PKI Disclosure Statement

Version date	**2024-04-08**
Classification	**Unclassified**
OID	**1.2.752.253.1.10**

Revision history of this document

This document PKI Disclosure Statement 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
2024-04-08	Updated version of the PKI Disclosure Statement created	Comfact Certificate Service’s Management Team

Table of contents

1 Introduction

The PKI Disclosure Statement (PDS) presented in this document provides a simplified overview of some of the content covered in Comfact CPS (e.g. contact information, certificate types, validation, issuance, revocation, and usage of digital certificates). This document is structured to align with ETSI 319 411-1 Annex A and serves to assist Public Key Infrastructure (PKI) users in making an informed trust decision. Please note that this document is not an agreement between Comfact and any organization, legal or natural person.

The full Comfact CPS is available at:

- https://comfact.se/repository

2 Contact Information

Comfact Certificate Service's Policy Management Team is responsible for authoring, reviewing, and approving changes to this PKI Disclosure Statement.

Contact information
Comfact AB
Certificate Services
Norra Liden 2A
SE-411 18 Gothenburg, Sweden
+46 (0)31 13 53 15
support@comfact.com

3 Certificate type, validation and usage

Certificates issued by Comfact Certificate Services can be used in a variety of applications to establish integrity, authenticity, and confidentiality as detailed below:

- *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.

Certificates issued by Comfact Certificate Services are specified in accordance with NCP+ as defined by ETSI 319 401 and ETSI 319 411-1 and are not intended for electronic communication or 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 in Comfact CPS) 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, server and client authentication, or Microsoft document signing. See section 10.1 in Comfact CPS for more information.

Certificates issued by Comfact Certificate Services shall not be used in any circumstance that may breach Swedish law, regulation, or any relevant agreements with Comfact AB.

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

Only legal or natural persons that is in agreement with Comfact and meets the requirements of validation and identification can request a certificate application which will be evaluated by Comfact Certificate Services Team. 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 Services CA G1	Applications for end-entity certificates can be submitted by an authorized Comfact Certificate Services employee.

Note: see Comfact CPS section 7, 9.1.7 and the Certificate Profiles in section 10 for further specification of the registration, identification and validation procedure as well as the intended usage for each certificate type.

4 Reliance Limits

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

5 Obligations of Subscribers

The obligations of the Subscriber are listed in Comfact Service Agreement in which the terms of use are listed. In addition, the Subscriber is also obligated to fulfill the requirements as detailed in Comfact CPS, which requires the Subscriber to provide complete and accurate information to Comfact Certificate Services at the time of the certificate request, adhere to the accepted use and secure storage requirements of the private key, and to request certificate revocation upon a suspected compromise of the private key.

6 Certificate Status Checking Obligations of 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.

6.1.1 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 Services CA G1	http://pki.comfact.com/crls/comfact-services-ca-g1.crl

6.1.2 Publication of OCSP

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

7 Limited Warranty and Disclaimer/Limitation of Liability

Warranty and liability limitations are detailed in the Subscriber's Comfact Service Agreement.

8 Applicable Agreements, CPS, CP

Information related to Comfact Certificate Services can be found at the Comfact Repository:

- https://www.comfact.se/repository

Other relevant documents include:

- Normalized Certificate Policy (NCP+) as outlined in ETSI 319 411-1,
- The Swedish National Policy Requirements as stated in DIGG Policy.

9 Privacy Policy

Comfact handles personal data in accordance with applicable Swedish and EU legislation, agreed Data Processing Agreement and Comfact Service Agreement.

10 Refund Policy

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

11 Applicable Law, Complaints and Dispute Resolution

When interpreting this document and Comfact CPS, as well as when assessing Comfact Certificate Services actions in connection with the issuance of a certificate in accordance with this document, Swedish law shall apply. Disputes arising from this document or Comfact CPS shall be finally settled in a Swedish court of law.

12 Repository Licenses, Trust Marks, and Audit

Comfact Certificate Services is a CA (Certification Authority), which has been active since 2008. Comfact Certificate Services is subject to conformity assessment according to the Swedish Agency for Digital Government (DIGG) and ETSI EN 319 411-1 and ETSI 319 411-2.

When disseminating this document or 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.

-@-