

Records concerning Comfact Certificate Services CA certificates are held of a period of two (2) years or longer if required by local laws and regulations.

8.4.4 Protection of audit log

The confidentiality of audit logs is protected through logical and physical role-based access controls. Only trusted Comfact Certificate Services System Administrator shall have access to system audit logs. The integrity of the logs is protected with the use of digital timestamps.

8.4.5 Audit log backup procedures

Daly (every 24 hours), incremental backups of audit logs shall be performed, and a full backup weekly (every 7 days). All backups are kept separate from the system being backed up and protected to the same degree as the original logs.

8.4.6 Audit collection system (internal vs. external)

Automated audit logs are generated and collected at the network, application, and operating system level. While physical, manual audit logs (e.g., entries and exists to / from the CA facility) are recorded by authorized personnel only.

8.4.7 Notification to event-causing subject

No stipulation.

8.4.8 Vulnerability assessments

In addition to actions taken in section 8.4.2, physical, logical, and administrative vulnerability assessments are part of the information security management system, and performed regularly (e.g., via automated vulnerability scanning). Vulnerabilities are analyzed, evaluated, and mitigated in accordance with the routines set up for managing security risks. However, due to security reasons, these routines are not publicly disclosed herein.

8.5 Records archival

Comfact Certificate Services archives sufficient details to show that a certificate was issued in accordance with its CPS. All archived records are stored in so that they cannot be easily deleted or destroyed, e.g., off-site backup and by parallel storage, see 8.5.3-8.5.5.

8.5.1 Types of records archived

In addition to the information outlined in section 8.4.1, Comfact Certificate Services also archives:

- The public repository material, as outlined in section 5.2,
- The CA system (the installed and configured software) constituting Comfact Certificate Services PKI, and
- Configurations related to IT equipment (e.g., firewall, switches, and databases).

8.5.2 Retention period for archive

Comfact Certificate Services will retain archived data for at least seven (7) years, unless longer period is required by local law, standard, or regulations.

8.5.3 Protection of archive

Archived data are stored separate to the system whose data is being archived, with the same level of security as the original data had. Archives in physical form (e.g., paper and logbooks) are retained in a safe area which only authorized personnel can access.

8.5.4 Archive backup procedures

Archived data is stored on systems which are backed up to separate systems on a daily (24 hours) basis, keeping the same level of security as the original data.

8.5.5 Requirements for time-stamping of records

All records (e.g., certificates, CRLs, and critical database entries) shall be time stamped using the system time. The system time of the service is synchronized with ±1 second of UTC, or better, by calibration with multiple independent time sources.

8.5.6 Archive collection system (internal or external)

Comfact Certificate Services use internal archive systems and servers for archiving information.

8.5.7 Procedure to obtain and verify archive information

Comfact Certificate Services verify the integrity of backups and archived information is verified upon restoration. Only authorized personnel shall have access to backups and archives.

8.6 Key changeover

CA keys generated by Comfact Certificate Services are retired at the end of their associated certificate's maximum lifetime, as defined in section 9.3.2. Three months before retirement, new CA key pairs shall be issued for continued supported services, and enters a staging period of maximum 24-hours. The process follows the recommendations as outlined in RFC 6489.

8.7 Compromise and disaster recovery

8.7.1 Incident and compromise handling procedures

Comfact Certificate Services has implemented a redundant CA system and related IT environment, located at a separate, geographically different location, configured to automatically sync relevant data, and assume operation on failover in case of a disaster, incident at the primary site, or high availability.

Comfact Incident Response and Disaster Recovery procedures are outlined in documents that fall under a different classification level than this CPS, further details are therefore not disclosed herein.

8.7.2 Computing resources, software, and/or data are corrupted

Comfact Certificate Services CA systems are backed up on a daily basis, and keys made on security modules (except keys for short-lived, end-entity certificates issued to a natural person which keys are generated by Comfact Certificate Services HSMs, since they deleted directly after use) are backed up upon creation and duplicated at security modules at Comfact Certificate Services mirror site. In addition, backups of CA keys are kept off-site in a secure location. In the event of a disaster, Comfact Certificate Services mirror site will take over operation. Should the data synchronized between the two sites be corrupt, relevant data can be restored from the off-site system backups. Meanwhile, the primary site can be restored, either by new system setup or on replacement hardware.

8.7.3 Entity private key compromise procedures

Should a CA private key be compromised, corrupt, or lost, Comfact Certificate Service's personnel shall follow an investigation, as outlined in the internal incident response procedure, resulting in a report detailing the event, cause of compromise, and recommended actions to take to prevent future, similar occurrences. After which, the associated CA-certificate will be revoked and an emergency re-keying of the affected CA will take place, affected Subscribers and Relying Parties will be informed, and the new certificates distributed in accordance with section 9.1.3.

In summary, on suspicion that Comfact Certificate Services does no longer have full and exclusive control of a CA's private key, the following actions are taken:

- Collect information related to the incident,

- Revoke the certificate associated with the CA private key, and
- Inform all affected Subscribers of the CA key compromise, and where the new CA certificate can be obtained. Relying Parties is outside of Comfact influence, but are informed about the compromise through the revocation information.

8.7.4 Business continuity capabilities after a disaster

Comfact Certificate Services mission critical systems are implemented with redundancy, in terms of hardware, software, and configurations, distributed over two geographically separate data centers. In addition, Comfact is prepared for business continuity in a Disaster Recovery Plan procedure, which outlines the steps to be taken in case of e.g., computing resources, software, or data failure/corruption.

Procedures for routine backups of critical CA information (e.g., CA-key pairs, issuance logs, audit logs, and database records) are maintained offsite. Private keys are backed up in an encrypted format with the same level of security as its primary location of operation.

8.8 CA or RA termination

In the event of Comfact Certificate Services CA or a Subscriber's CA cease to operate, Comfact shall inform Subscribers, Relying Parties, and other (affected) entities, within reasonably affordable means, about the termination. Prior to the termination, Comfact Certificate Services shall therefore publish a notification on the matter online, no less than one (1) year in advance.

Prior to the termination, Comfact will proceed with the following steps:

- Inform Subscribers, Relying Parties, other (affected) entities Comfact has contracted CA services with, as well as relevant authorities, about the termination, at least three months before termination,
- The CA keys ceases to issue any new certificates or other trusted tokens,
- Where applicable, Comfact Certificate Services may transfer the repository of public keys and handling of the revocation status for unexpired certificates that have been issued to a reliable third party,
- At the end of the one (1) year notice period, all issued certificates are revoked, all CA keys and backups thereof are destroyed, and further revocation issuance ceases to function, and
- All critical data, e.g., registration information, revocation status information, archived information and logs (see section 8.4.1), are kept during the archival period, and then destroyed in a secure manner. Comfact Certificate Services may transfer this information to be retained by a reliable third party.

9 Technical security controls

9.1 Key pair generation and installation

9.1.1 Key pair generation

Comfact Certificate Services follow recommendations as described in ETSI TS 119 312. CA keys issued by Comfact Certificate Services are generated in a security module (e.g., HSM or Smart Card) certified to at least NIST FIPS 140-2 level 3. Security modules maintained by Comfact are physically protected as per section 8.1.

The following table outlines the key generation practices for each issuing CA:

Issuing CA	Key-pair Generation
Comfact Root CA G1	After an approved certificate application, the CA system generates either a self-issued root, or a new intermediate (subordinate) CA key-pair and associated certificate. Multiple (n=2) trusted personnel of Comfact Certificate Services are required to generate the new CA keys and create the public key certificate in the CA system. The ceremony process is documented and follows a predefined

	script and under control by two (2) System Administrators (see section 8.2.1, and witnessed by several people, at least two of which are impartial. The generation of a new CA key-pair is followed by the generation of a shared secret to manage it. The key ceremony script and procedure for generating the new CA keys and creating shared secret is described in an internal document and contains details regarding: • Number and types of roles required to be participating in the ceremony, • Functions to be performed by each of the aforementioned roles and in what phase of the ceremony, • Responsibilities during and after the ceremony, and • Required documentation and evidence to be collected during the ceremony. All steps of the ceremony are video recorded and the details (as listed above) are collected as evidence, resulting in a report that is signed by everyone present during the ceremony.
Comfact Signature CA G1	Short-lived, end-entity keys issued to a natural person, that are generated on Comfact Certificate Services HSMs on demand from the auto-RA function, never leaves the HSM. For key-pairs that are not generated by Comfact Certificate Services HSMs, a secure cryptographic device (e.g., smart card) is used. An existing smart card can be used, but all local keys will be re-generated. The user activation data (e.g., PIN) is then securely prepared or distributed separately from the secure cryptographic device (e.g., set by the Subject themselves on site, or sent via certified postal mail).
Comfact Seal CA G1	Short-lived, end-entity keys issued to a legal person are generated on request and can be hosted and maintained by Comfact Certificate Services HSM or on the Subscriber/Subjects own security module. For key-pairs that are not hosted and maintained by Comfact Certificate Services a secure cryptographic device (e.g., smart card) is used. An existing smart card can be used, but all local keys will be re-generated. The user activation data (e.g., PIN) is then securely prepared or distributed separately from the secure cryptographic device (e.g., set by the Subject themselves on site, or sent via certified postal mail).
Comfact Services CA G1	Short-lived, end-entity keys issued to a Comfact AB owned service are generated on request and are hosted and maintained by Comfact Certificate Services HSM.

9.1.2 Private key delivery to Subscribers

End-user's private keys not generated by Comfact Certificate Services HSMs (i.e., by the use of a personal smart card) are generated and delivered to the Subject (the end-user) physically at Comfact after successfully having validated the natural or legal person's identity. Upon initializing the new smart card, the Subject sets the PIN to control the locally generated key. A receipt shall then be signed upon delivery of the newly created smart card.

9.1.3 Public key delivery to certificate issuer

The following table outlines how the public key is distributed:

Issuing CA	Public Key Distribution
Comfact Root CA G1	Public keys are made publicly available through the digital certificates published on Comfact Certificate Services repository website, see section 5.2.
Comfact Signature CA G1	The Subjects public keys are provided through the digital certificate included in the signed data provided by the Subscribers requesting system. In the case of the key being provided on a smart card, the Subjects public key is delivered with the private key on the used smart card. The public key can also be delivered via a removable media or other means (e.g., a USB-thumb drive or email) in accordance with existing agreements.
Comfact Seal CA G1	The Subjects public keys are delivered with the private key on the used smart card. The public key can also be delivered via a removable media or other means (e.g., a USB-thumb drive or email) in accordance with existing agreements.
Comfact Services CA G1	The service's public keys are delivered to the internal service thought manual installation of the certificate.

9.1.4 CA public key delivery to Relying Parties

Comfact Certificate Services provide CA public keys to Relying Parties through the use of the publicly available PKI repository (see section 5.2), in the form of a digital certificate (X.509 v3).

9.1.5 Key sizes

Comfact Certificate Services follow recommendations as described in ETSI TS 119 312. As such, the following key-sizes are used:

RSA Based Keys	ECDSA Based Keys
The following key-sizes are used for RSA based keys: a) Root keys are generated with RSA using a minimum length of 4096 bits with Secure Hash Algorithm 2 of 256 bits (SHA-256), b) End-entity keys are generated with RSA using a minimum length of 2048 or 3072 bits with Secure Hash Algorithm 2 of 256 bits (SHA-256). Note: all certificates that are set to expire after first of January 2025 must have a key-size of at least 3072 bits for RSA.	The following key-sizes are used for ECDSA based keys (generated with NIST P-curves): a) Intermediate CA keys are generated with ECDSA using a curve size of 256 bits with Secure Hash Algorithm 2 of 256 bits (SHA-256), b) End-entity keys are generated with ECDSA using a curve size of 256 bits with Secure Hash Algorithm 2 of 256 bits (SHA-256).

9.1.6 Public key parameters generation and quality checking

All keys are generated using True Random Number Generator (TRNG acc. AIS31 class PTG.2) that meet the required level of testing and certifying under FIPS 140-2 level 3.

Personnel at Comfact Certificate Services are required to keep up to date with the development within cryptography and adjust the recommended algorithms and keys sizes accordingly.

9.1.7 Key usage purposes (as per X.509 v3 key usage field)

Certificates issued by Comfact Certificate Services includes the key usage field to define suitable areas of application for the cryptographic key and associated certificate. Note that Comfact Signature Services and Comfact Certificate Services are not responsible for how end-entity keys are used, other than assigning the key usage field within the certificate to define its intended purposes:

a) Root certificates include the following key usage “keyCertSign” and “cRLSign”,
b) Intermediate CA certificates include the following key usage “keyCertSign” and “cRLSign”,
c) End-entity certificates include the following key usage “nonRepudiation”.

9.2 Private key protection and cryptographic module engineering Controls

9.2.1 Cryptographic module standards and controls

Comfact Certificate Services use hardware security modules (HSM), certified to FIPS 140-2 level 3, to protect all private keys hosted and retained by Comfact.

Keys stored by Subscribers and Subjects outside of Comfact Certificate Services must be stored on a secure cryptographic module (e.g., Smart Card) certified by at least FIPS 140-2 level 3.

9.2.2 Private key (n out of m) multi-person control

See section 8.2.2.

9.2.3 Private key escrow

No stipulation, i.e., Comfact Certificate Services shall not escrow its private keys.

9.2.4 Private key backup

Private keys are routinely backed up in an encrypted format with the same level of security as its primary location of operation, for disaster recovery purposes. Backed up keys that resides outside of their primary location (i.e., the hardware security module) is always in an encrypted format and stored on a secure token, e.g., Smart Card. The backup routine itself as well as the re-activation of the backups are protected using a multi-person control (n-out-of-m), as described in section 8.2.2.

Offline CA keys are kept as offsite key backups, and restored only temporarily when needed (e.g., to sign a new intermediate CA certificate or CARL). However, note that no backups are made of short-lived, end-entity keys, e.g., Subscribers’ private digital signature keys.

9.2.5 Private key archival

Comfact Certificate Services will archive CA private keys for disaster recovery purposes, but does not archive subscribers’ private keys.

9.2.6 Private key transfer into- or from a cryptographic module

The hardware security modules (HSM) used by Comfact Certificate Services can be configured to allow for keys to be duplicated between modules. The duplication is in the form of restoring a backup, and the private keys are always in an encrypted format when outside an HSM (as described in section 9.2.4). Note that the backup routine itself as well as the re-activation of the backups onto the HSM are protected using a multi-person control (n-out-of-m), as described in section 8.2.2.

9.2.7 Private key storage on cryptographic module

Comfact Certificate Service’s private keys are stored on a cryptographic module which has been evaluated and certified to at least FIPS 140-2 level 3.

Subscribers private key that are not maintained by Comfact Certificate Services are stored as described in section 9.2.1.

9.2.8 Method of activating private key

Private keys generated and maintained by Comfact Certificate Services are activated by a set of security tokens, e.g., smart cards, assigned to selected trusted role personnel. The activation procedure of private keys is protected by multi-person control (n-out-of-m), as described in section 8.2.2.

Comfact Certificate Services maintains no involvement in the protection of private keys maintained by Subscribers.

9.2.9 Method of deactivating private key

The private key is deactivated using the inbuilt deactivation function as specified by the hardware security module manufacture. The deactivation procedure of private keys is protected by multi-person control (n-out-of-m), as described in section 8.2.2.

9.2.10 Method of destroying private key

Private keys are destroyed on the hardware security modules using the inbuilt delete function within the module. The deletion procedure of private keys is protected by multi-person control (n-out-of-m), as described in section 8.2.2. Backups of private keys are destroyed by zeroing its content by performing three (3) consecutive failed login attempts.

The destruction process is documented, along with how the process was carried out and who witnessed it.

9.2.11 Cryptographic module rating

See section 9.2.1.

9.3 Other aspects of key pair management

9.3.1 Public key archival

Comfact Certificate Services retains a copy of all Public Keys and corresponding certificate for archival. These archived keys and certificates are maintained for at least one (1) year after expiration of the certificate.

9.3.2 Certificate operational periods and key pair usage periods

The maximum operational period for Comfact Certificate Service's certificates is based on the type (see table below). Comfact Certificate Services rely on a two-tier hierarchy, where each issued certificate has a maximum life time half that of its parent.

Type	In Use Issuing Certificates	Certificate Terminated
Root CA	10 years	20 years
Intermediate CA	8 years	10 years
End-Entity	No stipulation.	2 years

Note that CA keys are only used for 10 and 8 years respectively for issuing new certificates, but expire first after 20 and 10 years in order to revoke subordinate certificates throughout its full lifetime. By the time the lifetime has passed, the certificates are re-keyed following the key changeover process as described in section 8.6.

9.4 Activation data

9.4.1 Activation data generation and installation

Comfact Certificate Services uses a set of Smart Card-based authentication tokens required to operate private keys and the cryptographic modules (i.e., activate the hardware security module).

9.4.2 Activation data protection

Activation data for the hardware security modules (HSM) are protected on secure authentication tokens, e.g., Smart Cards, which are held under separate, role-based physical control. The authentication tokens are themselves protected with a PIN-code, chosen by the trusted personnel in control of it.

9.4.3 Other aspects of activation data

No stipulation.

9.5 Computer security controls

9.5.1 Specific computer security technical requirements

Comfact Certificate Services facilitates are physically secured as described in section 8. Both logical and physical security controls are put in place to separate and only allow certain roles (as per section 8.2) and individuals access, after authentication in accordance with section 8.2.3. As such, access to any of Comfact Certificate Services production systems are on an individual level, where access (physical as well as logical) is logged. Examples of when access to the production systems is required include updates of software, starting or stopping services and applications, and similar maintenance. In addition, the production network is logically separated from other networks and components.

9.5.2 Computer security rating

No stipulation.

9.6 Life cycle security controls

9.6.1 System development controls

For Comfact Certificate Services CA systems, the following development controls shall be followed to minimize unstable or insecure production systems and environments:

- Any logical, physical, or administrative changes must be planned, documented, and approved by at least one Senior Administrator (e.g., Operations Manager, PKI administrator, or System Administrator), but cannot be the same person who submitted the request,
- All changes to Comfact Certificate Services production systems (e.g., the CA-system), must be extensively tested in its separate development and test environment before put into production,
- Third-party components are selected based on market reputation, quality and ability to deliver (e.g., service level agreements), and likelihood of their continuous business, and
- All software developed by Comfact verifies, upon loading, that it or used libraries and assemblies have not been modified by only using strong-named components.

9.6.2 Security management controls

Security risks towards Comfact Certificate Services production environment is continuously assessed and evaluated through an established risk management process. Anomalies to systems (e.g., access controls) or networking (e.g., firewalls or routers) as well as reporting of relevant weaknesses and threats (e.g., entries in common vulnerabilities and exposures databases) which are then assessed to determine their likelihood and impact to potentially vulnerable systems.

9.6.3 Life cycle security controls

Design requirements and future developments of systems or storage undergoes a risk analysis before being put into action. Any changes are documented and follows procedure for change control to monitor and log releases and modifications, but also emergency software fixes.

Systems within Comfact Certificate Services are protected against viruses and other malicious software by employing anti-malware. Security patching are typically applied as circumstances require to ensure they do not introduce additional vulnerabilities or instabilities that otherwise outweigh the benefit of applying them. The patching of the system is documented.

9.7 Network security controls

Comfact Certificate Services production environment is on a separate network with a firewall implemented to limit the type of communication between client and servers to what is strictly required. Communication outside of the local, restricted network is encrypted (e.g., by the use of TLS) for VPN and HTTPS. Unused network ports, accounts, applications, services and protocols are disabled as default, and only system that requires access to Internet services are allowed such connections to be established.

The network layout is designed after a risk assessment that considered logical and physical security considerations, and have segmented the network accordingly to isolate critical and sensitive systems.

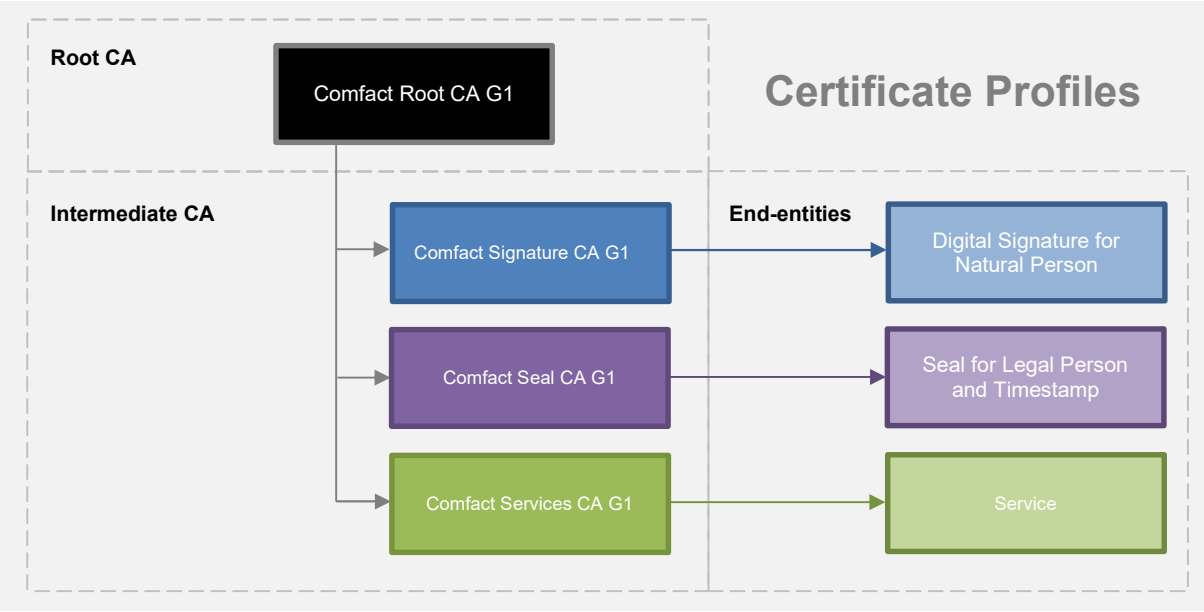
9.8 Timestamping

Systems time used by Comfact Certificate Services are synchronized with ±1 second of UTC, or better, by calibration with multiple independent time sources. These include e.g., Meinberg LANTIME M300/GPS and local NTP servers with external time authorities.

10 Certificate, CRL, and OCSP profiles

10.1 Certificate profile

Certificates and CRLs issued by Comfact Certificate Services are in conformance with RFC 5280, with the additional clarifications as outlined in this chapter.



Note: serial numbers for all certificates issued by Comfact Certificate Services consist of a non-sequential, non-negative integer that is between 64-160 bit long. Hereinafter simply referred to as “unique serial number”.

10.1.1 Profile of Root CA Certificate: Comfact Root CA G1

10.1.1.1 Basic Fields

Field	Value
Version	3 certificates (i.e., integer value 2).
Serial Number	Unique serial number
Signature	RSASSA-PSS 4096 bit with SHA256
Validity	See section 9.3.2
Subject Public Key Info	RSA 4096 bit
Issuer DN	– CN = Comfact Root CA G1 – OU = Certificate Service – O = Comfact AB – C = SE
Subject DN	– CN = Comfact Root CA G1 – OU = Certificate Service – O = Comfact AB – C = SE

10.1.1.2 Extensions

Extension	Critical	Value
Subject key identifier	No	Comfact Root CA G1 public key identifier
Certificate Policies	No	policyIdentifier is set to the OID referring to this CPS and the public address to the repository, as described in sections 4.2 and 5.1 respectively
Basic Constraints	Yes	cA = TRUE
Key Usage	Yes	For CA certificates the following flags are set: – Key certificate signing (keyCertSign), – CRL signing (cRLSign)

10.1.2 Profile of Intermediate CA Certificate: Comfact Signature CA G1

10.1.2.1 Basic fields

Field	Value
Version	3 certificates (i.e., integer value 2).
Serial Number	Unique serial number
Signature	RSASSA-PSS 4096 bit with SHA256
Validity	See section 9.3.2
Subject Public Key Info	ECDSA 256 bit
Issuer DN	– CN = Comfact Root CA G1 – OU = Certificate Services

	– O = Comfact AB – C = SE
Subject DN	– CN = Comfact Signature CA G1 – OU = Certificate Services – OI = 5563426666 – O = Comfact AB – C = SE

10.1.2.2 Extensions

Extension	Critical	Value
Authority key identifier	No	Comfact Root CA G1 public key identifier
Subject key identifier	No	Comfact Signature CA G1 public key identifier
Certificate Policies	No	policyIdentifier is set to the OID referring to this CPS and the public address to the repository, as described in sections 4.2 and 5.1 respectively
Authority Information Access	No	Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.comfact.com/certificates/comfact-root-ca-g1.cer
CRL Distribution Points	No	The location of where the CRL is available is indicated in this extension. The relevant addresses are described in section 5.2
Basic Constraints	Yes	cA = TRUE pathLenghtConstraint = 0
Key Usage	Yes	For intermediate CA certificates the following flags are set: – Key certificate signing (keyCertSign), – CRL signing (cRLSign)

10.1.3 Profile of Intermediate CA Certificate: Comfact Seal CA G1

10.1.3.1 Basic fields

Field	Value
Version	3 certificates (i.e., integer value 2).
Serial Number	Unique serial number
Signature	RSASSA-PSS 4096 bit with SHA256
Validity	See section 9.3.2
Subject Public Key Info	RSA 4096 bit
Issuer DN	– CN = Comfact Root CA G1 – OU = Certificate Services – O = Comfact AB – C = SE

Subject DN	– CN = Comfact Seal CA G1 – OU = Certificate Services – OI = 5563426666 – O = Comfact AB – C = SE

10.1.3.2 Extensions

Extension	Critical	Value
Authority key identifier	No	Comfact Root CA G1 public key identifier
Subject key identifier	No	Comfact Seal CA G1 public key identifier
Certificate Policies	No	policyIdentifier is set to the OID referring to this CPS and the public address to the repository, as described in sections 4.2 and 5.1 respectively
Authority Information Access	No	Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.comfact.com/certificates/comfact-root-ca-g1.cer
CRL Distribution Points	No	The location of where the CRL is available is indicated in this extension. The relevant addresses are described in section 5.2
Basic Constraints	Yes	cA = TRUE pathLenghtConstraint = 0
Key Usage	Yes	For intermediate CA certificates the following flags are set: – Key certificate signing (keyCertSign), – CRL signing (cRLSign)

10.1.4 Profile of Intermediate CA Certificate: Comfact Services CA G1

10.1.4.1 Basic fields

Field	Value
Version	3 certificates (i.e., integer value 2).
Serial Number	Unique serial number
Signature	RSASSA-PSS 4096 bit with SHA256
Validity	See section 9.3.2
Subject Public Key Info	RSA 4096 bit
Issuer DN	– CN = Comfact Root CA G1 – OU = Certificate Services – O = Comfact AB – C = SE
Subject DN	– CN = Comfact Services CA G1 – OU = Certificate Services

	– OI = 5563426666 – O = Comfact AB – C = SE

10.1.4.2 Extensions

Extension	Critical	Value
Authority key identifier	No	Comfact Root CA G1 public key identifier
Subject key identifier	No	Comfact Seal CA G1 public key identifier
Certificate Policies	No	policyIdentifier is set to the OID referring to this CPS and the public address to the repository, as described in sections 4.2 and 5.1 respectively
Authority Information Access	No	Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.comfact.com/certificates/comfact-root-ca-g1.cer
CRL Distribution Points	No	The location of where the CRL is available is indicated in this extension. The relevant addresses are described in section 5.2
Basic Constraints	Yes	cA = TRUE pathLenghtConstraint = 0
Key Usage	Yes	For intermediate CA certificates the following flags are set: – Key certificate signing (keyCertSign), – CRL signing (cRLSign)

10.1.5 Profile of End-entity certificate: Digital Signature for Natural Person

10.1.5.1 Basic fields

Field	Value
Version	3 certificates (i.e., integer value 2).
Serial Number	Unique serial number
Signature	RSASSA-PSS 4096 bit with SHA256
Validity	See section 9.3.2
Subject Public Key Info	The end-entity public key can be one of the following: – ECDSA 256 bit, or – RSA 2048 or 3072 bit See section 9.1.5
Issuer DN	– CN = Comfact Signature CA G1 – OU = Certificate Services – OI = 5563426666 – O = Comfact AB

	– C = SE
Subject DN	The identity of a natural person contains at minimum the following attributes: – CN = First name and surname, – C = Country where the Subject is officially registered, – givenName = First name, – SN = Surname But may also include the following attributes: – serialNumber = unique identifier, e.g., an identifier assigned by a government or civil authority, – dateOfBirth = Specifies the date of birth of the person.

10.1.5.2 Extensions

Extension	Critical	Value
Authority key identifier	No	Comfact Signature CA G1 public key identifier
Subject key identifier	No	Public key identifier of the Subject
Certificate Policies	No	policyIdentifier is set to the OID referring to this CPS and the public address to the repository, as described in sections 4.2 and 5.1 respectively
Authority Information Access	No	Access Method = Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL = http://pki.comfact.com/ocsp/comfact-signature-ca-g1 Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.comfact.com/certificates/comfact-signature-ca-g1.cer
CRL Distribution Points	No	The location of where the CRL is available is indicated in this extension. The relevant addresses are described in section 5.2
Basic Constraints	No	cA = FALSE
Key Usage	Yes	For end-entity certificates, the following flag is set: – Non repudiation (nonRepudiation)
Extended Key Usage	No	End-entity certificates key usage may be further refined to include the following key usage: – “MS Document Signing”

10.1.6 Profile of End-Entity Certificate: Comfact Time Stamping Authority

10.1.6.1 Basic fields

Field	Value
Version	3 certificates (i.e., integer value 2).

Serial Number	Unique serial number
Signature	RSASSA-PSS 4096 bit with SHA256
Validity	See section 9.3.2
Subject Public Key Info	The end-entity public key can be one of the following: – ECDSA 256 bit, or – RSA 2048 or 3072 bit See section 9.1.5
Issuer DN	– CN = Comfact Seal CA G1 – OU = Certificate Services – OI = 5563426666 – O = Comfact AB – C = SE
Subject DN	The identity of a natural person contains the following attributes: – CN = A name commonly used by the subject to represent itself, – C = Country where the Subject (legal person) is established, – O = Full registered name of the subject (legal person), – OI = Identification of the subject organization

10.1.6.2 Extensions

Extension	Critical	Value
Authority key identifier	No	Comfact Seal CA G1 public key identifier
Subject key identifier	No	Public key identifier of the Subject
Certificate Policies	No	policyIdentifier is set to the OID referring to this CPS and the public address to the repository, as described in sections 4.2 and 5.1 respectively
Authority Information Access	No	Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.comfact.com/certificates/comfact-seal-ca-g1.cer
CRL Distribution Points	No	The location of where the CRL is available is indicated in this extension. The relevant addresses are described in section 5.2
Basic Constraints	No	cA = FALSE
Key Usage	Yes	For end-entity certificates, the following flag is set: – Digital signature (digitalSignature)
Extended Key Usage	Yes	End-entity certificates key usage is further refined to include the following key usage: – id-kp-timeStamping

Profile of End-entity certificate: Seal for Legal Person

10.1.6.3 Basic fields

Field	Value
Version	3 certificates (i.e., integer value 2).
Serial Number	Unique serial number
Signature	RSASSA-PSS 4096 bit with SHA256
Validity	See section 9.3.2
Subject Public Key Info	The end-entity public key can be one of the following: – ECDSA 256 bit, or – RSA 2048 or 3072 bit See section 9.1.5
Issuer DN	– CN = Comfact Seal CA G1 – OU = Certificate Services – O = Comfact AB – C = SE
Subject DN	The identity of a natural person contains the following attributes: – CN = A name commonly used by the subject to represent itself, – C = Country where the Subject (legal person) is established, – O = Full registered name of the subject (legal person), – OI = Identification of the subject organization

10.1.6.4 Extensions

Extension	Critical	Value
Authority key identifier	No	Comfact Seal CA G1 public key identifier
Subject key identifier	No	Public key identifier of the Subject
Certificate Policies	No	policyIdentifier is set to the OID referring to this CPS and the public address to the repository, as described in sections 4.2 and 5.1 respectively
Authority Information Access	No	Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.comfact.com/certificates/comfact-seal-ca-g1.cer
CRL Distribution Points	No	The location of where the CRL is available is indicated in this extension. The relevant addresses are described in section 5.2
Basic Constraints	No	cA = FALSE
Key Usage	Yes	For end-entity certificates, the following flag is set:

		– Non repudiation (nonRepudiation)
Extended Key Usage	No	End-entity certificates key usage may be further refined to include the following key usage: – "MS Document Signing"

10.1.7 Profile of End-Entity Certificate: Comfact [Service]

10.1.7.1 Basic fields

Field	Value
Version	3 certificates (i.e., integer value 2).
Serial Number	Unique serial number
Signature	RSASSA-PSS 4096 bit with SHA256
Validity	See section 9.3.2
Subject Public Key Info	The end-entity public key can be one of the following: – ECDSA 256 bit, or – RSA 2048 or 3072 bit See section 9.1.5
Issuer DN	– CN = Comfact Services CA G1 – OU = Certificate Services – OI = 5563426666 – O = Comfact AB – C = SE
Subject DN	The identity of a natural person contains the following attributes: – CN = A name commonly used by the service to represent itself, – C = Country where the service is established, – O = Full registered name of the service owner, – OI = Identification of the service organization

10.1.7.2 Extensions

Extension	Critical	Value
Authority key identifier	No	Comfact Services CA G1 public key identifier
Subject key identifier	No	Public key identifier of the service
Certificate Policies	No	policyIdentifier is set to the OID referring to this CPS and the public address to the repository, as described in sections 4.2 and 5.1 respectively
Authority Information Access	No	Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://pki.comfact.com/certificates/comfact-services-ca-g1.cer

CRL Distribution Points	No	The location of where the CRL is available is indicated in this extension. The relevant addresses are described in section 5.2
Basic Constraints	No	cA = FALSE
Key Usage	Yes	For end-entity certificates, the following flags may be set: – Digital signature (digitalSignature), – Key encipherment (keyEncipherment), – Key agreement (keyAgreement)

Version number(s)

Comfact Certificate Services issues X.509 version 3 certificates (i.e., integer value 2).

10.1.8 Certificate extensions

The following tables describe the extensions used in certificates issued by Comfact Certificate Services.

Extension	Critical	Description	In Root CA
Authority key identifier	No	The identity of the CAs public key is indicated in this extension though a SHA-256 hash of the key.	Yes
Subject Key Identifier	No	The identity of the Subjects public key is indicated in this extension through a SHA-256 hash of the key.	Yes
Certificate Policies	No	The certificate policy by which the certificate has been issued is indicated in this extension along with the public repository address. The OID covering this CPS and the public repository is described in section 4.2.	No
Key Usage	Yes	The intended key usage is indicated in this extension. For CA certificates the following flags are set: – Key certificate signing (keyCertSign), – CRL signing (cRLSign) For end-entity signature certificates (natural and legal person), the following flag is set: – Non repudiation (nonRepudiation) For end-entity timestamping certificates, the following flag is be set: – Digital signature (digitalSignature) For end-entity certificates used for Comfact Services, the following flag is be set: – Digital signature (digitalSignature) – Key encipherment (keyEncipherment)	Yes
CRL Distribution Points	No	– The location of where the CRL is available is indicated in this extension.	No

		The relevant addresses are described in section 5.2.	
Basic Constraints	Yes	The extension indicates if the certificate is a CA certificate, and is therefore set to “true” in all CA certificates. The “pathLenConstraints” field of this extension indicate the maximum number of CA certificates following in a certification path. As such, root CAs have a value of “none” to indicate no restrictions of subordinate CAs path length. While CAs’ that only issues end-entity certificates have a “pathLenghtConstraints” set to a value of “0”.	Yes
Authority Information Access	No	The information in this extension indicates where the issuing CA certificate is available. For short-lived, end-entity signature certificates, the address to the OCSP location is included.	No
Extended Key Usage	Yes/No	End-entity certificate’s key usage may be further refined to either include the following two mutually exclusive extended key usages: – “MS Document Signing” whereupon this extension shall not be marked as critical, or – “Timestamping”, whereupon this extension shall be marked as critical.	No

10.1.9 Algorithm Object Identifiers

Comfact Certificate Services uses the following algorithms for signing issued certificates:

- id-RSASSA-PSS (OID 1.2.840.113549.1.1.10)
  - MGF-1 (OID 1.2.840.113549.1.1.8) with SHA-256 (OID 2.16.840.1.101.3.4.2.1) and a salt length of 32 bytes
  - MGF-1 (OID 1.2.840.113549.1.1.8) with SHA-512 (OID 2.16.840.1.101.3.4.2.3) and a salt length of 64 bytes
- ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)
  - Based on curve P-256 (OID 1.2.840.10045.3.1.7)
- ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)
  - Based on curve P-384 (OID 1.3.132.0.34)
- ecdsa-with-SHA512 (OID 1.2.840.10045.4.3.4)
  - Based on curve P-521 (OID 1.3.132.0.35)

10.1.10 Name forms

The subject and issuer fields of each certificate are populated with a unique Distinguished Name (DN) in the form of an X.501 DirectoryString in accordance with section 6.1.

10.1.11 Name constraints

No stipulation, Name Constraints extension is not used.

10.1.12 Certificate Policy object identifier

The certificate policy object identifier is in accordance with the one described in section 4.2.

10.1.13 Usage of policy constraints extension

No stipulation.

10.1.14 Policy qualifiers syntax and semantics

No stipulation.

10.1.15 Processing semantics for critical certificate policies extension

No stipulation.

10.2 CRL profile

Comfact Certificate Services issue CRLs that conform to RFC 5280.

10.2.1 Version numbers(s)

Comfact Certificate Services issues version two (2) CRLs, in accordance with RFC 5280.

10.2.2 CRL and CRL entry extensions

The following table outlines the extensions that may be used in CRLs issued by Comfact Certificate Services. Note that “optional” here refers to whether or not the extension is always used in Comfact Certificate Service’s CRLs.

Extension	Critical	Description	Optional
CRL Number	No	The CRL number indicates a monotonically increasing sequence number for a given CRL to determine when a particular CRL supersedes another CRL.	No
Authority Key Identifier	No	The authority key identifier indicates what public key is to be used to verify the signature of the certificate that issued the CRL.	No
Invalidity Date	No	Indicates a date which is the known or suspected date and time for when the private key was compromised, which may pre-date the revocation date in the CRL entry.	Yes
Reason Code	No	Indicate the reason for the certificate revocation.	Yes

10.3 OCSP profile

The profile for the online certificate status protocol (OCSP) messages issued by Comfact Certification Services follows the specifications as detailed in RFC 6960.

10.3.1 Version number(s)

Comfact Certification Services support version 1 of the OCSP request and response.

10.3.2 OCSP extensions

No stipulation.

11 Compliance audit and other assessment

To ensure that requirements of this document are being implemented and enforced, Comfact performs internal audits and revisions by team of internal auditors.

11.1.1 Frequency or circumstances of assessment

Compliance audits are conducted at least yearly. More than one audit per year is conducted if this is requested by the audited party or is a result of unsatisfactory results of a previous audit.

11.1.2 Identity/qualifications of assessor

Comfact Management Team is responsible for Comfact CPS and Comfact Certificate Services and appoints who should perform compliance audits. Auditors must have competence of compliance audits, specifically regarding requirements in the area of issuing and managing certificates.

11.1.3 Assessor's relationship to assessed entity

The internal auditor shall not audit his/her own areas of responsibility. External auditors of conformity assessment bodies shall be independent from Comfact assessed systems.

Internal audits are performed according to ISO 27001 according to a schedule resulting in a Statement of Applicability.

11.1.4 Topics covered by assessment

The topics covered by the assessment are to verify that all procedures and processes used for issuing certificates comply with this Comfact CPS and relevant parts of standard documents.

The assessment also includes parts of applications, policies, practices, facilities, personnel and assets that are related to Comfact Certificate Services.

11.1.5 Actions taken as a result of deficiency

Comfact has implemented an ISO 27001 Information Security Management System (ISMS). Results of a compliance audit are handled within this standard.

Deficiencies will be entered into the ISMS system either as incidents or as risks and tracked accordingly. Through the use of a supporting tool, Comfact ensures that all issues are being tracked and resolved in due course. Reporting and escalation are part of the system. The Management Team decides commercially reasonable efforts of corrective actions of deficiencies.

11.1.6 Communication of results

Comfact Management Team decides how and to whom results of a compliance audit shall be notified and published.

12 Other business and legal matters

12.1.1 Fees

12.1.1.1 Certificate issuance or renewal fees

Certificate issuance and or renewal are included in the applicable Comfact Service Agreement.

12.1.1.2 Certificate access fees

Certificate access fees are included in the applicable Comfact Service Agreement.

12.1.1.3 Revocation or status information access fees

Revocation or status information access fees are included the applicable Comfact Service Agreement.

12.1.1.4 Fees for other services

Fees for other services are included in the applicable Comfact Service Agreement.

12.1.1.5 Refund policy

A refund policy is included in the applicable Comfact Service Agreement.

12.1.2 Financial responsibility

12.1.2.1 Insurance coverage

Comfact has a commercially reasonable level of liability insurance coverage to support its business practices.

12.1.2.2 Other assets

No stipulation.

12.1.2.3 Insurance or warranty coverage for end-entities

No stipulation.

12.1.3 Confidentiality of business information

12.1.3.1 Scope of confidential information

Information that Comfact obtains in the course of its business transactions is considered confidential, except for information defined in section 12.1.3.2.

12.1.3.2 Information not within the scope of confidential information

Information not within the scope of confidential information already publicly available, contained in certificates or certificate status information (CRL and OCSP) is not deemed to be confidential.

12.1.3.3 Responsibility to protect confidential information

Comfact secures confidential information from compromise and disclosure to third parties by implementing different security controls in order to prevent unauthorized viewing, modification or deletion. Comfact handles confidential information in accordance with applicable Swedish and EU legislation and Comfact Service Agreement.

12.1.4 Privacy of personal information

Comfact handles personal data in accordance with applicable Swedish and EU legislation and Comfact Service Agreement.

12.1.4.1 Privacy plan

See section 12.1.4.

12.1.4.2 Information treated as private

See section 12.1.4. All keys handled by Comfact Certificate Services are handled as private and kept confidential.

12.1.4.3 Information not deemed private

See section 12.1.4. Any information already publicly available or contained in a certificate issued by Comfact Certificate Services, or its CRL, or by a publicly available service shall not be considered confidential. Note that, in instances where short-lived, end-entity certificates contains personal identifiable information, such certificates are not made publicly available through the repository but remains confidential.

12.1.4.4 Responsibility to protect private information

See section 12.1.4. Comfact secures private information from compromise and disclosure to third parties and complies with all applicable privacy laws.

12.1.4.5 Notice and consent to use private information

See section 12.1.4. Comfact will only use private information if a Subscriber given full consent during the registration process.

12.1.4.6 Disclosure pursuant to judicial or administrative process

See section 12.1.4. Comfact will release or disclose private information on judicial or other authoritative order.

12.1.4.7 Other information disclosure circumstances

See section 12.1.4.

12.1.5 Intellectual property rights

When disseminating this Comfact CPS, no information may be altered, deleted, or added. It must be clearly stated that Comfact is the issuer and copyright holder of this document.

Comfact owns or has licensed the intellectual property rights on all the components of the Comfact Certificate Services.

12.1.6 Representations and warranties

Comfact retains the overall responsibility for conformance with the procedures prescribed in this Comfact CPS when issuing and managing certificates provided to CAs, RAs, sub-CAs and Subscribers.

12.1.6.1 CA representations and warranties

See section 4.3.1.

12.1.6.2 RA representations and warranties

See section 4.3.2.

12.1.6.3 Subscriber representations and warranties

See section 4.3.3 and 12.1.9.

12.1.6.4 Relying Party representations and warranties

Comfact will require that Relaying Party complies with this Comfact CPS.

12.1.6.5 Representations and warranties of other participants

No stipulation.

12.1.7 Disclaimers of warranties

Comfact assumes no liability except as stated in the Comfact Service Agreement pertaining to certificate issuance and management.

12.1.8 Limitations of liability

Comfact assumes no liability except as stated in the Comfact Service Agreement pertaining to certificate issuance and management.

12.1.9 Indemnities

Indemnities are stated in the Comfact Service Agreement.

12.1.10 Term and termination

12.1.10.1 Term

This Comfact CPS takes effect based on the specified start time in connection with the publication in Comfact Repository.

12.1.10.2 Termination

This Comfact CPS is valid until it is replaced by a new version or until the Comfact Certificate Services ceases to operate. See also section 8.8.

12.1.10.3 Effect of termination and survival

This Comfact CPS applies in applicable parts after termination. See section 8.8 and 12.1.11.

12.1.11 Individual notices and communications with participants

Comfact will define appropriate provisions governing notices.

12.1.12 Amendments

Decisions with respect changes of this this Comfact CPS are at the sole discretion of the Comfact Management Team.

12.1.12.1 Procedure for amendment

Comments regarding this Comfact CPS can be submitted to Comfact as detailed in section 4.5.2.

Decisions to implement changes in Comfact CPS that require a new OID (see section 12.1.12.3) are made by Comfact Management Team for the Comfact Certificate Services (see section 4.5).

12.1.12.2 Notification mechanism and period

Publication of a new version of Comfact CPS must take place before it is put into operation. The publication must also contain information about what has changed.

12.1.12.3 Circumstances under which OID must be changed

Small changes to Comfact CPS that do not affect the meaning of the document can be made without the need to change the OID. If Comfact Management Team decides that a new OID is required this will be assigned and appropriate amendments made.

12.1.13 Dispute resolution procedures

Disputes arising from this Comfact CPS shall be finally settled in a Swedish court.

12.1.14 Governing law

When interpreting this Comfact CPS and when assessing Comfact Certificate Services actions in connection with the issuance of a certificate in accordance with this document, Swedish law shall apply.

12.1.15 Compliance with applicable law

Comfact Certificate Services are handled in accordance with Swedish law.

12.1.16 Miscellaneous provisions

No stipulation.

12.1.16.1 Entire agreement

Circumstances regarding entire agreement is stated in Comfact Service Agreement.

12.1.16.2 Assignment

Circumstances regarding assignment is stated in Comfact Service Agreement.

12.1.16.3 Severability

Should any provision or part thereof in this policy be found to be invalid, this shall not mean that the policy as a whole is invalid.

12.1.16.4 Enforcement (attorneys' fees and waiver of rights)

Circumstances regarding enforcement is stated in Comfact Service Agreement.

12.1.16.5 Force Majeure

Circumstances regarding force majeure are stated in Comfact Service Agreement.

12.2 Other provisions

12.2.1 Organizational

Policies and procedures under which the Comfact Certificate Services operates are non-discriminatory and has a properly documented agreements and contractual relationships in place.

Operations for certificate generation and revocation management have a structure that safeguards impartiality of operations as documented in this CPS.

12.2.2 Additional testing

Comfact provides customers with the possibility of testing all types of certificates it issues. Test certificates are clearly indicated that they are for testing purposes only.

12.2.3 Disabilities

Comfact Certificate Services are made accessible for persons with disabilities by following Web Content Accessibility Guidelines (WCAG) 2.1.

12.2.4 Terms and conditions

Comfact makes its terms and conditions available in Comfact Repository.

12.3 Framework for the definition of other certificate policies

No stipulation.

12.3.1 Certificate policy management

No stipulation.

12.3.2 Additional requirements

No stipulation.

-@-