Certification Practice Statement

Certipost e-Certificates

Version	3.0
Effective date	31/01/2012
Document name	CPS_CTP_e-Certificates_V3_0.docx
© Certipost NV ALL RIGHTS RESERVED.	

1. Document control

© Certipost nv, Ninovesteenweg 196, 9320 Erembodegem. No part of this document may be used, reproduced or distributed, in any form including electronically, without written permission of Certipost nv.

Review history

Reviewer	Date	Action	Version	Status
CEPRAC members	19/12/2003	Initial version	1.0	Approved
CEPRAC members	15/08/2006	CA issuer change	2.0	Approved
CEPRAC members	22/12/2008	Certipost branding update	2.1	Approved
CEPRAC members	08/12/2009	Update to add new CA & certificate profiles	2.2	Approved
CEPRAC members	14/07/2010	Update for restriction on chains	2.3	Approved
CEPRAC members	12/01/2011	Minor changes and logo update	2.4	Approved
CEPRAC members	31/01/2012	Update for new PKI hierarchy and document refactoring	3.0	Approved

2. Index

3. Definitions and Acronyms

Definitions and acronyms have a dynamic nature as they tend to be expanded regularly. A generic document with the definitions and acronyms is available on-line on http://pki.certipost.com

This document is under strict control of the Certipost CErtification PRactices Council (CEPRAC).

More information about CEPRAC can be found in section 5.1.5.4 of the Certification Practice Statement (CPS).

(Reference to RFC 3647: 1.6)

4. Introduction to this document

This document describes the Certification Practice Statement (CPS) for the Certification Service Provider (CSP) "Certipost". Several "Certipost" Certificate Policies (CP) are realized according to this CPS. Both CAs owned by Certipost and dedicated to customers make use of "Certipost" as a CSP in accordance with this CPS.

A third type of document, "General Terms and Conditions" also exists to supplement the information (mostly from a contractual perspective) provided by CP and CPS.

This CPS is based on RFC 3647. However in format an alternative approach was chosen in order to:

- Avoid redundancy and thus possible inconsistencies of data. Some sections and elements described in the CPs are not repeated in the CPS and visa versa. For example, certificate profiles can be found in the CPs while CRL profiles can be found in the CPS.
- Lower maintenance cost: every change should have a minimal impact on the entire document by making sure the information is not redundant

5. Set of Provisions

5.1. Introduction

5.1.1. Overview

The PKI that is at the basis of Certipost as Certificate Service Provider consists out of a separate outsourced Certificate Factory unit and an in-house infrastructure for all other services described in this CPS that are not provided by the Certificate Factory.

Certipost and the parties to whom Certipost may outsource service are obliged to maintain the Certipost PKI Infrastructure in accordance with this CPS

For the subscriber, Certipost is the sole Certificate Service Provider. Certipost is a Certification Authority in multiple hierarchies and with Registration Authorities in different modes.

There are multiple possible levels of assurance that may or may not be provided by certificates within the PKI in this scope, for example:

- Qualified & Normalized assurance level

This is either:

- The highest level of assurance provided by a Qualified Trusted Service Provider (supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC). Evidence of the identity is checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence.
  - For this level of assurance, Certipost shall ensure that all requirements for the CA are implemented in conformance with the ETSI Technical Specification TS 101456 or equivalent

Or:

- The highest level of assurance provided by a Qualified Trusted Service Provider (supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC), supporting the same level of quality as certification authorities issuing qualified certificates (as required by article 5.1 of the Directive) but "normalized" for wider applicability. Evidence of the identity is checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence.
  - For this level of assurance, Certipost shall ensure that all requirements for the CA are implemented in conformance with the ETSI Technical Specification TS 102042 (Normalized level) or equivalent

- Lightweight Assurance level

  - A medium level of assurance provided by a Qualified Trusted Service Provider (supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC). Evidence of the identity is checked against a physical person either directly or indirectly using means which do not necessarily provide equivalent assurance to physical presence.

    - For this level of assurance, Certipost shall ensure that all requirements for the CA are implemented in conformance with the ETSI Technical Specification TS 102042 (Lightweight level) or equivalent

- Other Assurance levels

Except for the segregated "Qualified" hierarchy that has the purpose to facilitate Qualified Electronic Signatures in accordance with the Directive 1999/93/EC, the assurance level is only determined by the CP.

The root CA certificates and the operational (issuing) CA certificates are described in section 5.7.

This also applies to the ARLs and CRLs.

The certificate profiles of the end-entity certificates are described in the CP of CPs referenced in these end-entity certificates.

5.1.1.1. Trusted Roots, Intermediate CA Certificates and Issuing CA Certificates

Distributed trusted roots:
GTE Cybertrust root
Certipost E-Trust TOP Root CA
Baltimore CyberTrust Root
Verizon Global Root CA

Non- distributed trusted roots: internal use
Certipost Internal Use CA SHA-1
Certipost Internal Use CA SHA-256

Primary CA's / Issuer	GTE Cybertrust root	Certipost E-Trust TOP Root CA	Baltimore CyberTrust Root	Verizon Global Root CA
Certipost E-Trust Primary Qualified CA	x	x	x	no
Certipost E-Trust Primary Normalized CA	x	x	x	no
Certipost E-Trust Primary LightWeight CA	x	x	x	no

Secondary & issuing CA / issued by	Certipost E-Trust Primary Qualified CA	Certipost E-Trust Primary Normalized CA	Certipost E-Trust Primary LightWeight CA	Baltimore CyberTrust Root	Verizon Global Root CA
Certipost E-Trust Secondary Qualified CA for Physical Persons	x				
Certipost E-Trust Secondary Qualified CA for Legal Persons	x				
Certipost E-Trust Secondary Qualified CA for Communities	x				
Certipost E-Trust Secondary Qualified CA for Publilink	x				
Certipost E-Trust Secondary Normalized CA for Physical Persons		x			
Certipost E-Trust Secondary Normalized CA for Legal Persons		x			
Certipost E-Trust Secondary Normalized CA for Communities		x			
Certipost E-Trust Secondary Normalized CA for Publilink		x			
Certipost E-Trust Secondary Normalized CA for Carenet		x			
Certipost E-Trust Secondary Normalised CA for SSL and Code		x			
Certipost E-Trust Secondary Normalized CA for EUROCONTROL		x			
Certipost E-Trust Secondary Lightweight CA for Physical Persons			x		
Certipost E-Trust Secondary Lightweight CA for Communities			x		
Certipost E-Trust Secondary Lightweight CA for IDABC			x		
Certipost E-Trust Secondary Lightweight CA for EUROCONTROL			x		
Certipost Public CA for Qualified Signatures				x	x
Certipost Public CA for Persons and Organizations				x	x
Certipost Public CA for Devices, Addresses and Services				x	x
Certipost Internal Use CA Root Signed SHA-1				x	
Certipost Internal Use CA Root Signed SHA-256					x
Certipost Lightweight CA for EUROCONTROL					x

All the hierarchies which extend up to the distributed trusted roots are considered as public.

The other hierarchies, which extend up to the "Non-distributed trusted roots: internal use", are not considered as public.

5.1.2. Document name and identification

Certification Practice Statement Name:

CPS_CTP_e-Certificates_v3_0

Object Identifiers: **[1.3.6.1.4.1.3860.1.1.1.3]**

iso.org.dod.internet.private.enterprise (**1.3.6.1.4.1**).Certipost(**3860**).pki(**1**).CPS(**1**).CPS-type(**1**).Version(**3**)

(Replaces: 0.3.2062.Certipost (7).E-Trust(1).CPS(0).CPS-type(1).Version(2).Sub-version(3))

The version number of the OID equals this document version. The sub version number indicates the document revisions which do not impact the content and the version of the CPS.

Current CPs and their identifiers can be found in the repository.

5.1.3. PKI participants

5.1.3.1. Certification authorities

The sole Certificate Authority in scope of this CPS is Certipost.

Certipost is the Certificate Authority and Certificate Service Provider of the issuing CAs indentified in section 5.1.1.1.

In addition:

- Certipost allows for cross-certification engagements. Any request for cross-certification engagements by an external CA will have to be submitted to Certipost Certificate Services according to the contact information in section 5.1.5.2 .
- Certipost reserves right to set-up additional Issuing CAs in accordance with the current Certipost CPS.

5.1.3.2. Registration authorities

The RA is obliged to accurately represent the information it prepares for a CA.

The RA is also obliged to (depending on the CP) keep, for up to 30 years after the expiry of the last certificate, corresponding to this registration, supporting evidence for any Certificate request made to a CA (e.g., Certificate request forms) in accordance with the CPS. In particular a copy is archived of all information used to verify the identity of the Certificate Holder and any references to his professional status, including any reference numbers on the documentation submitted for verification, and any limitations of its validity together with a copy of the contractual agreement signed by the Subscriber, including all obligations incumbent on him.

Resellers and Registration Authorities (RAs) cannot issue certificates on behalf of any public CA under this CPS.

a) In accordance with the provisions of this CPS, the following Registration Authorities can be distinguished:

- Certipost Central RA,
    - In that case Certipost can still outsource parts of the registration activities but remains the sole RA.
- Certipost authorized Local RAs (LRAs) as specified in the applicable CP and as ruled by formal contractual agreement between Certipost and the concerned legal entity acting as Local RA,
- Community Specific Local RAs as specified in the applicable CP and as ruled by formal contractual agreement between Certipost and the concerned legal entity acting as Local RA.

a) Any Registration Authority which operates within the Certipost PKI in accordance with this CPS or any applicable CP shall:

- Register with, and obtain the approval of a CA that issues Certificates in accordance with this CPS (in

case of Certipost CAs, this approval shall be obtained from the Certipost CErtification PRactices Council (CEPRAC)).

- Undertake to conform to the stipulations of this CPS, the applicable CP under which the Certificate that has been applied for is issued, and to internal procedures**.**
- Enter into Contractual agreements set up according to the relevant sections of this CPS.

The list of Local RAs that are allowed to register requests for a Lightweight Certificate under the Certipost CPS is stated in the related CP according to the relevant sections of this CPS or in a separate contract.

5.1.3.3. Subscribers

a) In accordance with the corresponding CP, Subscribers that are the subject of the issued Certificates may be:

- Any physical person, which can be identified in accordance with the related CP. Please see applicable CP for details.
- Any physical person associated with an organization, which can be identified in accordance with the related CP. Please see applicable CP for details.
- Any physical person acting as a representative – in the name of – an organization , which can be identified in accordance with the related CP. Please see applicable CP for details.
- Any organization or legal person, which can be identified in accordance with the related CP.
- Any other end-entity, being a device, an address or a service, which can be identified in accordance with the related CP. Please see applicable CP for details.

b) In accordance with the corresponding CP, Subscribers that are not the subject of the issued Certificates may be an organization under the condition that it can be uniquely identified

5.1.3.4. Relying parties

Any party relying on the data certified in the certificates for public trust is considered a relying party. The responsibility of the CSP towards the relying parties is limited in accordance with the provisions in the CP.

The CSP does not grant any guarantee about the ability of applications to make use of the certificates and the services. Neither does the CSP guarantee that these applications will make correct use of the certificates. The responsibility to ensure the correct use and ability to use the certificates lies entirely at side of those entities responsible for the applications.

The CSP declares to provide certificates and certificate services in accordance with the standards identified in this CPS.

5.1.3.5. Other participants

5.1.3.5.1. The Certificate Service Provider

Certipost acts as the Certificate Service Provider (CSP) with ability to outsource different services and tasks to other parties.

5.1.3.5.2. The Subject

The Subject is the entity which is certified by the certificates. As such the subject may be a participant. The subject may be the subscriber or somebody or some entity associated with the subscriber.

5.1.3.5.3. Subject device provision service

A participant, with a distinct responsibility, that can be an outsourced partner of the CSP is the Subject device provision service. This participant is responsible to handle and manage the devices that store private keys of certificates (generally called "private key holding devices" here). In particular, secure tokens, smart cards, SCDs, Secure User Devices (SUDs), or SSCDs can be subject to the management of this participant. The main role of this participant is to handle the life cycle of these tokens according to the provisions of this CPS.

5.1.3.5.4. Policy Approval Authority

a) The Policy Approval Authority of Certipost is a high level management body named CEPRAC (CErtification PRActice Council) with final authority and responsibility for:
   - Specifying and approving the Certipost trusted service provider (TSP) services, policies and practices.
   - Approving the Certification Practice Statement(s), Certificate Policies, Signing Policies, Time-stamping Policies and other TSP related documents or decisions which have a possible impact on the responsibility and/or liability of Certipost as trusted service provider.
   - Defining the review process including responsibilities for maintaining the policies.
   - Defining the review process that ensures that the certificate practices are properly implemented by the trusted authorities e.g. Certification Authorities (CAs), PKI participants, Signing authority, Time-stamping Authorities (TSA) etc.
   - Defining the review and audit process that ensures that the trusted roles and authorities are compliant with and act in accordance with the policies.
   - Publication of the policies and their revisions to the subscribers and relying parties.
   - Specifying cross-certification procedures and handling cross-certification requests.
b) The Policy Approval Authority organization rules are part of an internal document which is available for internal use and for inspection by auditors.

5.1.4. Certificate usage

5.1.4.1. Appropriate certificate uses

Appropriate certificate uses depend of and are described in the CP or CPs referenced in these certificates. If two CPs are referenced the appropriate uses are a sum of both. However, some CPs prohibit the combination of one CP with another CP in the same certificate. In this case there will only be one CP referenced in the certificate concerned.

5.1.4.2. Prohibited certificate uses

Prohibited certificate uses are always those that are not explicitly listed in the appropriate Certificate uses.

5.1.5. Policy administration

5.1.5.1. Organization administering the document

The Certipost CErtification PRactices Council (CEPRAC) is the organization administering this document.

5.1.5.2. Contact person

All questions and comments concerning this CPS must be addressed to:

Contact persons:

Certipost CErtification PRactices Council (CEPRAC)

c/o Guy Ramlot

Ref.: CPS Administration

Muntcentrum

B-1000 Brussels

Belgium

http://www.certipost.com

service.desk@certipost.com

5.1.5.3. Person determining CPS suitability for the policy

a) Certipost CErtification PRactices Council (CEPRAC) determines a risk assessment policy that shall be carried out to evaluate business requirements and determine the security requirements in relation with this CPS.

b) Certipost CErtification PRactices Council (CEPRAC) is responsible for determining the Certipost CPS suitability for any Certipost CP.

c) Certipost CErtification PRactices Council (CEPRAC) is responsible for determining and issuing the CPs, determining their suitability to CPS and to authorize (Local) RAs to register Certificate requests and CAs to issue Certificates under a particular Certipost CP and this CPS.

d) Certipost CErtification PRactices Council (CEPRAC) is responsible for initiating audits.

e) To contact the Certipost CErtification PRactices Council (CEPRAC), please use the contact information in section 5.1.5.2

5.1.5.4. CPS and Definitions and Acronyms approval procedures

For the CPS:

a) The only changes that Certipost may make to this specification without notification are editorial or typographical corrections, or changes to the contact details.
b) Errors, updates, or suggested changes to this document shall be communicated to the contact in section 5.1.5.2 of this CPS. Such communication must include a description of the change, a change justification, and contact information of the person requesting the change.
c) The Certipost CErtification PRactices Council (CEPRAC) shall accept, modify or reject the proposed change after completion of the review period.
d) The date of publication and the effective date are indicated on the title page of the CPS.
e) All changes to the CPS or CP, other than editorial or typographical corrections, or changes to the contact details, will be subject to a new Object Identifier for the CPS or CP.

For Definitions and Acronyms:

- No additions or modifications are allowed that create ambiguity in regard to existing definitions and acronyms.
- Additions and modifications are accepted, modified or rejected by CEPRAC
- The latest and most up-to-date version is published

5.1.6. Definitions and acronyms

See section 3

5.2. Publication and repository responsibilities

5.2.1. Repositories

The publication of the material described in the next section happens on a publicly available web site.

Of those end-entity certificates that Certipost shall publish, a copy is published in publicly available repositories, after the certificate has been issued by Certipost.

The repositories described above, may be published by either Certipost or an outsourced party. In any case, Certipost will do its best efforts to obtain an uptime of 99.5 % for its public repository service.

5.2.2. Publication of certification information

CAs within the Certipost PKI shall make publicly available, in their repositories:

- The Certipost Certificate Services CPS;
- The list of Definitions and Acronyms
- The publically applicable CPs under which certificates are issued according to this CPS;
- Certification Revocation Lists;
- Authority Revocation Lists;

- All CA certificates issued by the CA, self signed CA Certificates and cross certificates for cross certified CAs – if these exist;
- General terms and conditions;
- Certificates issued by the CA in conformance with this CPS – only if stipulated in the CP referred to in the certificates.
  - In case such end-entity certificates are published, publication of these certificates is subject to acceptance by the certificate holder or subscriber. The CP can state that the acceptance of a certificate implicitly acknowledges the correctness of the data certified in the certificate.

Certipost shall provide relevant information about issued Certificates when necessary to aid in dispute resolution concerning, for example, electronic signatures.

CRL's shall contain revocation status information about all revoked and suspended Certificates, during the lifetime of the corresponding CA Certificate.

Certipost will make available the CA-Certificates for all public CA-keys in the Certipost Certificate Public Registry until at least 30 years after the Certificates' expiration.

5.2.3. Time or frequency of publication

- CRL publication shall be in accordance with the CP. If a certificate refers to more than one CP, the highest publication frequency specified within shall take precedence.
- ARL publication shall be in accordance with in the "ARL Profile" in section 5.7.
- CPS publication shall be in accordance with the CPS change procedures.

5.2.4. Access controls on repositories

- There shall be no access controls on the reading of the public CP or of the public CPS. Everybody has read access.
- Access controls on certificates are optional at the discretion of the CA and may be part of a specific rule of a particular CP.
- There shall be appropriate access controls controlling who – as determined by the Certipost CErtification PRactices Council (CEPRAC) – can write or modify items in the electronic repository concerned by 5.2.25.2.2
- Documents in the Certipost Public Registry that have no intrinsic protection like certificates and CRLs, including the GTC, list of Definitions and Acronyms, CPs and CPS are under strict control of the Certipost CErtification PRactices Council (CEPRAC) and are protected against unauthorized modification by means of procedures established by the Certipost CErtification PRactices Council (CEPRAC). This Certipost CErtification PRactices Council (CEPRAC) identifies the valid versions of the CPs and CPS and signed masters are stored securely.

5.3. Identification and authentication

5.3.1. Naming

5.3.1.1. Types of names

This is determined in the CP.

5.3.1.2. Need for names to be meaningful

This is determined in the CP.

5.3.1.3. Anonymity or pseudonymity of subscribers

The use of a pseudonym is allowed by Certipost CSP, but only in addition to other attributes and in conformance with the CP.

5.3.1.4. Rules for interpreting various name forms

This is determined in the CP.

5.3.1.5. Uniqueness of names

The rules for the uniqueness of names are determined in the CP.

5.3.1.6. Recognition, authentication, and role of trademarks

Certipost cannot guarantee that the names issued in the certificates will include the trademark requested by the subscriber.

No RA, or any CA within the Certipost Infrastructure is obliged to perform any trademark infringement investigation at the time the Naming information is provided by an entity. Certipost is not liable for any trademark infringement by a Subscriber or a third party.

In case of any name claim dispute, the requester will contact Certipost Certificate Services (see contact information in section 5.1.5.2) Certipost will investigate the grounds on which the name claim dispute is based.

Any entity acting within the Certipost PKI Infrastructure is obliged to give appropriate and sufficient co-operation to an investigation mentioned in this section.

In case the name claim dispute is due to an error of Certipost, Certipost will undertake immediate action – free of charge – to solve the problem.

In case the name claim dispute is due to negligence or malicious actions (genuine will to harm) of a Subscriber or a Relying Party, Certipost reserves the right to terminate the contract(s) immediately, to revoke the certificate and to refuse to continue any collaboration with that person. Certipost reserves the right to undertake legal actions.

5.3.2. Initial identity validation

5.3.2.1. Method to prove possession of private key

Whether this is required is determined in the CP.

In general the following situations can occur:

- The private key is created in a secure token or in a SSCD which is already in the possession and under the sole control of the subject
- The private key is created on a server at the subscribers premises
- The private key is created on a secure HSM at the subscriber's premises and the creation needs to be witnessed by Certipost during a key ceremony
- The private key is created centrally by Certipost in a secure environment and transferred securely to the subject
- The private key is created centrally by Certipost in a secure environment and transferred securely to the subject where it is injected securely in a secure token which is under the sole control of the subject
- The private key is created in a token which is not yet in the possession of the subject

Where applicable, all Certificate requests must be signed by the Subscriber using the Private Key that corresponds with the Public Key in the request (e.g. using PKCS#10 standards). This will enable the RA to verify the user's Private Key possession.

Other requirements may be that the origin of the request itself (namely a particular secure token or SSCD) is authenticated as well.

The methods employed to achieve the above objectives are described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement) internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.3.2.2. Authentication of organization identity

The RAs within the Certipost PKI Infrastructure are obliged to undertake the procedures set forth in the related CP and in the appropriate internal documents in order to authenticate the organization identity.

Depending on the assurance level, (e.g. Qualified, Normalised or Lightweight) the authentication of an organization will require the appropriate documents as specified in the applicable CP (see applicable CP for details).

5.3.2.3. Authentication of individual identity

The RA within the Certipost PKI Infrastructure is obliged to undertake the procedures as set forth in the related CP and in the appropriate internal documents in order to authenticate the identity of the applicant.

Depending on the assurance level, (e.g. Qualified, Normalised or Lightweight) the authentication of an individual entity will require the appropriate documents as specified in the applicable CP (see applicable CP for details).

5.3.2.4. Non-verified subscriber information

The RA within the Certipost PKI Infrastructure is obliged to undertake the procedures as set forth in the related CP. In general non-verified information shall not be certified.

5.3.2.5. Validation of authority

The RA within the Certipost PKI Infrastructure is obliged to undertake the procedures as set forth in the related CP.

If relevant, the application should include the authorization from a legal representative (or a mandated person) of the organization that the applicant can obtain and use the requested professional identity.

5.3.2.6. Criteria for interoperation

Not applicable.

5.3.3. Identification and authentication for re-key requests

This must be on the same level of trust as the initial identity validation. If the re-key request is not the result of changes in certified data and the means exist for trusted communication between the subscriber and the RA, then the re-keyed certificate may make use of the data based on the original verification. Otherwise a process that gives the same level of assurance as the initial registration shall be performed.

5.3.4. Identification and authentication for revocation request

The initiator of a revocation request should be sufficiently authenticated and authorized to perform the revocation in order to reduce the risk of wrongful revocation.

The methods employed to achieve the above objectives are described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement) internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.4. Certificate life-cycle operational requirements

5.4.1. Certificate Application

5.4.1.1. Who can submit a certificate application

The CP determines who can submit a certificate application. Different allowed methods of enrollment can exist depending on who can submit the application,.

Typically the following participants are candidates for the certificate application:

- The future certificate holder or subject

- A RA or LRA
- Mandated persons of the subscriber organization
- Authorized systems of the subscriber organization

5.4.1.2. Enrollment process and responsibilities

The enrollment process can be initiated in different ways:

a) Before the actual application the requestor is provisioned by mandated persons or services and given the right to apply for certain certificates
   - In this case a contractual agreement between Certipost and the subscriber organization (to which the mandated persons or services belong) must exist and stipulate the rights and constraints of the subscriber organization to provision subjects

b) An individual submits a request in his / her own name
   - In this case a contractual agreement between Certipost and the individual requestor needs to be established before the enrollment process can proceed

In the next step the actual certificate application needs to be submitted. The CP can limit by whom and in what way this must happen.

If the RA or LRA does not submit the certificate application – either after reception from another participant or by their own initiative, the RA or LRA needs to establish a process and / or procedure for the requestor to submit their application.

The procedures are described in the applicable contractual agreement (e.g. purchase order, general terms and conditions and CP).

The RA or LRA is responsible to take all measures to ensure that the application is accurate.

Subscribers are obliged to give accurate and complete information to the certification service provider (CA, RA) in accordance with the related CP, particularly with regards to registration.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

As a result of the application and depending on the applicable CP the key pair will be generated by the requester or the CSP:

a) In case the requester generates the key pair, an electronic Certificate request will be provided during application.
b) In case the CSP (e.g. at RA premises) generates the key pair, measures will be taken to protect the private key during transference to the Certificate holder.

Requester will accept the applicable contractual agreement (purchase order, general terms and conditions and CP) assuring that the information provided earlier is correct. Herewith the requester will also authorize the creation and the publication of the obtained Certificate in the Certipost Certificate Public Registry if this is in accordance with the CP.

5.4.2. Certificate application processing

5.4.2.1. Performing identification and authentication functions

The application is required to be strongly authenticated. This can happen either explicitly or implicitly.

A valid approach of how application processing can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.4.2.2. Approval or rejection of certificate applications

Applications can be based on accurate information sources. But these must be verified by the applicant and then accepted or rejected.

When certificate applications are made in accordance with this CPS and the applicable CP, the approval is by default and without introducing additional delays.

5.4.3. Certificate issuance

5.4.3.1. CA actions during certificate issuance

Unless otherwise foreseen in the applicable CP, the following applies:

- The issuing CA performs certificate issuance and for this ensures that new Certificates are issued securely.
- The process of issuing the certificates is securely linked to the associated registration, the certificate rekey, renewal or recertification. In particular, as part of certificate issuance by the issuing CA, the following procedures have to be followed:
    - The RA must compare the electronic information provided by the Requester to the information presented in the signed contractual agreement in case a separate contractual agreement is signed. The information provided in the signed contractual agreement prevails on the electronic information.
    - The RA sends the request securely to the CA.
    - The certificate holder or the mandated person (if this is allowed by the CP) verifies and approves the information to be certified.
    - If the Requester takes care of the key generation, the RA checks the self-signed request (e.g., PKCS#10 request).
    - If the issuing CA (CSP) generates the subscriber's private key, then it is securely transferred to the requester in accordance with the CP
    - Dependant on the applicable CP and in case the private key pair is generated by the CSP a copy of the Certificate Holder's private key (used for encryption purposes) will be archived during certificate issuance.
    - The CA will generate the certificate and publish it in the Certipost Certificate Public Registry if this is in accordance with the CP
    - Certificates are generated and issued in accordance with the applicable laws and regulations
    - The Certificate is sent directly to the requester.
    - An audit trail is created of all the requests and the resulting generations of certificates
    - The RA archives all the information in accordance with the CP.

5.4.3.2. Notification to subscriber by the CA of issuance of certificate

The subscriber can be notified by the CA by means of reporting that the Certificate was issued.

5.4.4. Certificate acceptance

5.4.4.1. Conduct constituting certificate acceptance

The certificate is deemed accepted by default if the certificate was created as a result of an issuance process triggered by the requester. During that issuance process the Subscriber is asked to verify the accuracy and correctness of the content of his/her Certificate. In case of reported inconsistencies the issuance process will be halted or the data will be corrected. This will be the Subscriber's sole remedy for any acceptance refusal.

In case the subject or the subscriber wants to revoke this acceptance, certificate revocation may still be used but the provisions of certificate revocation will apply.

5.4.4.2. Publication of the certificate by the CA

Whether or not the certificate is published and where it is published is determined in the CP.

5.4.4.3. Notification of certificate issuance by the CA to other entities

Whether or not notification of certificate issuance to other entities takes place and which entities are involved is determined in the CP.

5.4.5. Key pair and certificate usage

5.4.5.1. Subscriber private key and certificate usage

Appropriate use of the private key and certificate is determined by the CP.

5.4.5.2. Relying party public key and certificate usage

Appropriate use of the private key and certificate is determined by the CP.

5.4.6. Certificate renewal

5.4.6.1. Circumstance for certificate renewal

A precondition for renewal is that the CP must allow this.

Certificate renewal must be considered as a new certificate application with the exception that a previously certified public key and the corresponding private key is reused and all the certified data, including the CP, is still valid.

Certificate renewal may never take place after the certificate has been revoked because of key compromise or a significant risk of key compromise or when the certificate is suspended.

It also has to be ensured that there are no changes in the certified data (except for the validity interval), the trust chain or the CP.

If evolutions in technology or other conditions with the same effect require the CSP to change the cryptographic key lengths and algorithms, the CP must be modified and therefore certificate renewal is not allowed.

Furthermore, the subscriber must still have a contractual agreement with Certipost that is valid in the new validity interval of the certificate or must agree to a new one that covers the extended period.

The new validity interval must be in accordance with the CP, which can impose limitations of maximum validity.

If these conditions are met, renewal can take place when a certificate is bound to expire.

If the renewed certificate is used before the expiry of a previous certificate, then this previous certificate should be revoked by the subscriber to avoid further use of the previous expiring certificate.

5.4.6.2. Who may request renewal

The CP determines who may request renewal – if this is allowed.

5.4.6.3. Processing certificate renewal requests

- Renewal may be requested "as a rule" by the subscriber based on an agreement with Certipost.
  - In that case the possibly to initiate a certificate renewal within a certain timeframe before and after expiry is preconfigured by the CSP.
  - The certificate holder or a mandated person (if this is allowed by the CP) may then initiate an automatic renewal within the configured timeframe.
- Renewal may also be requested by the subscriber where an agreement exists between Certipost and the subscriber that future purchases may be made by the subscriber to renew the certificate.

The RA is responsible to ensure that the conditions for renewal are met.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.4.6.4. Notification of new certificate issuance to subscriber

The subscriber can be notified of renewed certificate issuance by means of reporting.

5.4.6.5. Conduct constituting acceptance of a renewal certificate

Since the renewal of the certificate is requested and in some cases also initiated by the subscriber, acceptance is deemed to be by default, after the certificate holder or the mandated person (if this is allowed by the CP) verifies and approves the information to be certified.

5.4.6.6. Publication of the renewal certificate by the CA

Whether or not the certificate is published and where it is published is determined in the CP.

5.4.6.7. Notification of certificate issuance by the CA to other entities

Whether or not notification of certificate issuance to other entities takes place and which entities are involved is determined in the CP.

5.4.7. Certificate re-key

5.4.7.1. Circumstance for certificate re-key

A precondition for re-key is that the CP must allow this.

Any change in the certified data (including the CP) and the CA hierarchy, any action or event (such as certificate expiration or revocation), any evolution which necessitates a new key length and/or algorithm change can be a circumstance for certificate re-key.

Furthermore, the subscriber must still have a contractual agreement with Certipost that is valid in the new validity interval of the certificate or must agree to a new one that covers the new period.

The new validity interval must be in accordance with the CP, which can impose limitations of maximum validity.

If these conditions are met, re-key can take place whenever a new certificate is needed due to the invalidity of the previous certificate.

If this is allowed by the CP and the conditions for such an action are met, certificate renewal or certificate modification with re-certification can be alternatives for a re-key.

- If it is advantageous to limit the number of keys the alternatives can then be preferred over re-keying.

5.4.7.2. Who may request certification of a new public key

The CP determines who may request certification of a new public key.

5.4.7.3. Processing certificate re-keying requests

- Re-key may be requested "as a rule" by the subscriber based on an agreement with Certipost.
  - In that case the possibility to initiate a certificate re-key within a certain timeframe before and after expiry is preconfigured by the CSP in order to deal with expiry.
  - In that case the possibility to initiate a certificate re-key after the certificate has been revoked, or the CP has been changed can also be preconfigured by the CSP
  - The certificate holder or a mandated person (if this is allowed by the CP) may then initiate an automatic rekey, either within the configured timeframe in case of due expiration or after revocation or change of the CP.
- Re-key may also be requested by the subscriber where an agreement exists between Certipost and the subscriber that future purchases may be made by the subscriber to renew the expired certificate or replace a revoked certificate or a certificate that has become outdated due to a CP change.

The RA is responsible to ensure that the conditions for re-key are met.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.4.7.4. Notification of new certificate issuance to subscriber

The subscriber can be notified of the new certificate issuance by means of reporting.

5.4.7.5. Conduct constituting acceptance of a re-keyed certificate

Since the re-key of the certificate is requested and in some cases also initiated by the subscriber, acceptance is deemed to be by default, after the certificate holder or the mandated person (if this is allowed by the CP) verifies and approves the information to be certified.

5.4.7.6. Publication of the re-keyed certificate by the CA

Whether or not the certificate is published and where it is published is determined in the CP.

5.4.7.7. Notification of certificate issuance by the CA to other entities

Whether or not notification of certificate issuance to other entities takes place and which entities are involved is determined in the CP.

5.4.8. Certificate modification

5.4.8.1. Circumstance for certificate modification

A precondition for certificate modification is that the CP must allow this.

Certificate modification must always be in combination with re-certification, where a process exists similar to the "Initial identity validation" for the modified information. Certificate modification must therefore be considered as a new certificate application with the exception that a previous key pair can be reused.

Certificate modification may never take place after the certificate has been revoked because of key compromise or a significant risk of key compromise or when the certificate is suspended.

Any change in the certified data (including the CP) and the CA hierarchy can be a circumstance for certificate modification, except when such a change also results in the revocation of the certificate.

Furthermore, the subscriber must still have a contractual agreement with Certipost that is valid in the new validity interval of the certificate or must agree to a new one that covers the new period.

The new validity interval must be in accordance with the CP, which can impose limitations of maximum validity.

If these conditions are met, modification can take place whenever a new certificate is needed due to the invalidity of the previous certificate.

It must be assured that the previous certificates, when not yet expired are revoked.

5.4.8.2. Who may request certificate modification

The CP determines who may request modification – if this is allowed.

5.4.8.3. Processing certificate modification requests

- Modification may be requested "as a rule" by the subscriber based on an agreement with Certipost.
  - In that case the possibilityto initiate certificate modification can be preconfigured by the CSP in order to deal with changes in the certified data.
  - The certificate holder or a mandated person (if this is allowed by the CP) may then initiate an automatic certificate modification after changes to the certified data.
- Modification may also be requested by the subscriber where an agreement exists between Certipost and the subscriber that future purchases may be made by the subscriber to modify the certificate that has changed or has become outdated due to a CP change.

The certificate that will be replaced by the modified certificate because of any changes in the certified data must be revoked.

The certificate that will be replaced by the modified certificate because of changes in the CP may be revoked.

The RA is responsible to ensure that the conditions for modification are met.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.4.8.4. Notification of new certificate issuance to subscriber

The subscriber can be notified of the new certificate issuance by means of reporting.

5.4.8.5. Conduct constituting acceptance of modified certificate

Since the modification of the certificate is requested and in some cases also initiated by the subscriber, acceptance is deemed to be by default, after the certificate holder or the mandated person (if this is allowed by the CP) verifies and approves the (new) information to be certified.

5.4.8.6. Publication of the modified certificate by the CA

Whether or not the certificate is published and where it is published is determined in the CP.

5.4.8.7. Notification of certificate issuance by the CA to other entities

Whether or not notification of certificate issuance to other entities takes place and which entities are involved is determined in the CP.

5.4.9. Certificate revocation and suspension

5.4.9.1. Circumstances for revocation

Revocation of a valid (unexpired) certificate must happen as soon as:

- The certified information is not valid any more or the content has changed. (including the end of existence of the subject)
- There is a significant risk of private key compromise or the private key has already been compromised.
    - Note: previous certificates of the same key that have not expired and have not yet been revoked must also be revoked in this case.
- The security of algorithms and key lengths employed in the certificate risks to become below the standard of acceptability in the near future
- The certificate has been delivered from wrong or falsified information.
- The subscriber has violated or otherwise ended the contractual provisions and agreement (e.g. the subscription to the certificate service has not been paid in respect with the purchase agreement.)
- The certified entity does not exist anymore as an entity associated with the subscriber
- The CA stops its activities without another CA taking over its activities. Even though revocation checking should encompass the complete certification path and thus the revocation of the issuing CA should be sufficient to invalidate all issued end-entity certificates, in practice it may be recommended to also revoke each end-entity certificate issued by the CA. Note that in this case the subscribers will be informed at least 12 months before revocation.
- The issuing CA certificate's private key has been compromised.

5.4.9.2. Who can request revocation

The main responsibility lies with the first two actors.

- The certificate holder (subject)
- A mandated person of the subscriber's organization. These persons can also be considered certificate holders, for example in the case of a non-personal certificate or a certificate that does not identify a physical person in the certificate's subject.
- If the subject is a physical person certified as belonging to an organization and this organization is the subscriber, then a mandated person of the subscriber's organization has the responsibility to request revocation in case the certified person is leaving the organization.

Depending on the circumstances leading to the revocation the revocation request can also be made by:

- A RA or LRA having taken part in the registration of the concerned certificate
- The CSP (represented by the Certipost CErtification PRactices Council (CEPRAC))
- A mandated person representing the CA
- An authorized legal authority

5.4.9.3. Procedure for revocation request

Revocation requests are submitted after adequate authentication and authorization of the requestor.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

The revocation procedures that are set forth in this CPS and the applicable CP will be in accordance with the applicable law. The certificate holder and, if applicable, the legal representative of the Organization (or his authorized delegate) will be notified of the revocation.

In case the Certificate has been revoked due to CA compromise or operator errors, CA will provide, free of charge, a new equivalent certificate to the subscriber.

The request for revocation shall be recorded and archived. All relevant information about the Certificate will stay archived for a period as specified in the CP.

Once a certificate is definitively revoked (i.e., not suspended), it shall not be reinstated.

5.4.9.4. Revocation request grace period

The revocation request must be made as soon as possible if the reason for revocation include the invalidity of the certified data or the possible (future) compromise of the private key, at maximum after 12 hours if the requestor is not subject to Force Majeure.

The CSP shall not be held responsible for unauthorized use of a certificate's private key during the revocation request grace period or afterwards.

5.4.9.5. Time within which CA must process the revocation request

This is determined by the CP.

Revocation management services are available 24 hours per day, 7 days per week. Upon system failure, service failure or other factors that are not under the control of the CA, the CA shall make best endeavors to ensure that this service is not unavailable for an unreasonable long period of time.

5.4.9.6. Revocation checking requirement for relying parties

Revocation status information is available 24 hours per day, 7 days per week. Upon system failure, service or other factors that are not under the control of the CA, the CA shall make best endeavors to ensure that this information service is not unavailable for an unreasonable long period of time.

The integrity and authenticity of the status information in the CRL is ensured by the fact that this CRL is electronically signed by the issuing CA.

Revocation status information is also publicly and internationally available on http://status.pki.certipost.com/

The relying party must take into account a grace period for the revocation period which includes:

- A grace period for the propagation delay (between the reporting of the revocation request and the actual availability of up-to-date revocation information for relying parties). In practice this will be the CRL issuance frequency.
- A grace period for the delay in between a cause for revocation existed (e.g. the device holding the private key has been stolen) and the actual reporting. In practice it will not always be possible for the certificate holder or mandated person to make a report to the revocation service immediately.

The relying party may choose to accept the risk of not applying a grace period either in general of for a first checking of validity for either of the above components. The CSP is not responsible if the relying party suffers damages due to outdated validity data in the case the relying party chose not to take a grace period into account for either initial checking or a later (re-)validation.

5.4.9.7. CRL issuance frequency (if applicable)

The CRL issuance frequency is determined by the CP. It shall be at least every twenty-four (24) hours.

5.4.9.8. Maximum latency for CRLs (if applicable)

The CRL maximum latency is determined by the CP.

5.4.9.9. On-line revocation/status checking availability

In general On-line revocation/status checking is not available. OCSP (Online Certificate Status Protocol) services may be additionally provided, see applicable CP and Certificate content for details

5.4.9.10. On-line revocation checking requirements

Not applicable.

5.4.9.11. Other forms of revocation advertisements available

If allowed by the CP, suspension / revocation status information is also publicly and internationally available on www.e-trust.be/en/x500.

5.4.9.12. Special requirements key compromise

If the reason for requesting revocation is key compromise, the requestor should make the request with a minimum of delay. It must be noted though that the CSP does not record the reason for the revocation request and neither does the CRL include this type of information.

5.4.9.13. Circumstances for suspension

Any circumstance that may lead to the need for revocation and any circumstance in which requester chooses to temporarily suspend the certificate in order to prevent the use of the certificate during a certain time, can be considered as a valid reason for suspension.

Example reasons for suspension are:

- The device holding the private key has been misplaced but will probably be found again
- The device holding the private key is broken
- The certificate holder has a lengthy leave during which he or she will not make use of the certificate
- A payment as agreed in the contract between Certipost and the subscriber has not been made

5.4.9.14. Who can request suspension

- The certificate holder (subject)
- A mandated person of the subscriber's organization
- A RA or LRA having taken part in the registration of the concerned certificate
- The CSP (represented by the Certipost CErtification PRactices Council (CEPRAC))
- An authorized administrator of the CSP or acting for the CSP
- A mandated person representing the CA
- An authorized legal authority

5.4.9.15. Procedure for suspension request

Suspension requests are submitted after adequate authentication and authorization of the requestor.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

The suspension / un-suspension procedures that are set forth in this CPS and the applicable CP will be in accordance with the applicable law. The certificate holder and, if applicable, the legal representative of the Organization (or his authorized delegate) will be notified of the suspension.

The request for suspension shall be recorded and archived. All relevant information about the Certificate will stay archived for a period as specified in the CP.

A suspended certificate can be un-suspended by the same parties that can request the suspension in accordance with the CP.

Un-suspension requests are submitted after adequate authentication and authorization of the requestor.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

The request for un-suspension shall be recorded and archived. All relevant information about the Certificate will stay archived for a period as specified in the CP.

5.4.9.16. Limits on suspension period

The limits on the suspension period are determined by the CP.

5.4.10. Certificate status services

5.4.10.1. Operational characteristics

The CRL status checking shall take place by downloading the relevant CRL from the web site specified in the CP.

5.4.10.2. Service availability

Revocation status information is available 24 hours per day, 7 days per week. Upon system failure, service or other factors that are not under the control of the CA, the CA shall make best endeavors to ensure that this information service is not unavailable for an unreasonable long period of time.

5.4.10.3. Optional features

Not applicable.

5.4.11. End of subscription

The end of subscription is the result of either a contractual agreement with a stipulated end time or condition which automatically ends the subscription (like a payment that has not been made after a maximum grace period) or a new agreement made between the subscriber and Certipost.

If the end of subscription occurs before the certificate has been revoked, the certificate will be revoked as soon as the subscription is being ended. This is due to the fact that the certificate cannot be revoked anymore in the future if this would be needed. If the end of subscription is after this, and no new certificate has been produced, the certificate does not need to be revoked and simply remains expired.

5.4.12. Key escrow and recovery

5.4.12.1. Key escrow and recovery policy and practices

There are three types of key recovery supported by this CPS:

- Recovery of an archived key by the certificate holder (e.g. subject) in case of a personal certificate
- Recovery of an archived key of a personal certificate by mandated person of Certipost
- Recovery of an archived key by mandated person belonging to an organization in the case of group-managed non-personal certificates

Whether any of the above is allowed is determined by the CP.

If the CP allows the archiving of a private key, then the archiving takes place automatically and securely as soon as the key is generated.

The private key is stored in a secure key archive encrypted by a master key which can only be exported and revealed in a restrictive procedure under special circumstances such as dual control.

A valid approach of how this can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.4.12.2. Session key encapsulation and recovery policy and practices

For all types of key recovery actions the parties involved must be authenticated and authorized securely and all events need to be traced in secure audit trails.

Recovery of an archived key of a personal certificate by mandated person of Certipost must take place under "dual control" where both an authorized requester and authorized approver exist. Before the requester can recover the private key the approver needs to approve this. In this case, segregation of duties is strict.

In general the circumstance for such a recovery is a request by a recognized authority which can demonstrate the legal right to make such a request and for the purpose of a legal investigation.

The Certipost CErtification PRactices Council (CEPRAC) determines which persons are authorized to fulfill the roles above and which conditions and procedures need to be adhered to.

5.5. Facility, management, and operational controls

Note: Different functions that support the CSP may be outsourced to specialized partners. In that case the controls in this section may vary and are described in more detail in the documentation of the outsourced service providers. However, Certipost is the sole CSP. And thus the minimal required controls may be exceeded but must be met.

The methods employed to achieve the controls below are described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement) internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.5.1. Physical controls

The Certificate Authorities in scope of this CPS have the following minimal physical controls.

5.5.1.1. Site location and construction

The CSP implements physical controls on its own, leased or rented premises.

The infrastructure is logically separated from any other certificate management infrastructure, used for other purposes.

5.5.1.2. Physical access

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

5.5.1.3. Power and air conditioning

Power and air conditioning have built-in redundancy to avoid a failure of the infrastructure due to the loss of power or extreme temperatures.

5.5.1.4. Water exposures

Physical sites are protected from water exposure.

5.5.1.5. Fire prevention and protection

The CSP implements prevention and protection as well as measures against fire exposures.

5.5.1.6. Media storage

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

5.5.1.7. Waste disposal

Waste disposal is controlled and any material that contains confidential or private data is destroyed sufficiently to prevent data exposure.

5.5.1.8. Off-site backup

The CPS implements a partial off-site backup.

5.5.2. Procedural controls

5.5.2.1. Trusted roles

The internal security policies define trusted roles for security sensitive tasks.

5.5.2.2. Number of persons required per task

The internal security policies define the number of persons required per task.

5.5.2.3. Identification and authentication for each role

Each trusted role is duly identified and authenticated.

5.5.2.4. Roles requiring separation of duties

The internal security policies define the Roles requiring separation of duties.

Where dual control is required at least two trusted members of the staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

5.5.3. Personnel controls

5.5.3.1. Qualifications, experience, and clearance requirements

The CSP implements personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties. The CSP obtains a signed statement from each member of staff for maintaining confidentiality and protecting personal data.

5.5.3.2. Background check procedures

The CSP conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness.

5.5.3.3. Training requirements

The CSP organizes training that provides reasonable assurance of the trustworthiness and competence of the members of the staff.

5.5.3.4. Retraining frequency and requirements

The CSP organizes retraining that provides reasonable assurance of the trustworthiness and competence of the members of the staff.

5.5.3.5. Job rotation frequency and sequence

The internal security policies define any job rotation frequencies if needed.

5.5.3.6. Sanctions for unauthorized actions

The CSP ensures that all actions with respect to the Certipost CAs and the other CSP services can be attributed to the system and the person that has performed the action. The CSP appropriately sanctions any unauthorized action.

5.5.3.7. Independent contractor requirements

Independent contractors performing tasks of trusted roles or tasks that may endanger the security of the CSP are subject to the same personnel control requirements as internal staff.

5.5.3.8. Documentation supplied to personnel

Personnel are supplied with sufficient documentation in order that they can perform their duties in a satisfactory way.

5.5.4. Audit logging procedures

5.5.4.1. Types of events recorded

The types of events that are recorded in audit logs are (non-limitative):

- Tasks performed by users in any role (this includes operators and administrators)
- Tasks performed by automated services and applications
- The creation and status changes of the Certipost certificates
- Other transaction requests together with record of the requesting identity, type of request, indication of whether the transaction was completed or not and eventual reason why the transaction was not completed.
- The creation of public registry entries

5.5.4.2. Frequency of processing audit log

All the information that is mentioned in section 5.5.4.1 of this CPS is processed on-line.

5.5.4.3. Retention period for audit log

Audit logs will be retained for a period of up to 30 years depending on the CP.

5.5.4.4. Protection of audit log

Logs created by the CA/RA components of the Certipost Infrastructure are adequately protected.

Only dedicated internal Certipost qualified staff members and duly (sub-)contracted and authorized personnel are allowed to process these files.

Access control is restricted to the database access and physical location access to which only authorized people have access.

5.5.4.5. Audit log backup procedures

The back-up of the application audit log files is done with an adequate frequency.

The back-up location is protected with similar security level measures as the principal location.

5.5.4.6. Audit collection system (internal vs. external)

Both are used.

5.5.4.7. Notification to event-causing subject

Not applicable.

5.5.4.8. Vulnerability assessments

Security Information and Event Management tools are deployed when needed.

5.5.5. Records archival

5.5.5.1. Types of records archived

All audit data, mentioned in the previous section, is archived.

In addition, all certificate application information, and documentation supporting certificate applications must also be archived. This may include, if applicable, the signed registration forms (contractual agreements) from subscribers' applications for Certificates.

Furthermore the following information pertaining to the Certificate Authorities are archived:

- Electronic Certificate requests.
- Contents of issued Certificates.
- Records on CA re-keying including key identifiers and cross Certificates.
- Records on cross certification including the inquiry for cross certification and the performed actions.
- CRL's.
- Results of an audit or assessment.
- Current and former CPs and CPS's.

5.5.5.2. Retention period for archive

The retention period for archives depends on the CP.

5.5.5.3. Protection of archive

The archive is protected for a reasonable level against data loss, loss of integrity and loss of confidentiality.

5.5.5.4. Archive backup procedures

These procedures are described in internal documentation.

5.5.5.5. Requirements for time-stamping of records

The archive employs the most suitable techniques for integrity protection.

5.5.5.6. Archive collection system (internal or external)

Archive collection applies to both internal and external sources.

5.5.5.7. Procedures to obtain and verify archive information

The CSP specifies the procedures to obtain and specify archive information in internal documents.

5.5.6. Key changeover

5.5.6.1. CA keys

- A new CA root key generation process is initiated. (see section 5.6.1 of the present CPS);
- Note that an overlap occurs between the old and new root key: If the greatest Subscribers' certificates' validity time is X, new CA keys are generated and used to sign all the new requested Certificates, at least X before the end of validity of the old CA keys. This avoids the case where a Certificate is still valid but the corresponding CA key is no more valid.

5.5.6.2. User keys

Not applicable: the regular re-key procedures apply.

5.5.6.3. Cross-certification keys

Not applicable.

5.5.7. Compromise and disaster recovery

5.5.7.1. Incident and compromise handling procedures

This is described in internal documents.

5.5.7.2. Computing resources, software, and/or data are corrupted

These sources are backed up and/or foreseen to enable the resumption of the CA in due time.

5.5.7.3. Entity private key compromise procedures

This is described in internal documents. Such an incident will be communicated without reasonable delay and necessary steps will be taken.

5.5.7.4. Business continuity capabilities after a disaster

A Business Continuity Plan is foreseen to enable the resumption of the CA in due time.

5.5.8. CA or RA termination

a) Transfer of services from one organization to another organization, or the CA service pass over from an old CA key to a new CA key are not considered as CA Termination.

b) In the event that all the CA services are to be interrupted, suspended or terminated, i.e. the situation where all services associated with a CA is terminated permanently, Certipost shall send notification to all Subscribers to ensure the availability of the archive and the current Certificates.

c) Before the CA terminates its services the following procedures have to be completed as a minimum:

- Inform all Subscribers, cross-certifying CA's and Relying Parties with which the CA has agreements or other form of established relations.
- Inform the legally established Administration of the termination and its possible consequences.
- Realize the assumption of the take-over of its activities by another CA of the same quality and security level; if this is not possible, revoke the Certificates two (2) months after having informed the Subscribers and archive all relevant Certificate information during 30 years.
- If possible, make publicly available information of its termination at least 3 month prior to termination.
- Terminate the revocation checking service for all Certificates issued under the terminated issuing keys. This will stop any of these Certificates from being accepted by any relying party who follows proper revocation checking procedures according to section 4.4 of this CPS.
- Terminate all authorizations of subcontractors to act on behalf of the CA in the process of issuing Certificates.

d) The CA shall forecast arrangement to cover the costs to fulfill these minimum requirements in case the CA becomes bankrupt or for other reasons is unable to cover the costs by itself.

RA termination, when referring to LRA, is handled in RA agreements. In such a case the CA and also in case of the central RA termination, the CA will take over the obligations of the RA concerning evidence archiving or outsource these to a suitable CSP which complies with this CPS. Otherwise the same conditions and procedures – where relevant – apply as in the case of CA termination.

5.6. Technical security controls

5.6.1. Key pair generation and installation

5.6.1.1. Key pair generation

CA certificate key pair generation is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

For the Certipost's CAs' keys' generation, this shall be undertaken in a physically secure environment by personnel in trusted roles under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices. The keys that are encrypting the

CA backup keys, are split in several parts that cannot be used alone to decrypt the CA back-up keys. After this initialization step, access rights granted to the previously authorized persons are retracted and can only be reinstated again after approval of the Certipost CErtification PRactices Council (CEPRAC).

If the Subscriber generates its keys: to generate their cryptographic key pairs, and to use them properly, Subscribers are obliged to use reliable technical means that present an adequate security level in order to, among others, prevent or detect any integrity flaw to a piece of data that has been encrypted or decrypted with the keys and to prevent or detect any unauthorized usage of a Private Key. In particular, the Subscriber is obliged to generate its keys using a key generation algorithm, a key length, and a signature algorithm recognised as being fit for the purposes of certificate usage. If the CP requires use of an SSCD and the Subscriber generates its keys, then the key shall be created within an SSCD.

The allowed methods of key pair generation and the minimal requirements for end-entity certificates are determined by the CP.

5.6.1.2. Private key delivery to subscriber

Delivery of the private key depends on the type and level of the generation.

In general, if there is need for delivery, this delivery should be secure – protecting the integrity, authenticity and confidentiality of the private key.

For Qualified certificates, the private key must be generated on the SSCD of the certificate holder and must not be delivered in any other way.

If allowed by the CP, an exception could be that the private key is generated during a key ceremony on the secure HSM of the subscriber or a secure HSM which sufficiently guarantees that the private key never leaves the secure HSM and can only be used by the subscriber.

If the Private/Public Key pair is generated by the CSP (e.g., at LRA premises), the Private Key can be provided by:

- SSCD delivery: provided that processes are in place to ensure that the SSCD can only be used by the SSCD holder (subject) with the private key.
- Secure connection: for assurance levels Normalized and lower
- CD-ROM or memory stick: for assurance levels Normalized and lower, provided the private key is protected with a password (in conformance with the password policy) which will only be known by the subscriber.
- By e-mail: for assurance levels Lightweight and lower, provided the private key is protected with a password (in conformance with the password policy) which will only be known by the subscriber.

A valid approach of how private key delivery can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.6.1.3. Public key delivery to certificate issuer

There are different ways to deliver a Certificate signing requests depending on the CP. All are based on PKCS#10 requests in DER or PEM format:

- A PKCS#10 submitted from a Private Key Holding Device, a SCD or SSCD via a secure channel which protects the authenticity of origin of the request, the integrity and the confidentiality
  - In case of an SSCD used by a qualified certificate, the SSCD itself must be authenticated
- A PKCS#10 submitted via a secured online web form by a Subscriber which identity is authenticated;
- A PKCS#10 on a memory stick or floppy-disk delivered in person by the Subscriber to the LRA;
- A PKCS#10, included in an e-mail, signed by the Subscriber private key that was previously certified, provided the related certificate is still valid.
- A PKCS#10, signed by the Subscriber private key that was previously certified, provided the related certificate is still valid. This is only possible when using an electronic re-key possibility and when authorized in the applicable CP.

5.6.1.4. CA public key delivery to relying parties

The CA Public Keys are published on the Certipost Public Registry and Certipost e-Certificates web-site.

5.6.1.5. Key sizes

It is advised forcertificates to have a key size (RSA) of minimum 2048 bits. However, for specific applications, other key lengths could be specified in the CP.

5.6.1.6. Public key parameters generation and quality checking

Public Key RSA exponents are chosen with security considerations.

The Public Key module generation is done with state of the art parameter generation technology.

CA components of the Certipost PKI use Hardware Security Modules (HSM) that includes internal key pair generation. In this case the key is inside the HSM and cannot be retrieved in the clear. HSM devices used by Certipost are FIPS 140-1 level 3.

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

Each CA key pair key pair has the key usage "Signing Certificates and CRL's" enabled in the corresponding certificate and is only used for the purpose of generating Certificates and CRL's, as defined in section 7.3.3 of ETSI TS 101 456, within physically secure premises.

The X.509v3 Certificates issued by the CA contain the Key Usage Certificate extension, restricting the purpose to which the Certificate can be applied, in compliance with the CP under which the Certificate is issued. See applicable CP for details.

5.6.2. Private Key Protection and Cryptographic Module Engineering Controls

5.6.2.1. Cryptographic module standards and controls

CA key generation shall be carried out within a device which either:

- meets the requirements identified in FIPS 140-2 [3], level 3 or higher; or

- meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [6],

CWA 14167-3 [7] or CWA 14167-4 [8]; or

- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [4], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

NOTE 1: The rules of clause 7.2.2 (b to e) apply also to key generation even if carried out in a separate system.

Certification authority key generation shall be performed using an algorithm recognized as being fit for the purposes of qualified certificates;

The selected key length and algorithm for CA signing key shall be one which is recognized as being fit for the purposes of qualified certificates as issued by the CA;

NOTE 2: See TS 102 176-1 [14] for guidance on algorithms and their parameters.

A suitable time before expiration of its CA signing key (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy.

NOTE 3: These operations should be performed timely enough to allow all parties that have relationships with the CA (subjects, subscribers, relying parties, higher level CAs, etc.) to be timely aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a CA which will cease its operations before its own certificate-signing certificate

The HSM's that are used by the CA components of the Certipost PKI segment are FIPS 140-1 Level 3. These HSM's are also EAL4+ Common Criteria certified.

For Cryptographic modules for subscribers the CA closely follows the relevant standards (like ETSI TS 14169) where applicable for different private key holding devices. The following categories are identified:

- SSCD requirements
- SCD requirements
- SUD requirements
- Other user device or non-personal device requirements

The CP determines which type must be minimally used.

In any case, Subscribers are obliged to protect their Private Key at all times, against loss, disclosure, modification and unauthorized use, in accordance with this CPS and the related CP. From the creation of their key pair, Subscribers are personally and solely responsible of the confidentiality and integrity of their Private Keys. Every usage of their Private Key is assumed to be the fact of its owner. The PIN or password, used to protect against unauthorized use of the Private Key shall never be stored in the same location as the Private Key itself or next to its storage media, shall never be stored unprotected, and shall give sufficient protection. Subscribers shall not leave their Private Key unattended in an unlock state (i.e., unattended in a workstation when the PIN or password has been entered).

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

The Private Keys of the Certipost CA's are encrypted by a Storage Master Key (SMK), a strong encryption key that is split-up over smart cards that are protected with multiple password (shares) protects all roots. A certain number of shares ('N' out of 'M') out of the total shares held by different operators (or managers depending on security level) need to be available to restart an engine.

5.6.2.3. Private key escrow

Not applicable.

5.6.2.4. Private key backup

When outside the secure cryptographic device the CA private signing keys shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device;

The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secure environment. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices;

Backup copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use;

Where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.

5.6.2.5. Private key archival

Upon expiration of a Certipost CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 1 year using the hardware cryptographic modules that meet the security requirements of this CPS. These CA key pairs shall not be used for any signing events after their expiration date, unless the CA Certificate has been renewed in terms of this CPS;

If required and allowed (see applicable CP) the Certificate Holders' private encryption keys will be securely archived within the Certipost CA infrastructure in accordance with this CPS;

The private keys used for electronic signatures should never be archived; In case of Qualified Certificates, key archival is strictly prohibited

Access to the Certificate Holder's private key (key recovery) by an entitled authority requires dual control:

For the recovery of a private key the strongly-authenticated request of an authorized person, acting on behalf of the authority that is entitled to demand the key recovery, must be approved by strongly-authenticated and authorized Security Officer. The recovery must happen in a secure way in order that only the entitled authority can get access to the private key.

For the recovery of a private key by the certificate holder(s), a strongly-authenticated and authorized request is required. The recovery must happen in a secure way in order that only the certificate holder(s) can get access to the private key.

A valid approach of how private key delivery can be achieved is described in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.6.2.6. Private key transfer into or from a cryptographic module

This depends on the CP. Private key transfer must happen in a sufficiently secure way to meet the requirements of the CP. The procedure is described in internal documents.

5.6.2.7. Private key storage on cryptographic module

This depends on the CP. Private key storage on a cryptographic module must happen in a sufficiently secure way to meet the requirements of the CP. The procedure is described in internal documents.

5.6.2.8. Method of activating private key

There are 2 types of methods of activating private key supported:

Private Key activation by a person: for personal certificates, this is the mandated method. The private key is activated each time the PIN code is correctly entered or a similarly strong level or stronger level of authentication is attained by the certificate and key holder.

Private Key activation by a service: for non-personal certificates. The private key is activated automatically each time a strongly authenticated request accesses the service.

5.6.2.9. Method of deactivating private key

Private Keys are always deactivated after each activation and subsequent use.

5.6.2.10. Method of destroying private key

Private Key destruction requires that the private key data does not exist anymore in any way. This can happen by fully erasing the memory where the key is stored or by physically destroying the device that holds the Private Key, provided that the destruction is such that the private key can never be extracted or used anymore.

A logical destruction of the private key is discussed in internal documents, which can be made available to auditors or other parties after the approval of CEPRAC and under the conditions defined by CEPRAC (such as the signing of a Non-Disclosure Agreement).

5.6.2.11. Cryptographic Module Rating

The CSP defines the following levels of Cryptographic Module Rating:

- SSCD: The requirements are defined by the relevant CEN/ETSI Technical Specifications and EN standards.
- SCD: The requirements are defined by the relevant CEN/ETSI Technical Specifications and EN standards.
- SUD: The requirements are defined by the relevant CEN/ETSI Technical Specifications and EN standards.
- Private Key Holding Device: The requirements, though they are not strict, are defined by the relevant CEN/ETSI Technical Specifications and EN standards.

5.6.3. Other aspects of key pair management

5.6.3.1. Public key archival

Public key archival – where required – meets the requirements of 5.5.5

5.6.3.2. Certificate operational periods and key pair usage periods

The maximum periods are defined by the CP. Shorter periods may be selected at the discretion of the requestor, wherever the CP allows this.

5.6.4. Activation data

5.6.4.1. Activation data generation and installation

Activation data generation and installation meets the requirements to protect the security of the activation data. The details are discussed in internal documents.

5.6.4.2. Activation data protection

Activation data protection meets the requirements to protect the security of the activation data. The details are discussed in internal documents.

5.6.4.3. Other aspects of activation data

Not applicable.

5.6.5. Computer security controls

5.6.5.1. Specific computer security technical requirements

These are described in internal documents.

5.6.5.2. Computer security rating

Computer security rating is such that the security meets the required level defined by the relevant CP.

5.6.6. Life cycle technical controls

5.6.6.1. System development controls

The controls are such that the security meets the required level defined by the relevant CP.

5.6.6.2. Security management controls

The controls are such that the security meets the required level defined by the relevant CP.

5.6.6.3. Life cycle security controls

The controls are such that the security meets the required level defined by the relevant CP.

In particular, for certificate generation, the CSP shall ensure that:

- Certificate and revocation status information signing cryptographic hardware is not tampered with during shipment
- Certificate and revocation status information signing cryptographic hardware is not tampered with while stored
- The installation, activation, back-up and recovery of the CA's signing keys in cryptographic hardware shall require dual control of at least two trusted roles
- Certificate and revocation status information signing cryptographic hardware is functioning correctly
- CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement

In particular, if the CA issues a SSCD:

- The SSCD preparation shall be securely controlled by the service provider
- The SSCD shall be securely stored and distributed whenever the storage or distribution could possibly lead to key compromise or misuse of the SSCD
- SSCD deactivation and reactivation shall be securely controlled
- Where the SSCD has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure signature-creation device. This may be achieved by ensuring distribution of activation data and delivery of SSCD via a different route and medium.

5.6.7. Network security controls

The CSP shall ensure that:

- Network components are kept in a physically secure environment and their configurations periodically audited for compliance with the requirements specified by the CSP
- Continuous monitoring and alarm facilities shall be provided to enable the CSP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources. This may use, for example, an intrusion detection system, access control monitoring and alarm facilities.

5.6.8. Time-stamping

When specified time-stamping can be employed to protect the integrity of archives.

5.7. Certificate, crl, and ocsp profiles

5.7.1. Certificate profile

Certificates issued under this CPS shall be constructed according to ISO 9594-8 (X.509).

Inclusion of data elements in Certificates shall be consistent with the applicable CP.

Content of the certificates are given in the applicable CPs.

5.7.1.1. Version number(s)

Certificates issued under this CPS are X.509 version 3 Certificates.

5.7.1.2. Certificate extensions

5.7.1.2.1. Root CA and Issuing CA certificates

- **Baltimore CyberTrust Root**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 33554617 (0x20000b9)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
        Validity
            Not Before: May 12 18:46:00 2000 GMT
            Not After : May 12 23:59:00 2025 GMT
        Subject: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:a3:04:bb:22:ab:98:3d:57:e8:26:72:9a:b5:79:
                    d4:29:e2:e1:e8:95:80:b1:b0:e3:5b:8e:2b:29:9a:
                    64:df:a1:5d:ed:b0:09:05:6d:db:28:2e:ce:62:a2:
                    62:fe:b4:88:da:12:eb:38:eb:21:9d:c0:41:2b:01:
                    52:7b:88:77:d3:1c:8f:c7:ba:b9:88:b5:6a:09:e7:
                    73:e8:11:40:a7:d1:cc:ca:62:8d:2d:e5:8f:0b:a6:
                    50:d2:a8:50:c3:28:ea:f5:ab:25:87:8a:9a:96:1c:
                    a9:67:b8:3f:0c:d5:f7:f9:52:13:2f:c2:1b:d5:70:
                    70:f0:8f:c0:12:ca:06:cb:9a:e1:d9:ca:33:7a:77:
                    d6:f8:ec:b9:f1:68:44:42:48:13:d2:c0:c2:a4:ae:
                    5e:60:fe:b6:a6:05:fc:b4:dd:07:59:02:d4:59:18:
                    98:63:f5:a5:63:e0:90:0c:7d:5d:b2:06:7a:f3:85:
                    ea:eb:d4:03:ae:5e:84:3e:5f:ff:15:ed:69:bc:f9:
                    39:36:72:75:cf:77:52:4d:f3:c9:90:2c:b9:3d:e5:
```

```
                c9:23:53:3f:1f:24:98:21:5c:07:99:29:bd:c6:3a:
                ec:e7:6e:86:3a:6b:97:74:63:33:bd:68:18:31:f0:
                78:8d:76:bf:fc:9e:8e:5d:2a:86:a7:4d:90:dc:27:
                1a:39
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:3
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: sha1WithRSAEncryption
        85:0c:5d:8e:e4:6f:51:68:42:05:a0:dd:bb:4f:27:25:84:03:
        bd:f7:64:fd:2d:d7:30:e3:a4:10:17:eb:da:29:29:b6:79:3f:
        76:f6:19:13:23:b8:10:0a:f9:58:a4:d4:61:70:bd:04:61:6a:
        12:8a:17:d5:0a:bd:c5:bc:30:7c:d6:e9:0c:25:8d:86:40:4f:
        ec:cc:a3:7e:38:c6:37:11:4f:ed:dd:68:31:8e:4c:d2:b3:01:
        74:ee:be:75:5e:07:48:1a:7f:70:ff:16:5c:84:c0:79:85:b8:
        05:fd:7f:be:65:11:a3:0f:c0:02:b4:f8:52:37:39:04:d5:a9:
        31:7a:18:bf:a0:2a:f4:12:99:f7:a3:45:82:e3:3c:5e:f5:9d:
        9e:b5:c8:9e:7c:2e:c8:a4:9e:4e:08:14:4b:6d:fd:70:6d:6b:
        1a:63:bd:64:e6:1f:b7:ce:f0:f2:9f:2e:bb:1b:b7:f2:50:88:
        73:92:c2:e2:e3:16:8d:9a:32:02:ab:8e:18:dd:e9:10:11:ee:
        7e:35:ab:90:af:3e:30:94:7a:d0:33:3d:a7:65:0f:f5:fc:8e:
        9e:62:cf:47:44:2c:01:5d:bb:1d:b5:32:d2:47:d2:38:2e:d0:
        fe:81:dc:32:6a:1e:b5:ee:3c:d5:fc:e7:81:1d:19:c3:24:42:
        ea:63:39:a9
```

- **Verizon Global Root CA**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Verizon Business, OU=OmniRoot, CN=Verizon Global Root CA
        Validity
            Not Before: Jul 30 14:27:04 2009 GMT
            Not After : Jul 30 14:27:04 2034 GMT
        Subject: C=US, O=Verizon Business, OU=OmniRoot, CN=Verizon Global Root CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:8a:00:0c:70:1d:bf:eb:34:86:c3:99:45:35:1e:
                    7f:43:f7:ab:6f:24:2d:cd:19:c2:10:bb:b0:ca:29:
                    5b:a9:20:ab:ab:72:2c:c4:e2:02:39:6d:82:b8:c5:
                    11:ea:f8:fb:b3:9e:62:f8:33:1e:b0:1f:c9:e3:f6:
                    37:db:04:c8:3b:63:4f:36:e2:85:a4:25:1d:c7:69:
                    1f:04:bd:68:45:13:96:07:1f:94:50:f5:3e:c5:27:
                    54:9e:c0:49:57:44:8e:07:63:d4:a6:ae:ed:22:99:
                    cc:4d:96:69:04:13:6e:76:89:9f:74:16:94:f9:1d:
                    54:bd:a2:b9:d2:83:01:22:0c:4d:44:80:aa:fe:35:
                    89:27:25:a7:86:89:c6:d5:1a:92:e3:8f:c5:95:a0:
                    14:72:9a:e8:56:c5:02:55:1c:97:f9:20:2e:d0:f5:
                    3c:13:19:5a:f6:e1:f9:0b:03:82:69:a7:8c:b7:d6:
                    6f:9c:56:3e:9d:e8:2a:09:60:6d:4b:e6:fb:8b:99:
                    14:f7:34:4f:65:59:80:8d:b9:57:c8:a2:35:21:d8:
                    88:71:56:5d:ee:82:57:2d:26:90:18:9f:9a:9c:9c:
                    8f:ef:d4:c5:63:a7:54:7d:47:91:87:7d:1a:12:a8:
                    1b:18:6f:a9:6f:b1:27:ba:e4:04:74:ce:37:1e:7f:
```

```
                66:c5
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                4C:38:11:B8:98:00:5B:5A:2B:70:3E:AA:78:E4:D5:67:67:67:A7:7E
    Signature Algorithm: sha256WithRSAEncryption
        01:5f:a0:b1:06:01:f4:79:d7:65:18:60:3e:cf:79:a0:ba:c2:
        23:4f:23:df:87:96:5f:81:0e:38:15:2e:5c:c8:02:68:29:20:
        fc:8b:ee:a5:8a:18:81:64:5c:98:35:7e:39:30:82:a4:82:8a:
        50:b5:ba:c3:e8:5a:d6:a8:9e:e2:c3:17:db:db:c4:eb:b0:0a:
        20:0d:e9:9e:e3:ff:60:54:47:f1:3b:9d:d4:28:3c:a2:ae:a3:
        fb:aa:8b:82:22:2a:35:87:90:b8:1c:59:47:90:d5:9d:2e:fa:
        49:e3:65:a8:36:eb:c7:e4:1c:68:dc:b3:31:6c:ab:4e:ce:24:
        80:15:c8:10:59:10:11:72:4d:7a:9c:98:9c:c4:fc:61:e0:b3:
        b2:9d:4e:a0:c6:c2:59:ab:18:d6:a2:55:45:ec:29:aa:25:37:
        d6:4e:4a:3d:0b:40:c1:e4:93:e4:fc:cd:91:0b:f8:e6:ab:cc:
        b3:76:c4:62:bf:19:ed:86:b6:79:c3:29:54:54:bc:99:7d:46:
        57:cf:a6:cf:f4:54:2a:9a:03:65:47:01:a1:42:2a:cb:25:47:
        6e:7c:5e:00:4b:91:d9:f9:1b:10:06:70:f9:42:15:a6:5f:aa:
        d7:40:1e:fd:c9:48:9d:97:81:ea:5c:68:c2:a0:e7:89:a1:53:
        4d:bf:c7:e3
```

- **Certipost Public CA for Qualified Signatures (signed by "Baltimore CyberTrust Root")**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 120024006 (0x7276bc6)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
        Validity
            Not Before: Jan 11 19:15:25 2012 GMT
            Not After : Jan 11 19:15:04 2022 GMT
        Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Public CA for Qualified Signatures
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:a3:0d:eb:9a:e6:4a:64:c9:c6:85:04:46:78:4c:
                    d9:2b:84:c7:7a:ae:7d:08:8a:8a:e8:1b:1e:4b:12:
                    e6:67:7b:21:f3:39:d8:d0:50:4d:2b:83:97:98:51:
                    23:d1:8f:7d:42:72:32:00:9c:67:53:96:dc:bd:24:
                    81:15:02:8f:c2:d0:f9:70:57:26:a5:cc:8f:ec:14:
                    4e:8b:af:cc:c8:90:84:e8:13:03:f3:07:12:eb:50:
                    89:7c:b9:66:f3:fa:7f:55:11:7d:2a:c0:df:6b:a7:
                    cc:77:f5:b5:82:16:ea:ef:c3:b0:6b:6d:be:52:05:
                    e9:16:bd:bb:7a:a0:42:b1:4c:c4:89:9c:9a:e5:c2:
                    0b:59:73:0e:86:63:fe:64:4d:ce:8b:ba:4b:67:f0:
                    e1:fb:9d:2d:9f:f4:7e:3f:42:15:04:12:32:a6:2c:
                    9c:9f:1f:ee:e1:0f:f5:a0:4a:8c:cb:2f:83:17:58:
                    ae:31:f0:9b:0a:91:36:3d:bc:33:d1:1f:92:0a:a9:
                    45:35:e4:4e:f5:d9:5f:98:9e:57:96:94:ab:e4:ae:
                    dd:29:72:4f:f0:38:28:33:0f:02:bb:97:c6:2d:4f:
                    33:da:ac:2a:c7:ed:d9:bc:e5:dd:c4:33:45:7b:68:
                    3c:1c:75:f8:59:d3:32:9a:14:b3:6e:69:cb:8c:65:
                    58:ad
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Certificate Policies:
Policy: X509v3 Any Policy
CPS: https://www.certipost.com/showpolicy

X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Authority Key Identifier:
keyid:E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

X509v3 CRL Distribution Points:
URI:http://cdp1.public-trust.com/CRL/Omniroot2025.crl

X509v3 Subject Key Identifier:
0E:37:33:C7:28:6E:BF:CE:5F:E6:2A:E6:98:90:8B:AC:C1:E6:28:44
Signature Algorithm: sha256WithRSAEncryption
41:3d:3b:54:1f:a7:4e:04:46:00:22:d7:e8:55:c0:3f:75:af:
16:de:32:b6:e9:75:a1:28:e1:7a:c9:77:ea:8b:36:5d:0a:98:
b8:61:a3:5a:14:66:c1:04:38:81:6d:05:cd:b3:60:3a:91:8e:
97:c6:04:4c:dc:d8:b6:bb:66:b0:a3:8d:ae:a7:bd:09:86:69:
b1:6c:6c:60:77:22:89:ec:91:eb:74:1e:78:55:8d:5f:ff:ca:
ab:81:e2:31:f3:66:72:ee:59:3b:f4:f8:87:9f:74:ac:f0:ae:
b2:c6:cc:92:a3:74:8d:ba:08:84:38:f6:7c:30:00:ad:e2:87:
0a:57:cb:f5:55:34:a8:5a:c8:8a:84:4e:d0:6f:ab:73:22:04:
41:fb:be:62:89:23:bf:c8:9f:11:5b:6c:31:36:b5:66:71:8d:
ee:70:8b:69:77:c6:0f:4a:8d:11:32:fb:25:74:50:7d:c2:d8:
16:b3:89:4f:68:23:62:5f:03:ed:2c:7a:52:af:bb:3d:81:69:
42:42:d9:9d:d5:b0:81:e4:bd:c4:4a:f3:bb:43:e2:f5:f6:de:
d4:d0:c1:26:18:26:3c:1d:04:59:69:dc:62:d0:ce:c5:e0:4f:
ae:cf:12:d8:e2:0a:cc:37:b4:43:9b:f6:19:16:9c:19:2e:4b:
02:16:a4:9c

- **Certipost Public CA for Qualified Signatures (signed by "Verizon Global Root CA")**

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 904 (0x388)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Verizon Business, OU=OmniRoot, CN=Verizon Global Root CA
Validity
Not Before: Jan 11 19:45:06 2012 GMT
Not After : Jan 11 19:44:34 2022 GMT
Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Public CA for Qualified Signatures
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:a3:0d:eb:9a:e6:4a:64:c9:c6:85:04:46:78:4c:
d9:2b:84:c7:7a:ae:7d:08:8a:8a:e8:1b:1e:4b:12:
e6:67:7b:21:f3:39:d8:d0:50:4d:2b:83:97:98:51:
23:d1:8f:7d:42:72:32:00:9c:67:53:96:dc:bd:24:
81:15:02:8f:c2:d0:f9:70:57:26:a5:cc:8f:ec:14:
4e:8b:af:cc:c8:90:84:e8:13:03:f3:07:12:eb:50:
89:7c:b9:66:f3:fa:7f:55:11:7d:2a:c0:df:6b:a7:
cc:77:f5:b5:82:16:ea:ef:c3:b0:6b:6d:be:52:05:
e9:16:bd:bb:7a:a0:42:b1:4c:c4:89:9c:9a:e5:c2:
0b:59:73:0e:86:63:fe:64:4d:ce:8b:ba:4b:67:f0:
e1:fb:9d:2d:9f:f4:7e:3f:42:15:04:12:32:a6:2c:
9c:9f:1f:ee:e1:0f:f5:a0:4a:8c:cb:2f:83:17:58:
ae:31:f0:9b:0a:91:36:3d:bc:33:d1:1f:92:0a:a9:

```
                45:35:e4:4e:f5:d9:5f:98:9e:57:96:94:ab:e4:ae:
                dd:29:72:4f:f0:38:28:33:0f:02:bb:97:c6:2d:4f:
                33:da:ac:2a:c7:ed:d9:bc:e5:dd:c4:33:45:7b:68:
                3c:1c:75:f8:59:d3:32:9a:14:b3:6e:69:cb:8c:65:
                58:ad
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://www.certipost.com/showpolicy

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:4C:38:11:B8:98:00:5B:5A:2B:70:3E:AA:78:E4:D5:67:67:67:A7:7E

            X509v3 CRL Distribution Points:
                URI:http://cdp1.public-trust.com/CRL/Omniroot2034.crl

            X509v3 Subject Key Identifier:
                0E:37:33:C7:28:6E:BF:CE:5F:E6:2A:E6:98:90:8B:AC:C1:E6:28:44
    Signature Algorithm: sha256WithRSAEncryption
        73:f0:57:07:07:f3:34:de:48:53:1e:3e:0a:88:33:07:6c:55:
        49:d2:75:85:54:92:f2:80:19:1c:86:5d:d7:f4:10:35:18:31:
        ac:35:f8:8d:4b:0f:6d:66:4b:15:4c:28:91:12:78:3b:c4:b3:
        42:65:a8:44:46:a2:10:8c:f6:38:a0:aa:eb:8d:42:18:10:e1:
        21:ac:5b:2c:0d:c9:7c:35:6a:d2:0c:7e:9d:83:ec:5b:22:36:
        b4:dc:af:2d:f2:87:6b:f9:7f:16:77:0b:25:7b:a3:66:52:4b:
        ea:44:bc:58:6f:b9:fa:9d:65:49:60:67:ae:3f:46:13:dc:ab:
        56:55:ef:86:ac:26:e3:41:45:9e:d2:e8:81:77:3f:1c:c0:28:
        33:7d:62:da:7c:bc:9c:35:72:cd:51:a1:2f:f4:08:9f:fa:68:
        94:bc:1e:30:5c:f3:ad:d1:8f:7f:52:b1:c2:ff:cd:95:be:29:
        a9:ef:2e:fb:c3:69:f0:82:27:f1:4d:b9:a0:3c:d1:56:23:1d:
```

- **Certipost Public CA for Persons and Organizations (signed by Baltimore Cybertrust Root)**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 120024007 (0x7276bc7)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
        Validity
            Not Before: Jan 11 19:20:15 2012 GMT
            Not After : Jan 11 19:19:50 2022 GMT
        Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Public CA for Persons and Organizations
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b2:42:b7:3c:74:a5:43:8b:51:cb:44:3d:e6:ec:
                    6f:c7:5c:c8:19:38:8b:6c:0b:7d:5b:30:4a:6c:9e:
                    a3:02:20:cb:de:32:8d:53:7f:7d:06:d5:3c:d1:c5:
                    3e:bd:ff:fa:b9:fd:7f:14:a6:75:74:81:ab:da:a4:
                    77:5d:a1:50:ef:75:fd:a4:05:bc:ef:85:4f:67:a1:
                    fe:0b:19:cc:c0:40:f2:e1:08:ec:08:1f:c1:51:c7:
                    ac:a4:5f:16:18:10:b0:d3:fa:8e:b6:fd:23:46:ce:
                    49:a6:4b:e1:95:63:39:df:83:df:6c:b5:58:e7:39:
                    2b:70:06:37:a5:09:66:03:a1:60:56:c4:c5:dc:93:
```

```
                b2:28:f8:64:9c:9b:06:ea:ac:ca:c3:b8:df:30:85:
                4a:b8:be:0c:c1:c9:a6:e7:76:e8:ff:8f:16:fd:fe:
                ea:38:e4:ca:19:8f:4e:75:b0:0b:6e:9c:24:93:8a:
                69:fb:0b:5c:5a:e6:df:7c:fb:d1:ec:f1:fc:e7:3b:
                e8:f4:87:c9:3a:5f:42:36:8c:6b:cc:ad:76:c1:f1:
                65:0b:88:e2:04:18:73:8a:55:73:76:b9:b0:02:a0:
                e0:36:1e:b8:5c:a4:6e:70:b8:5c:11:56:6f:87:fc:
                f5:a1:db:ee:ba:46:4f:e6:39:ac:eb:52:6c:82:46:
                28:cd
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://www.certipost.com/showpolicy

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

            X509v3 CRL Distribution Points:
                URI:http://cdp1.public-trust.com/CRL/Omniroot2025.crl

            X509v3 Subject Key Identifier:
                76:BD:AD:0D:3B:0D:74:29:98:BA:C4:28:B4:F1:DD:16:C5:96:5B:F4
    Signature Algorithm: sha256WithRSAEncryption
        33:01:9b:86:97:5f:e6:e3:f6:a9:8f:1e:1b:72:ae:f4:fb:84:
        92:f9:7a:40:f6:b2:e6:61:0c:5f:c8:62:13:aa:3f:1c:15:7c:
        44:ee:bd:54:e0:cb:ee:5c:c0:81:ad:c3:9a:be:53:eb:c3:ac:
        7e:9f:74:b7:ef:b2:93:6f:55:c5:64:e7:d7:f0:89:a8:83:32:
        7f:e3:4e:ec:a2:2b:62:2b:1f:0a:4c:61:70:3c:50:b5:b5:1d:
        fc:c6:1b:96:a1:b9:68:a6:4b:4f:01:a9:37:19:40:b0:d1:52:
        72:12:cb:c7:33:1d:83:97:79:25:00:ff:78:43:40:65:8c:50:
        b5:a4:56:0d:6e:a5:07:b9:8d:f3:de:72:2a:1b:40:4c:e5:04:
        37:1a:f3:ea:8f:50:7b:37:a5:ad:b8:80:7d:42:5f:2d:59:39:
        1c:3d:42:47:a4:d4:91:98:89:0e:f2:40:56:10:7d:af:07:e6:
        54:ea:57:fa:04:60:c6:a6:3d:6f:19:5e:25:8e:87:34:26:05:
        69:f1:46:5e:9f:be:de:22:ec:6d:75:02:8c:61:87:6d:da:b0:
        d6:01:7f:f3:52:d9:8f:7d:ce:d2:3c:ac:86:72:8c:82:34:fc:
        0a:10:12:5c:91:04:51:c7:3d:85:74:80:ab:84:86:33:7c:52:
        5d:ef:c0:40
```

- **Certipost Public CA for Persons and Organizations (signed by Verizon Global Root CA)**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 905 (0x389)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Verizon Business, OU=OmniRoot, CN=Verizon Global Root CA
        Validity
            Not Before: Jan 11 19:47:20 2012 GMT
            Not After : Jan 11 19:46:56 2022 GMT
        Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Public CA for Persons and Organizations
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b2:42:b7:3c:74:a5:43:8b:51:cb:44:3d:e6:ec:
                    6f:c7:5c:c8:19:38:8b:6c:0b:7d:5b:30:4a:6c:9e:
```

```
                a3:02:20:cb:de:32:8d:53:7f:7d:06:d5:3c:d1:c5:
                3e:bd:ff:fa:b9:fd:7f:14:a6:75:74:81:ab:da:a4:
                77:5d:a1:50:ef:75:fd:a4:05:bc:ef:85:4f:67:a1:
                fe:0b:19:cc:c0:40:f2:e1:08:ec:08:1f:c1:51:c7:
                ac:a4:5f:16:18:10:b0:d3:fa:8e:b6:fd:23:46:ce:
                49:a6:4b:e1:95:63:39:df:83:df:6c:b5:58:e7:39:
                2b:70:06:37:a5:09:66:03:a1:60:56:c4:c5:dc:93:
                b2:28:f8:64:9c:9b:06:ea:ac:ca:c3:b8:df:30:85:
                4a:b8:be:0c:c1:c9:a6:e7:76:e8:ff:8f:16:fd:fe:
                ea:38:e4:ca:19:8f:4e:75:b0:0b:6e:9c:24:93:8a:
                69:fb:0b:5c:5a:e6:df:7c:fb:d1:ec:f1:fc:e7:3b:
                e8:f4:87:c9:3a:5f:42:36:8c:6b:cc:ad:76:c1:f1:
                65:0b:88:e2:04:18:73:8a:55:73:76:b9:b0:02:a0:
                e0:36:1e:b8:5c:a4:6e:70:b8:5c:11:56:6f:87:fc:
                f5:a1:db:ee:ba:46:4f:e6:39:ac:eb:52:6c:82:46:
                28:cd
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://www.certipost.com/showpolicy

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:4C:38:11:B8:98:00:5B:5A:2B:70:3E:AA:78:E4:D5:67:67:67:A7:7E

            X509v3 CRL Distribution Points:
                URI:http://cdp1.public-trust.com/CRL/Omniroot2034.crl

            X509v3 Subject Key Identifier:
                76:BD:AD:0D:3B:0D:74:29:98:BA:C4:28:B4:F1:DD:16:C5:96:5B:F4
    Signature Algorithm: sha256WithRSAEncryption
        89:af:3f:3a:64:f0:50:0e:d1:ab:a0:42:ce:9a:d7:33:b8:87:
        c4:62:4c:b6:9a:95:97:4a:6b:cf:aa:bd:4d:21:4c:7f:d7:e2:
        94:88:80:5c:17:24:26:8b:a6:a5:9d:06:8e:21:88:fc:f2:63:
        e5:fc:66:af:cd:12:f5:a8:8d:2c:88:03:04:76:0b:50:e6:3c:
        55:96:bd:a7:1b:07:5c:8f:45:f2:7a:89:b4:eb:74:09:e9:33:
        6e:a2:a9:61:0a:35:40:09:9b:e3:4c:d2:b5:b8:be:b2:65:3c:
        58:34:39:ee:68:10:13:af:54:87:28:1d:a3:10:0d:41:40:2c:
        95:91:82:1e:e2:15:1b:d8:99:37:77:5e:cb:d3:bf:57:86:dc:
        df:b4:18:b9:d9:64:ec:57:e0:f4:b5:d1:a7:48:9e:4a:02:eb:
        4c:9a:8a:fc:ac:1a:91:67:a0:97:34:d9:4e:60:2c:71:dc:78:
        35:f9:07:52:6e:bb:32:95:23:6c:d2:47:be:77:5e:54:0f:4a:
        e6:e7:f1:7f:a7:0f:5c:d7:3f:41:0d:d7:5b:5f:f7:88:b2:59:
        ca:86:79:ea:14:b5:77:a7:82:f9:4a:e3:3a:df:69:fa:8b:f4:
        45:cc:d5:07:ce:cb:9d:d9:e8:12:84:71:82:45:9e:3a:45:c9:
        a7:fd:67:f7
```

- **Certipost Public CA for Devices, Addresses and Services (signed by Baltimore Cybertrust Root)**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 120024008 (0x7276bc8)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
        Validity
```

```
        Not Before: Jan 11 19:21:57 2012 GMT
        Not After : Jan 11 19:21:31 2022 GMT
    Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Public CA for Devices, Addresses and Services
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:96:aa:25:f5:36:7f:3c:13:73:41:38:80:9a:89:
                cb:92:6c:c8:4f:01:b4:ea:a2:96:81:6f:fc:ac:89:
                4f:53:d8:9b:66:b7:55:9f:49:a3:8d:35:0e:9e:aa:
                76:76:2e:f6:b6:2d:d2:4d:89:69:e7:f0:84:16:85:
                ec:54:51:d8:99:70:d7:3d:34:9c:fe:ff:cd:1a:dd:
                8b:3f:2b:2c:bf:8d:57:f3:52:af:bb:7c:57:71:29:
                a1:03:43:ce:67:9c:67:3d:61:82:32:b0:e3:45:1a:
                f7:dc:87:3d:62:a5:ca:7e:cc:5c:8c:f9:49:8c:51:
                a8:3a:7a:da:ca:e6:50:1f:37:59:a7:c2:ff:19:aa:
                13:36:fb:16:69:d3:f2:6a:f6:0a:30:85:a4:0a:98:
                f3:9e:f5:5f:58:06:7f:bd:94:8c:36:8e:b9:58:4d:
                1b:7e:84:53:55:60:c9:38:8f:f8:88:92:17:f6:30:
                b1:31:d7:a5:5a:0f:b6:15:5d:97:8c:f5:2e:38:c2:
                13:2c:54:6b:8a:7f:25:14:da:0c:6a:05:ce:28:19:
                1e:cb:cb:54:2d:e2:c5:c3:a0:3c:53:3d:1f:63:95:
                f2:7a:4f:2e:8a:73:56:47:2e:49:0c:13:7c:d3:5a:
                00:d5:3d:cc:ef:6c:a6:a2:20:65:78:25:d5:df:42:
                bf:21
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:0
        X509v3 Certificate Policies:
            Policy: X509v3 Any Policy
              CPS: https://www.certipost.com/showpolicy

        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Authority Key Identifier:
            keyid:E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

        X509v3 CRL Distribution Points:
            URI:http://cdp1.public-trust.com/CRL/Omniroot2025.crl

        X509v3 Subject Key Identifier:
            C8:25:51:56:B9:3D:55:D6:CF:21:0D:BE:8B:B8:30:46:07:3E:53:7A
Signature Algorithm: sha256WithRSAEncryption
    a2:1d:b1:46:8b:00:00:96:14:14:6e:1d:78:85:74:13:40:e2:
    89:2f:4e:c4:03:fd:06:ce:73:32:f3:04:8d:6b:4b:06:07:4b:
    26:ec:e8:e3:3f:dc:3f:b1:2a:80:23:0b:e9:00:6d:e1:4e:57:
    b9:a0:60:3a:91:14:7a:c4:d7:45:b8:08:72:29:a7:6f:e2:eb:
    ca:e4:4e:36:04:49:06:fb:b5:cf:c7:0e:4e:48:45:3c:a5:49:
    85:58:d6:c9:7c:73:8b:71:f4:e3:f7:de:67:97:ac:9a:30:11:
    0b:12:3d:b6:04:c6:47:34:08:8c:02:2c:43:91:df:6e:02:43:
    44:ea:1c:3a:fa:9d:3f:72:85:f0:b7:5b:af:6f:ac:14:54:76:
    9b:38:2f:b1:7e:13:74:90:bc:09:7d:43:d0:15:65:cb:79:b7:
    05:7e:e0:fc:c9:0c:7a:a6:6d:43:cf:15:4e:9e:30:13:31:30:
    bf:fd:cd:cc:c7:9f:83:63:4f:5a:ac:9f:fd:97:37:38:18:98:
    43:f3:44:a1:3f:12:47:66:d7:86:b0:de:80:2a:40:e3:a8:bb:
    1f:25:e4:cf:25:ad:67:7b:b2:99:5f:6c:9a:f7:c9:1f:c0:ca:
    6d:e4:42:4f:3c:d7:30:f5:ad:7e:1e:04:86:85:9e:f4:bc:d5:
    07:78:1c:e1
```

- **Certipost Public CA for Devices, Addresses and Services (signed by Verizon Global Root CA)**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 906 (0x38a)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Verizon Business, OU=OmniRoot, CN=Verizon Global Root CA
        Validity
            Not Before: Jan 11 19:48:54 2012 GMT
            Not After : Jan 11 19:48:33 2022 GMT
        Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Public CA for Devices, Addresses and Services
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:96:aa:25:f5:36:7f:3c:13:73:41:38:80:9a:89:
                    cb:92:6c:c8:4f:01:b4:ea:a2:96:81:6f:fc:ac:89:
                    4f:53:d8:9b:66:b7:55:9f:49:a3:8d:35:0e:9e:aa:
                    76:76:2e:f6:b6:2d:d2:4d:89:69:e7:f0:84:16:85:
                    ec:54:51:d8:99:70:d7:3d:34:9c:fe:ff:cd:1a:dd:
                    8b:3f:2b:2c:bf:8d:57:f3:52:af:bb:7c:57:71:29:
                    a1:03:43:ce:67:9c:67:3d:61:82:32:b0:e3:45:1a:
                    f7:dc:87:3d:62:a5:ca:7e:cc:5c:8c:f9:49:8c:51:
                    a8:3a:7a:da:ca:e6:50:1f:37:59:a7:c2:ff:19:aa:
                    13:36:fb:16:69:d3:f2:6a:f6:0a:30:85:a4:0a:98:
                    f3:9e:f5:5f:58:06:7f:bd:94:8c:36:8e:b9:58:4d:
                    1b:7e:84:53:55:60:c9:38:8f:f8:88:92:17:f6:30:
                    b1:31:d7:a5:5a:0f:b6:15:5d:97:8c:f5:2e:38:c2:
                    13:2c:54:6b:8a:7f:25:14:da:0c:6a:05:ce:28:19:
                    1e:cb:cb:54:2d:e2:c5:c3:a0:3c:53:3d:1f:63:95:
                    f2:7a:4f:2e:8a:73:56:47:2e:49:0c:13:7c:d3:5a:
                    00:d5:3d:cc:ef:6c:a6:a2:20:65:78:25:d5:df:42:
                    bf:21
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://www.certipost.com/showpolicy

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:4C:38:11:B8:98:00:5B:5A:2B:70:3E:AA:78:E4:D5:67:67:67:A7:7E

            X509v3 CRL Distribution Points:
                URI:http://cdp1.public-trust.com/CRL/Omniroot2034.crl

            X509v3 Subject Key Identifier:
                C8:25:51:56:B9:3D:55:D6:CF:21:0D:BE:8B:B8:30:46:07:3E:53:7A
    Signature Algorithm: sha256WithRSAEncryption
        40:1c:e8:c0:ac:ac:9f:a2:a8:eb:90:30:c9:6a:82:d5:9e:9e:
        9c:a2:0f:27:d2:2a:f7:f9:e5:dd:14:85:5c:2d:31:08:f7:7e:
        64:96:18:ab:f2:38:da:a1:23:f3:9c:57:9a:71:72:39:82:8a:
        1c:2f:51:8a:53:30:64:48:df:e0:b1:a2:5c:09:d5:8d:7f:0e:
        16:e5:ba:14:27:e5:f6:7b:3d:d8:61:6c:61:24:7c:c8:bf:13:
        c6:de:3a:c6:13:6e:e3:e6:a5:be:e2:cf:c5:91:1f:a9:1b:76:
        f8:f1:a0:0e:00:1c:19:ae:e4:c4:5a:43:99:12:d0:48:f9:20:
        96:4e:53:ab:9e:ba:89:a1:b4:6b:37:04:05:c3:1f:67:a0:a3:
```

f5:33:19:ab:ae:95:65:21:d7:8b:dc:82:97:5d:45:95:85:87:
e8:86:53:fa:0f:8f:89:d5:82:aa:2a:f0:2c:80:19:58:65:f1:
a7:a6:ef:d1:85:98:dd:f2:2b:dd:8f:ca:29:f3:11:12:3b:13:
74:30:ac:1f:7d:61:39:90:d4:68:5b:a3:88:1f:43:57:1e:0c:
33:b7:a7:f9:71:9e:01:ae:f6:dd:70:aa:d5:2f:a5:97:9a:a3:
4e:93:42:57:29:f7:f6:2b:ce:83:ed:f2:b7:c4:f0:2e:d0:69:
e4:f4:63:f8

- **Certipost Internal Use CA Root Signed SHA-1 (signed by Baltimore Cybertrust Root)**

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 120024009 (0x7276bc9)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
Validity
Not Before: Jan 11 19:23:43 2012 GMT
Not After : Jan 11 19:23:23 2022 GMT
Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Internal Use CA Root Signed SHA-1
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:c5:71:6b:57:a2:9c:63:fa:6b:18:d8:2f:e7:0e:
57:86:bf:df:0b:68:17:2c:60:0e:35:a4:44:76:3f:
f2:85:b8:b2:67:77:ee:6d:e5:28:b3:83:0d:ab:79:
df:a5:5f:27:4f:d4:fc:37:b1:74:d3:52:80:90:ac:
09:a6:4a:4d:48:55:8f:46:0a:40:cc:23:07:6e:ef:
34:8c:81:48:dd:18:ba:85:2b:44:d8:bd:4d:b5:f4:
00:6a:5b:6b:1c:bd:56:3c:19:7e:8c:32:2a:bb:f5:
10:3c:b8:46:82:b0:89:91:da:65:ee:62:97:0d:4e:
41:d9:43:cb:3c:e7:87:06:a1:39:2d:d0:b1:c8:4d:
89:ce:d2:1c:81:29:5c:a8:14:ba:b6:9d:6f:db:b9:
26:b0:dd:25:1b:ab:3f:6a:27:1b:7f:d5:8d:8d:04:
97:0c:ce:4e:47:ed:94:e2:09:30:95:69:95:e6:fb:
5f:ad:bd:85:5f:57:a4:33:51:a0:12:8d:c1:98:ab:
46:14:90:1c:cf:54:00:1c:4b:7c:d9:8a:70:4b:92:
4f:2b:e1:b6:10:17:46:f1:de:58:dd:cf:ff:74:fe:
1b:77:0a:6a:a8:d3:1b:39:eb:ce:3e:dd:01:a0:f4:
27:72:8f:d8:c5:0c:a6:b6:aa:79:97:cb:5e:da:24:
85:99
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Certificate Policies:
Policy: X509v3 Any Policy
CPS: https://www.certipost.com/showpolicy

X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Authority Key Identifier:
keyid:E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

X509v3 CRL Distribution Points:
URI:http://cdp1.public-trust.com/CRL/Omniroot2025.crl

X509v3 Subject Key Identifier:
41:04:B6:B0:E6:1D:78:48:A7:17:3E:C1:CF:26:CA:1E:01:AB:0D:6B
Signature Algorithm: sha1WithRSAEncryption
94:66:a8:27:0c:8a:a7:54:be:d1:07:25:f1:52:c4:f3:7e:02:

24:05:e3:d4:58:03:81:56:93:2e:ce:79:d5:03:aa:ea:a7:f2:
58:fe:6e:98:15:cc:43:1f:77:b7:4a:77:f5:bc:44:6d:7a:f1:
7d:79:7c:cf:07:5b:da:94:03:a2:16:03:36:54:bd:17:01:6e:
2c:37:7f:ae:3a:0b:5e:9e:94:1c:f1:11:66:2f:08:cb:36:6a:
4f:c0:9a:86:a0:1a:c3:64:a3:b4:44:64:48:68:59:96:43:63:
6c:ad:ad:03:46:8d:36:00:54:80:2c:0b:31:23:95:f2:f2:d7:
c0:a1:67:ea:58:6c:7e:5d:6d:78:2d:cf:a5:fc:df:98:74:c3:
02:f7:33:7a:ad:62:67:98:23:65:98:6b:bb:7b:45:02:5d:ad:
a7:3e:b3:ec:76:23:00:9d:73:d3:91:42:9d:3a:d9:73:56:34:
ae:aa:02:8b:68:4c:c3:e6:16:f8:3d:87:86:fd:08:d4:d9:86:
56:9e:d7:50:d2:d4:a4:dc:4c:9b:d9:8f:1f:43:fd:69:31:16:
ac:0a:e5:40:d3:d9:6b:79:e5:77:80:87:6a:04:89:22:6b:83:
23:68:cf:ba:4d:b8:7b:1e:f6:1c:a9:b5:5d:34:dc:ae:72:6e:
34:ae:9d:35

- **Certipost Internal Use CA Root Signed SHA-256 (signed by Verizon Global Root CA)**

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 907 (0x38b)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Verizon Business, OU=OmniRoot, CN=Verizon Global Root CA
Validity
Not Before: Jan 11 19:50:26 2012 GMT
Not After : Jan 11 19:50:01 2022 GMT
Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Internal Use CA Root Signed SHA-256
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:d4:e2:4d:29:09:78:50:8b:82:c2:d7:d2:1d:e2:
b2:eb:f1:10:8d:ea:15:25:3c:87:a2:27:ac:50:ec:
b0:87:02:b1:71:c6:09:f1:ad:e3:0b:77:a2:5b:89:
89:b4:d0:ef:a6:59:cf:68:60:18:d4:85:2c:34:77:
6f:fa:d0:82:36:7c:64:e3:6f:98:e7:06:02:14:83:
7b:88:f3:66:46:a2:3b:63:d1:cd:c2:d1:06:d1:00:
35:c1:5d:cd:9b:0a:54:58:f8:eb:8e:f8:83:6c:02:
b9:c8:da:77:22:40:eb:c5:1d:d0:99:64:f7:3f:ba:
f0:1d:71:a1:53:4b:94:c4:8d:9e:62:40:e3:f7:ba:
3b:19:6f:3b:a9:cb:6d:0f:18:62:df:0e:39:15:81:
db:7d:66:16:82:52:e2:b4:7a:0b:8c:06:70:15:49:
e6:c8:e4:bf:de:66:7b:e6:e4:54:3a:95:64:4c:8e:
59:ef:43:5a:bd:b8:63:06:74:60:a0:0a:54:d9:35:
33:78:7b:12:42:64:52:e4:37:19:82:12:f4:7b:2c:
33:4f:0d:4d:f0:77:a9:a8:b0:83:e8:15:2a:03:f0:
8c:bf:44:94:73:ba:f6:c9:5e:0a:64:71:97:b4:c0:
ff:88:d0:34:98:4c:d7:5e:d9:41:05:97:7d:1e:62:
09:17
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Certificate Policies:
Policy: X509v3 Any Policy
CPS: https://www.certipost.com/showpolicy

X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Authority Key Identifier:
keyid:4C:38:11:B8:98:00:5B:5A:2B:70:3E:AA:78:E4:D5:67:67:67:A7:7E

```
            X509v3 CRL Distribution Points:
                URI:http://cdp1.public-trust.com/CRL/Omniroot2034.crl

            X509v3 Subject Key Identifier:
                1B:80:D6:C9:39:10:86:1A:BA:8F:D1:5A:45:06:E9:DA:1B:76:00:30
    Signature Algorithm: sha256WithRSAEncryption
        25:a8:f6:7f:76:f6:72:b7:65:2e:c0:49:38:3a:01:c9:3c:9f:
        0f:7c:c1:8d:bc:4e:92:61:ab:9d:04:65:31:f3:84:e8:8a:b6:
        9f:9f:ec:04:4e:f9:c1:b0:84:7d:5d:f2:f3:6f:76:2e:28:9b:
        7c:79:09:f3:4c:b8:0d:2f:4f:e3:b8:17:ad:28:9a:0b:72:70:
        89:70:bb:4b:51:53:0e:49:22:6f:8b:bc:61:c4:05:0d:57:43:
        af:51:b0:4d:e5:d6:52:5c:68:b5:10:e2:97:97:8f:ac:6d:4b:
        b3:34:4f:11:e5:71:76:c0:54:1b:30:08:16:6f:66:e8:2b:c9:
        87:b8:b3:70:bc:f6:4a:41:0b:3e:fd:e4:50:98:43:d8:4e:c2:
        04:d5:7d:8e:68:76:17:8e:cf:aa:df:45:a2:92:20:09:26:f8:
        06:4d:8d:c6:52:41:bf:d2:b1:95:1d:55:5a:5a:db:a3:8a:0d:
        00:70:23:45:a3:57:1a:d3:e4:38:39:b3:0f:83:5d:40:3b:28:
        14:47:e6:45:fb:bd:d7:4f:16:8a:d0:6b:43:af:fd:98:b6:db:
        f1:13:1c:2e:ab:42:0c:69:16:55:c2:8f:84:d8:ad:13:a0:3b:
        47:ea:62:fa:0b:0b:73:55:be:43:12:67:76:87:10:b4:98:66:
        3a:5c:a3:94
```

- **Certipost Lightweight CA for EUROCONTROL (signed by Verizon Global Root CA)**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 908 (0x38c)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Verizon Business, OU=OmniRoot, CN=Verizon Global Root CA
        Validity
            Not Before: Jan 11 19:52:37 2012 GMT
            Not After : Jan 11 19:52:13 2022 GMT
        Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Lightweight CA for EUROCONTROL
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:d0:98:20:21:b6:00:ba:2c:5f:8d:a9:71:8f:67:
                    b1:b1:74:8d:5b:25:88:37:73:60:b4:eb:cb:e4:a5:
                    07:52:dd:bb:e4:1a:07:b1:96:2e:73:49:3d:63:7d:
                    2c:6f:23:94:d6:12:b2:dc:1b:d9:08:7d:26:5e:ca:
                    4e:58:55:e0:8d:66:61:b0:b7:9a:c4:27:a6:d9:37:
                    9d:c0:58:75:67:71:5d:ca:2d:32:70:bf:7a:02:ec:
                    23:8f:7b:a7:f5:5c:66:d5:df:92:bd:69:ab:ab:7f:
                    c0:3c:20:c9:c2:0b:20:98:a8:52:7c:7a:61:0d:e8:
                    3b:23:b3:cb:10:9f:c9:16:a9:6f:8c:3f:84:c7:d3:
                    73:a8:61:42:0c:8a:c2:56:af:8b:27:a9:04:f9:cb:
                    bd:69:b8:42:c2:3e:3b:b1:d3:71:27:fc:56:21:d4:
                    67:26:82:33:dd:36:7a:75:a0:dc:5c:32:6c:14:a8:
                    e7:5f:6a:43:30:0f:b6:f6:59:0f:ea:b1:9d:65:2e:
                    10:74:65:60:13:70:7b:ce:c1:11:fe:b3:47:72:71:
                    ce:7c:01:04:cf:ae:59:b7:43:71:2e:ef:c8:2c:56:
                    17:b5:55:7b:b3:03:67:ef:23:dc:a8:c1:45:22:28:
                    b3:1c:e6:9b:db:9d:6f:75:7a:c4:6d:d8:7b:44:b4:
                    0c:bb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Certificate Policies:
```

```
            Policy: X509v3 Any Policy
              CPS: https://www.certipost.com/showpolicy

            X509v3 Key Usage: critical
              Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
keyid:4C:38:11:B8:98:00:5B:5A:2B:70:3E:AA:78:E4:D5:67:67:67:A7:7E

            X509v3 CRL Distribution Points:
              URI:http://cdp1.public-trust.com/CRL/Omniroot2034.crl

            X509v3 Subject Key Identifier:
              54:29:53:BB:7A:04:B8:7A:37:D4:A8:D7:76:7B:11:6C:24:D3:F3:85
    Signature Algorithm: sha256WithRSAEncryption
      6f:7c:a5:cc:88:4a:77:6e:f2:6b:12:20:24:81:eb:f0:6f:b7:
      01:1c:47:28:b0:c5:39:12:b8:e2:2f:7d:cf:a8:dd:f3:4f:7d:
      ab:75:71:4a:73:c9:3d:8f:d4:c4:7f:bd:26:c7:c4:a1:fe:9e:
      15:3f:fb:9c:a3:ca:52:fa:d0:97:bf:e3:a2:cd:a0:07:ce:7e:
      29:86:01:8d:f4:37:25:d0:90:3c:c8:d6:bb:31:56:39:9b:c3:
      ab:d1:9f:70:10:05:72:77:2d:77:f2:9a:6c:cf:db:a9:91:7a:
      3a:92:4b:f3:ab:d8:b5:a7:55:55:d6:eb:ae:05:e8:6d:a1:57:
      64:0b:7b:3f:dc:da:c3:d2:2b:c7:5a:a1:ca:99:0a:3f:7f:81:
      56:2a:9c:a4:92:94:c3:74:3b:b9:d0:f8:b1:af:fd:09:32:98:
      b2:04:cf:9b:2b:ed:87:4c:75:7d:56:ec:15:ac:80:59:61:d6:
      19:fe:6b:10:8c:b3:59:ed:e0:92:b5:4b:2c:54:13:4e:61:8d:
      de:ed:79:b2:82:a0:9e:02:ce:dd:39:cf:be:9b:6f:62:76:89:
      d6:b3:f0:77:7b:e9:ab:10:09:00:28:d4:82:13:e8:a9:4b:ab:
      20:f9:5d:18:32:c9:00:2e:2b:9a:3f:e2:f0:57:2f:66:d9:e0:
      1b:b9:d6:d8
```

- **Certipost Internal Use CA SHA-1 (self-signed)**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:00:00:00:00:01:34:67:07:09:c7
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=BE, O=Certipost n.v./s.a., CN=Certipost Internal Use CA SHA-1
        Validity
            Not Before: Dec 22 09:00:00 2011 GMT
            Not After : Oct 31 09:00:00 2026 GMT
        Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Internal Use CA SHA-1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e6:b1:af:30:fd:be:76:a9:1e:10:04:9d:14:1a:
                    f1:a1:75:4f:55:74:6a:81:38:0d:29:be:3e:85:ab:
                    5b:04:f4:a1:b1:33:f7:2b:3a:f2:a4:be:ed:b6:b3:
                    2d:c9:f4:e4:d4:48:d8:67:07:b7:0c:b4:4c:57:cc:
                    bc:c1:13:cd:49:49:3c:df:07:91:25:95:f1:98:91:
                    13:6d:91:b4:53:88:87:6b:09:28:59:b1:28:15:17:
                    2b:3b:70:ab:d2:cc:53:c5:32:47:3f:27:99:89:2b:
                    12:2d:7d:b8:13:82:64:f4:f3:8a:51:e0:2c:f9:d7:
                    ff:7a:55:06:aa:93:4b:a8:5a:3a:ba:55:a1:43:bc:
                    41:df:45:0b:2d:e7:d5:a8:4b:e0:56:72:3b:51:bc:
                    20:3d:52:6c:8e:3e:87:b8:4e:dc:74:c5:0c:05:f9:
                    6c:6c:57:20:fd:c7:36:be:e6:34:a8:c6:14:89:1e:
                    55:2c:31:93:97:2d:4e:ad:ce:63:e5:30:65:78:a7:
                    51:28:a7:02:45:10:b1:03:f0:91:f5:c8:a1:9e:4c:
```

```
                7b:db:7e:35:d3:c0:03:23:73:2f:1d:0d:4c:ae:03:
                29:21:8a:c2:16:fb:df:0b:dc:7b:a2:6c:9a:2c:e2:
                18:0d:59:ac:ed:a5:35:46:d7:97:e2:29:5f:89:c3:
                1f:af
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
56:CB:29:19:0A:5E:91:B1:5E:5E:CA:BC:ED:40:3C:CB:51:D8:CF:DA
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://www.certipost.com/showpolicy

            X509v3 Authority Key Identifier:
                keyid:56:CB:29:19:0A:5E:91:B1:5E:5E:CA:BC:ED:40:3C:CB:51:D8:CF:DA

    Signature Algorithm: sha1WithRSAEncryption
        b1:2a:70:1a:28:17:2a:e3:4e:b7:e7:1c:01:61:a2:fd:8d:3a:
        d2:9e:1f:ed:f8:6b:e5:e9:db:a9:a2:1b:89:28:2c:f4:7d:e9:
        07:82:e6:07:9b:ae:4e:25:cc:de:e9:e6:8c:80:c8:0d:b0:3b:
        55:ae:94:d5:02:29:c4:76:ab:97:a6:36:cf:ec:85:f3:6e:3b:
        46:e3:e2:cc:0b:a0:e3:d6:55:6a:b6:c0:dc:76:fc:b2:f0:8a:
        b2:dd:53:d6:b1:e2:b6:ce:25:50:4d:5e:5c:64:8f:77:ac:33:
        f0:f7:be:2d:bd:df:2c:a9:75:57:d4:92:e4:1f:ab:52:5a:cc:
        3c:5a:78:34:44:5e:08:9a:1d:85:5d:8d:42:f0:5b:f8:14:1b:
        1d:f6:c7:8d:0e:13:17:c8:55:8d:23:0c:09:65:f0:77:7c:bb:
        4f:64:32:9d:22:71:7a:46:32:7a:66:c1:ca:66:32:80:69:34:
        c3:d7:49:3f:8f:2c:61:10:15:89:7e:f5:3a:54:a9:02:54:2d:
        8c:99:47:67:d9:9f:e5:1a:9d:5c:18:ad:64:a0:ed:c2:9a:99:
        7b:71:51:7a:71:db:af:52:c6:68:e4:cd:6e:75:39:35:1b:7a:
        d5:4e:8e:b1:4a:0a:d7:a2:16:83:c7:26:3b:ff:7b:d5:84:87:
        af:4c:06:98
```

- **Certipost Internal Use CA SHA-256 (self-signed)**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:00:00:00:00:01:34:67:07:0c:58
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BE, O=Certipost n.v./s.a., CN=Certipost Internal Use CA SHA-256
        Validity
            Not Before: Dec 22 09:00:00 2011 GMT
            Not After : Oct 31 09:00:00 2026 GMT
        Subject: C=BE, O=Certipost n.v./s.a., CN=Certipost Internal Use CA SHA-256
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:a3:e7:d5:4c:6f:1e:b3:55:19:9e:8f:09:e8:54:
                    e1:0a:0a:bc:f4:73:27:f2:59:94:3f:7f:7f:a6:5f:
                    57:9a:df:5f:ea:6c:1c:34:25:c1:08:5d:b8:9c:5e:
                    60:f2:71:02:87:48:cc:12:97:35:01:94:76:a3:ad:
                    49:5e:3f:b8:e4:82:b6:f5:e3:d4:23:3d:32:d7:eb:
                    03:a2:04:14:54:12:ee:aa:99:f3:c7:a4:9e:0f:f7:
                    b2:b9:78:fe:7a:c8:34:ca:f5:dd:a8:fc:a3:cf:ab:
                    7e:d3:be:59:96:64:71:ee:2b:2f:7a:23:76:30:95:
```

```
                a3:1c:28:41:74:cd:80:e3:0e:5b:d3:78:6d:ca:e9:
                2c:d1:ed:14:e9:d8:3d:d8:28:74:97:2f:a9:19:4b:
                0c:db:73:ce:bc:f1:fb:4f:94:96:d8:19:cd:c0:1d:
                b3:60:f4:ab:88:d3:a7:31:34:83:39:38:84:bf:f0:
                d6:cf:65:c7:d3:56:89:c0:c8:20:65:76:45:6a:1e:
                e7:84:ac:e0:ed:53:28:83:71:a8:1b:6e:7a:11:8f:
                d3:13:aa:12:36:80:f0:16:2c:16:80:c2:13:bf:c3:
                83:5c:c2:45:39:01:30:cf:49:1b:a6:c2:c7:e9:d4:
                64:71:7e:85:5e:03:75:7d:70:88:bc:df:54:8b:31:
                c1:5f
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
                E8:41:7D:C3:0D:C7:33:89:FE:75:20:07:8B:D9:04:E5:A8:B7:5C:23
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://www.certipost.com/showpolicy

            X509v3 Authority Key Identifier:
                keyid:E8:41:7D:C3:0D:C7:33:89:FE:75:20:07:8B:D9:04:E5:A8:B7:5C:23

    Signature Algorithm: sha256WithRSAEncryption
        0c:ff:53:e7:c0:eb:c9:fe:8a:3a:e3:61:9c:de:57:ab:6b:7e:
        e0:46:36:cc:44:be:74:02:fe:eb:bb:c4:69:e3:fc:fa:c0:cd:
        d4:75:e5:31:1b:e1:a9:ba:1b:0d:59:fe:11:aa:98:1f:6d:73:
        b6:25:23:53:27:48:4b:cb:0e:b5:22:9b:7a:aa:eb:29:2c:17:
        1f:fb:f4:10:2f:39:e5:83:4e:d0:96:a7:6a:d2:cf:6f:88:4c:
        d2:9a:e1:cf:20:8d:19:8e:83:c4:18:1a:1a:9c:3e:91:39:8a:
        88:37:51:59:d7:b9:a5:60:a0:8b:be:fd:c9:09:b2:94:78:a6:
        9f:61:ce:ac:b4:66:29:ea:ac:05:cf:08:2f:e6:85:2a:ef:22:
        14:a4:a6:e4:0d:8f:8a:35:00:b4:ce:23:dc:46:b0:1a:2d:2b:
        ea:f9:db:3b:eb:95:d8:c9:94:56:b9:78:94:d3:36:0b:18:72:
        81:7f:28:db:e0:9c:fe:d4:e1:19:59:84:69:d9:7c:ef:63:60:
        97:bd:8c:8d:cb:4e:8b:f1:21:c4:30:d3:e6:51:82:09:c5:6c:
        8a:34:6b:7a:33:d4:77:d6:d2:e8:c6:96:ed:44:b5:bc:59:2f:
        45:53:14:9d:67:86:2c:85:95:9e:f3:4e:f2:b9:8a:9e:cb:2b:
        52:e6:02:4f
```

- **Certipost E-Trust Primary Qualified CA**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 120024016 (0x7276bd0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
        Validity
            Not Before: Jan 11 22:09:42 2012 GMT
            Not After : Jan 11 22:09:20 2022 GMT
        Subject: C=BE, O=Certipost s.a./n.v., CN=Certipost E-Trust Primary Qualified CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ae:20:d2:78:db:9a:a0:72:9c:04:52:25:2c:6d:
                    52:d8:d7:27:89:33:a0:e1:b2:d5:fb:30:75:6b:2d:
                    7f:1c:67:8e:0e:e7:1f:12:df:17:79:18:bb:b4:1b:
```

```
                6f:f8:3d:75:1b:9e:67:37:f0:f1:fa:0f:75:ed:86:
                9d:03:04:a1:28:70:2d:3c:b2:6b:a0:73:51:e3:35:
                a9:74:a5:08:3e:94:85:27:36:2a:aa:72:64:fc:77:
                ee:76:94:1c:72:eb:bf:32:c7:77:03:6a:25:82:09:
                05:af:5f:60:3c:7f:ac:1b:bc:92:e8:3c:74:59:ce:
                f1:7c:54:2d:38:ae:96:f0:ac:6f:a1:33:0c:21:5a:
                01:ba:23:20:5b:a0:86:02:d5:53:dc:49:1f:a8:32:
                b3:af:3b:46:3b:b6:ef:9f:39:b3:38:0b:e7:7a:8a:
                f6:28:f9:a7:6f:50:29:c8:79:58:8b:49:d2:a5:d8:
                85:7e:56:f1:69:15:78:44:11:35:d7:a5:54:3e:ab:
                66:25:d2:db:e3:18:f1:2e:2b:e2:71:23:09:37:64:
                43:42:74:32:96:77:de:97:a2:e9:96:86:9c:25:44:
                09:d4:01:9d:51:7e:33:b7:09:44:e5:80:97:0d:64:
                5b:77:18:97:a5:4b:a9:9e:10:9d:87:fa:56:a7:cf:
                0a:7d
            Exponent: 65537 (0x10001)
        X509v3 extensions:
X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:1
          X509v3 Certificate Policies:
            Policy: X509v3 Any Policy
              CPS: https://www.certipost.com/showpolicy

          X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
          X509v3 Authority Key Identifier:
            keyid:E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

          X509v3 CRL Distribution Points:
            URI:http://cdp1.public-trust.com/CRL/Omniroot2025.crl

          X509v3 Subject Key Identifier:
            F0:78:F9:07:77:10:BB:DC:1E:A1:AE:79:FB:30:10:DB:C6:34:F8:17
    Signature Algorithm: sha1WithRSAEncryption
        19:bd:e0:0a:63:11:aa:81:9a:4f:af:4b:e6:da:0d:d6:92:51:
        70:80:4f:f6:c1:6f:29:be:18:92:f3:50:d7:e8:31:69:a1:5b:
        a7:aa:ea:ac:f3:ef:40:f0:e5:fb:02:c1:e1:c1:b1:83:0e:f7:
        0f:a7:cc:be:02:3c:5c:79:ad:86:f5:18:eb:a6:53:5a:a1:98:
        78:fa:26:b6:e3:91:f2:3a:fa:a6:6b:ad:34:cf:89:6f:17:2c:
        70:48:01:7a:43:01:c3:81:3e:03:c3:c4:2e:21:dc:d0:87:52:
        17:af:ab:b0:e8:12:8a:b6:16:11:c5:6a:69:db:eb:bb:7a:8c:
        9f:50:23:ab:80:70:02:85:56:57:13:bf:94:9b:88:4b:23:49:
        ed:53:13:f0:df:a7:cc:12:ee:bc:e7:d5:14:99:10:72:4d:f4:
        7b:c7:6d:7f:56:7f:e9:73:a6:d8:82:0f:75:7b:19:03:24:da:
        ef:da:77:a8:e5:f0:f9:75:55:e9:b5:db:cd:e2:9a:cd:34:b3:
        bb:8a:0d:30:3e:55:cb:f7:a8:98:e8:2d:3d:a1:b8:b1:3c:b4:
        6f:88:b2:32:fe:ba:43:bd:c5:3f:74:59:18:76:1d:d9:93:b9:
        73:f6:63:25:36:b9:64:2c:9f:11:3b:d0:39:be:9c:98:ec:e2:
        1a:cc:3f:ad
```

- **Certipost E-Trust Primary Normalized CA**

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 120024017 (0x7276bd1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
        Validity
            Not Before: Jan 11 22:11:50 2012 GMT
            Not After : Jan 11 22:11:31 2022 GMT
```

```
        Subject: C=BE, O=Certipost s.a./n.v., CN=Certipost E-Trust Primary Normalised CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:d5:b3:aa:52:84:7a:17:93:22:0f:b8:04:18:ca:
                    c9:f2:82:2a:ac:15:0b:a7:50:71:b6:4c:25:6b:f7:
                    ff:01:aa:57:5a:77:4e:5e:13:14:0d:55:f2:1e:f1:
                    85:cd:85:d7:82:1c:0c:da:09:2b:bd:fd:bc:9e:fe:
                    6d:89:4d:a2:02:24:e6:51:ea:37:7f:31:46:5a:7b:
                    9a:76:b3:2e:a0:5d:5f:e4:f8:99:0a:07:be:ee:92:
                    26:12:c9:7b:e7:5d:6c:d0:83:47:0e:c0:8c:a7:d1:
                    79:57:c0:0b:19:9c:9b:9e:43:c5:4e:91:25:ce:88:
                    2b:6d:79:d9:79:8a:d6:66:4e:22:c3:1a:45:4e:ef:
                    c8:b0:62:26:4e:26:54:50:9f:0c:6f:b3:6b:cc:7c:
                    9f:7f:de:0f:0d:b5:8f:c3:6b:d4:e1:c2:fb:bb:56:
                    50:aa:8c:3d:8f:00:8b:3c:fc:48:17:6a:d2:5a:f3:
                    75:6d:65:81:bd:46:5d:9f:a2:62:53:ae:ce:f3:a9:
                    e4:91:2b:5a:26:c3:79:66:d1:a6:53:66:35:1c:06:
                    71:b1:ee:99:0e:c4:fb:58:12:ac:22:46:2d:e2:22:
                    92:db:e1:3c:bf:bb:fe:86:e7:93:34:73:cf:78:69:
                    d3:cb:de:f9:0c:b2:68:da:c9:8a:0a:60:54:c4:f3
56:63
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://www.certipost.com/showpolicy

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

            X509v3 CRL Distribution Points:
                URI:http://cdp1.public-trust.com/CRL/Omniroot2025.crl

            X509v3 Subject Key Identifier:
                11:F2:0B:96:D2:33:38:81:57:58:13:FD:40:A4:11:6F:4E:99:FA:67
    Signature Algorithm: sha1WithRSAEncryption
        83:4d:fc:e1:36:19:67:f9:a8:99:06:f7:43:2a:fc:5d:fb:f3:
        11:f8:7a:1f:3b:00:25:be:f5:7d:54:33:54:1f:90:7c:7d:1f:
        af:14:c1:38:3e:00:e0:eb:4c:e7:b6:06:44:62:0e:05:53:5d:
        ca:e7:7f:f6:53:d9:b8:be:f0:62:2e:94:4b:05:62:31:c9:76:
        99:f2:1c:2c:c7:ca:d1:70:a6:6f:39:16:a2:dc:13:03:39:4c:
        6a:2b:45:c0:97:97:af:6f:1c:dc:76:ba:67:d5:aa:3f:7c:95:
        11:2b:a2:01:6b:c8:db:94:1a:e1:37:29:e9:5c:28:63:e7:e7:
        67:35:28:5e:7e:53:74:9a:98:77:41:7a:8d:b3:c8:c0:17:19:
        b0:e3:93:aa:82:e3:bc:b4:47:c6:a6:0b:c6:a3:88:67:b6:c0:
        3c:95:6b:31:7a:b4:ab:b5:09:49:9d:5d:da:72:86:ae:5d:13:
        eb:a0:e7:53:53:6f:ae:2c:3e:5d:25:41:c4:5b:64:01:ff:8b:
        a6:fb:dc:53:04:3b:72:67:9e:58:81:38:36:69:a9:67:6c:f7:
        ad:d2:55:23:5b:74:91:35:80:44:68:45:83:36:c1:f4:bd:3a:
        16:ee:c8:d3:49:8d:20:11:6a:ef:04:e5:0c:f7:9b:be:6d:be:
        e6:22:9f:3c
```

- **Certipost E-Trust Primary LightWeight CA**

```
    Certificate:
```

```
Data:
    Version: 3 (0x2)
    Serial Number: 120024018 (0x7276bd2)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
    Validity
        Not Before: Jan 11 22:13:25 2012 GMT
        Not After : Jan 11 22:13:06 2022 GMT
    Subject: C=BE, O=Certipost s.a./n.v., CN=Certipost E-Trust Primary LightWeight CA
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:cd:af:1e:9f:10:40:5a:75:3a:17:be:33:d6:dd:
                fa:59:74:21:b8:76:83:b8:8a:67:a4:c1:d1:7f:45:
                1b:63:92:0d:80:74:4f:e8:8a:14:e7:3c:e3:0e:97:
                bf:29:76:fc:5c:f4:8a:f1:96:e9:82:df:84:1b:7c:
                34:78:8a:03:16:7b:49:7c:26:44:91:57:dd:9c:58:
                6e:b8:d0:06:5d:79:22:68:35:f5:4e:33:e2:4e:6d:
                30:7d:b5:89:2e:61:7c:64:28:21:2a:50:d9:f9:2f:
                4e:3d:69:92:eb:ed:78:67:df:76:9a:9f:67:7f:47:
                57:a0:96:91:2f:0d:37:3f:a4:bd:4e:a7:c9:a3:5b:
                42:4a:9f:fe:53:98:b2:36:5f:ac:08:6e:3f:bb:a6:
                4d:02:49:2f:de:45:ae:c2:62:74:c3:6e:d9:9b:df:
                41:08:d9:e5:0f:79:58:3b:9a:5c:ee:ed:22:5e:2c:
                bb:84:78:9b:64:64:a2:be:33:f8:d6:72:83:c4:fb:
                75:2c:b7:73:45:eb:bf:fb:70:7f:89:35:55:09:b4:
                 f8:5b:3b:df:23:5b:53:39:e9:f3:8e:0a:cb:df:c7:
                0f:83:69:89:33:01:b4:d5:58:aa:e1:a1:ba:26:06:
                c7:7d:3b:c8:14:a7:4e:7c:1f:59:cf:1b:33:42:67:
                aa:21
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:1
        X509v3 Certificate Policies:
            Policy: X509v3 Any Policy
              CPS: https://www.certipost.com/showpolicy

        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Authority Key Identifier:
            keyid:E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

        X509v3 CRL Distribution Points:
            URI:http://cdp1.public-trust.com/CRL/Omniroot2025.crl

        X509v3 Subject Key Identifier:
            D8:68:8B:29:34:E4:BB:75:12:22:13:32:FF:D4:9D:DE:B4:FA:63:EC
Signature Algorithm: sha1WithRSAEncryption
    07:75:37:49:7d:2b:dd:66:d3:47:5c:39:24:c8:2d:3b:72:5f:
    92:fe:79:aa:40:97:16:f5:0f:06:8f:3b:d3:18:15:47:a8:cd:
    cb:12:2f:48:b4:e2:ba:78:a5:af:1e:8c:15:a3:da:ae:76:77:
    ba:5d:af:b2:6a:93:c8:c1:05:ff:1b:fe:04:d1:22:21:7b:b4:
    38:19:32:19:0e:e9:54:4d:87:79:b9:ed:c6:52:2d:03:02:9d:
    ca:d6:ac:a5:2f:c4:12:c2:99:6f:1e:71:6f:eb:8b:6f:19:97:
    32:20:9d:fd:02:60:22:c2:84:c7:dd:dc:6e:59:a7:69:bd:58:
    e7:e5:5c:3d:4b:d0:5c:ae:43:1e:41:3a:97:09:d4:db:bb:29:
    44:51:4c:74:3d:d5:b2:2f:2a:05:87:0f:f3:c4:59:47:a6:29:
    5a:54:e8:92:79:95:ea:52:8c:09:eb:6b:3f:67:73:ec:67:a8:
    0d:8e:ef:7b:8a:3a:13:52:2c:37:9a:5f:9c:6e:5b:e5:e1:9f:
    d3:af:2b:8e:97:df:63:03:e7:e2:77:1f:c1:36:87:0f:16:43:
```

c3:d9:94:e3:8f:34:8a:83:be:d9:ce:4d:13:64:ac:dd:0a:98:
67:d1:5e:84:af:37:22:c6:07:8b:82:22:55:39:bb:cf:81:1a:
e3:cc:b5:4a

5.7.1.2.2. End-entity certificates

The certificate extensions and their criticality are specified in each CP.

5.7.1.3. Algorithm object identifiers

Applicable algorithm OIDs are specified in each CP.

5.7.1.4. Name forms

These are specified in each CP.

5.7.1.5. Name constraints

These are specified in each CP.

5.7.1.6. Certificate policy object identifier

This is specified in each CP.

5.7.1.7. Usage of Policy Constraints extension

These are specified in each CP.

5.7.1.8. Policy qualifiers syntax and semantics

These are specified in each CP.

5.7.1.9. Processing semantics for the critical Certificate Policies extension

These are specified in each CP.

5.7.2. CRL profile

5.7.2.1. Version number(s)

CRL version 2 is supported.

5.7.2.2. CRL and CRL entry extensions

Version= 2

Issuer= *Issuing CA (of the end-entity certificates)*

Effective date= *the issue date of the CRL*

Next update= *date by which the next CRL will be issued*

Signature Algorithm= *algorithm identifier for the algorithm used by the CRL issuer to sign the CertificateList* (e.g. **sha1RSA** or **sha256RSA)**

Authority Key Identifier= *Authority Key Identifier of Issuing CA*

CRL Number=*increasing sequence number for the given CRL scope and issuer*

CRL entry extensions:

Serial number= *certificates revoked by the CA are uniquely identified by the certificate serial number*

Invalidity Date= *date on which the certificate became invalid*

X509v3 CRL Reason Code= *either not-specified or* **certificateHold (6)**

5.7.3. OCSP profile

Not applicable.

5.8. Compliance audit and other assessments

5.8.1. Frequency or circumstances of assessment

The Certipost CErtification PRactices Council (CEPRAC), shall reserve the right to require periodic and non periodic inspections and audits of any CA facility within its domain to validate that the CA is operating in accordance with the security practices and procedures laid down in the present CPS, in the appropriate CP's and in internal documents.

CA's operating under this CPS shall be audited regularly for conformance with the present CPS and the appropriate CP's.

The Certipost CErtification PRactices Council (CEPRAC) shall reserve the right to require periodic and non periodic inspections and audits of any RA facilities to validate that the RA is operating in accordance with the security practices and procedures laid out in the present CPS, in the appropriate CP's and in internal documents.

5.8.2. Identity/qualifications of assessor

The auditor shall have qualifications in accordance with best commercial practice and as mandated by law. The auditor must perform CA or Information System Security Audits as its main task, and must be thoroughly familiar with the CA's CPS. The auditor shall be named in the Revision Status of the CPS and, if relevant, the appropriate CP's.

5.8.3. Assessor's relationship to assessed entity

The auditor and CA shall have a contractual relationship for the performance of the audit, and be sufficiently organizationally separated from the audited CA to provide an unbiased, independent evaluation. The auditor shall be a certified public auditor if required by the appropriate CP or by the law.

5.8.4. Topics covered by assessment

a) The audit only compares the practices laid down in this CPS and the appropriate CP's with the onsite CA's implementation. All aspects of the CA's operation as specified in this CPS shall be subject to an audit compliance inspection.
b) The audit shall also consider the operations of CA's subcontractors.
c) It is the Relying Party's and cross-certifying CA's own responsibility to judge whether the CPS meets the requirements in this CPS, or to trust the statement of compliance by the CA.

5.8.5. Actions taken as a result of deficiency

Any discrepancies between a CA's operation and a stipulation of its CP's /CPS must be noted and immediately notified to the Certipost CErtification PRactices Council (CEPRAC). The CEPRAC will determine a remedy, including a time for completion.

Any remedy may include permanent or temporary CA cessation, but several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes and the disruption to the Certificate using community.

Any remedy may include that other certifying CA's may:

Immediately revoke cross certification Certificates of the CA,

Allow the CA to continue operations for thirty days pending correction of any problems prior to revocation, or

Indicate the irregularities, but allow the CA to continue operations until the next audit without revocation.

The decision regarding what actions to take will be based on previous response to problems, the severity of the irregularities, and the recommendations from the auditor.

If a cross Certificate of another CA is revoked, the CA shall immediately update the Authority Revocation List. Depending on the situation, contractual agreements, applicable laws and regulations, the CA may have to notify all its Subscribers and indicate how it will proceed.

5.8.6. Communication of results

a) Conclusive results of the audits shall be distributed to the audited RA, the audited CA, and to the Certipost CErtification PRactices Council (CEPRAC). Conclusive result is here defined to be the information of all irregularities which may affect a relying party's trust in a Certificate, including an adequate judgment of its level of seriousness but excluding detailed information that can be used to attack the system.

b) In accordance with section 2.7.5., any CA or RA found not to be in compliance with this CPS shall be notified immediately at the completion of the audit. Required remedies shall be defined and communicated to such CA or RA as soon as possible to limit the risks. The implementation of remedies shall be communicated to the Certipost CErtification PRactices Council (CEPRAC). A special audit may be required to confirm the implementation of the effectiveness of the remedy.

5.9. Other business and legal matters

5.9.1. Fees

5.9.1.1. Certificate issuance or renewal fees

Fees are subject to change and are published on the Certipost web site. (www.certipost.com) or in subscriber agreements.

Fees can be based on a subscription for a period of time. In that case the fees for issuance and / or renewal are fixed by the purchasing agreement for the specified period of time.

5.9.1.2. Certificate access fees

Access to published certificates does not impose a fee payable to Certipost. All costs to make this access (e.g. on-line transfer) are to be incurred by the party which accesses the certificates.

5.9.1.3. Revocation or status information access fees

Access to revocation or status information does not impose a fee payable to Certipost. All costs to make this access (e.g. on-line transfer) are to be incurred by the party which accesses the revocation or status information.

5.9.1.4. Fees for other services

a) Fees are provided by Certipost on a regularly updated pricing sheet.

b) No fees related to policy information, other than those covering reasonable media reproduction and distribution costs, may be charged for supplying existing on-line or physical media copies of this CPS or for supplying on-line copies of a CP supported by this CPS.

5.9.1.5. Refund policy

Not applicable, except if a specific agreement is made

5.9.2. Financial responsibility

5.9.2.1. Insurance coverage

The CSP is duly insured to cover general financial responsibility.

5.9.2.2. Other assets

No general provisions are made. Specific provisions can be made for particular contractual agreements.

5.9.2.3. Insurance or warranty coverage for end-entities

No general provisions are made. Specific provisions can be made for particular contractual agreements.

5.9.3. Confidentiality of business information

5.9.3.1. Scope of confidential information

a) It is recommended that a certificate does not contain information that is not necessary for its effective use, such that no sensitive information is contained therein.
b) Certipost Certification Services may request not-to-be-certified information to be used in managing the Certificates, or for billing purposes, or for archiving purposes, or for any other reason, such as imposed by law. This information may contain sensitive information or personal data. The protection of the storage of these data shall be assured so that this remains confidential at all times in accordance to the data privacy law, and other applicable laws. The personal data which is supplied to Certipost or to the Local Registration Authority (paper or electronic information) by the Certificate Holder in the context of the Certificate request and delivery are duly incorporated, archived and protected according to the Belgian privacy law, in the files of CERTIPOST s.a./n.v., Centre Monnaie - Munt Centrum, 1000 Brussels. The data will be used for the provisioning of the Certipost PKI services. The Subscriber has the right to access and correct this data, and to refuse, on demand and without fees, any usage of this information for direct marketing purposes.
c) All information in the CA or RA records (not repository) shall be handled as sensitive, and access shall be restricted to those with official needs. Any personal or corporate information held by CA's or RA'S which is not appearing on issued Certificates is considered confidential and shall not be released without the prior consent of the Subscriber, unless required otherwise by law. Records that contain sensitive information shall have access control protection in place commensurate with the information to be protected.
d) No one, at all times, shall have access to a private signing key but the owner of the corresponding certificate; it is recommended that the owner is prevented from viewing its Private Keys in unencrypted form.
e) All Private Keys used and handled within the CA operation under this CPS are to be kept confidential.
f) Audit logs and records shall not be made available as a whole, except as required by law. Only records of individual transactions may be released according to this CPS.

5.9.3.2. Information not within the scope of confidential information

a) Certificates, CRL's, revocation/suspension information and any information available on http://www.certipost.com are not considered confidential.
b) Identification information or other personal or corporate information appearing on Certificates is not considered confidential.

5.9.3.3. Responsibility to protect confidential information

All participants that receive confidential information are under the obligation to secure it from compromise, and refrain from using it or disclosing it to third parties.

5.9.4. Privacy of personal information

5.9.4.1. Privacy plan

The applicable privacy plan that applies to a CSP or a subcontractor's activities will be recorded and reviewed to be in conformance with the CPS if this is needed and if required by applicable law or policy.

5.9.4.2. Information treated as private

Information that does not appear in the certificate or is not used for certificate management and token management services is considered as private.

5.9.4.3. Information not deemed private

See previous section.

5.9.4.4. Responsibility to protect private information

All information that is considered as private is subject to the applicable privacy plan. Participants that receive private information are obliged by contract to secure it, and refrain from using it and from disclosing it to third parties.

Information objects in certificates issued under this CPS and applicable CPs are regarded as personal data of the Subscriber. In order to carry out its tasks in an efficient manner, Certipost uses databases with these personal data. In this regard, Certipost respects the privacy of the persons concerned. The Subscriber authorizes Certipost to publish such personal data on its repositories.

5.9.4.5. Notice and consent to use private information

Any use of private information requires consent from individuals to whom this information refers. General consent can be given by accepting the General Terms and Conditions (GTC). This consent is preserved either explicitly by means of signed contracts or implicitly by making use of the Certipost Token Manager, in which the acceptance of the GTM is logged in audit trails.

5.9.4.6. Disclosure pursuant to judicial or administrative process

Any circumstances under which a participant is required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding must be demonstrated and the authorization will be archived by the CSP.

5.9.4.7. Other information disclosure circumstances

Other information disclosure circumstances must be approved by the individuals concerned or by the Certipost CErtification PRactices Council (CEPRAC) in accordance with legal restrictions.

5.9.5. Intellectual property rights

The present CPS and the applicable CPs are the property of Certipost and are protected by intellectual property rights, unless otherwise agreed. Any use not allowed by the CPS and the applicable CPs may entail civil and criminal proceedings.

5.9.6. Representations and warranties

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.7. Disclaimers of warranties

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.8. Limitations of liability

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.9. Indemnities

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.10. Term and termination

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.11. Individual notices and communications with participants

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.12. Amendments

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.13. Dispute resolution provisions

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.14. Governing law

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.15. Compliance with applicable law

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.16. Miscellaneous provisions

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.

5.9.17. Other provisions

This section refers to a section in the general terms and conditions or can be supplemented by additional contractual agreements.