Certipost E-Trust Services

Certification Practice Statement for Qualified, Normalised and Lightweight Certificates CERTIPOST CPS

O.I.D. 0.3.2062.7.1.0.1.2.0

Version 2.0

Publication Date:
15 August 2006
Effective Date:
31 August 2006

TABLE OF CONTENTS

DEFINITIONS

The 09 July 2001 Law	Belgian electronic signature law implementing the European Directive, published on 29 September 2001.
Activation Data	Data values, other than keys, that are required to use smart cards and that need to be protected (e.g. PIN and pass phrase).
Advanced Electronic Signature or Advanced Digital Signature	Electronic data, attached or logically linked to other electronic data, enabling authentication method and satisfying the following conditions: • Be uniquely linked to the signatory • Allow identification of the signatory • Be created by means that the signatory is the only person to control • Be linked to the correspondent electronic data so that any later modification of the data can be detected.
Certipost or Certipost E-Trust	Certipost SA/NV, with registered offices in Muntcentrum ,B-1000 Brussels, Belgium
Certipost E-Trust Infrastructure	The Certipost Public Key Infrastructure that is deployed by Certipost to provide the Certipost E-Trust Certification Services.
Certipost E-Trust PKI Certification Practices Council	The Policy Approval Authority within Certipost E-Trust is called the Certipost E-Trust PKI Certification Practices Council (CePraC). It is the high level management body with final authority and responsibility for – Specifying and approving the Certipost E-Trust infrastructure and practices. – Approving the Certipost E-Trust Certification Practice Statement(s) and Certipost E-Trust Certificate Policies. – Defining the review process for certification practices and Certificate Policies including responsibilities for maintaining the Certification Practice Statements and Certificate Policies. – Defining the review process that ensures that the certificate practices are properly implemented by the CAs. – Defining the review process that ensures that the Certificate Policies are supported by the CAs Certification Practice Statement(s). – Publication to the Subscribers and relying parties of the Certificates Policies and Certification Practice Statements and their revisions. – Specifying cross-certification procedures and handling cross-certification requests.
Certipost E-Trust Services	The Certipost Certification services.
Certipost E-Trust Enterprise Program	This program consists in providing corporate customers with a dedicated *Certipost E-Trust sub-Infrastructure*. This will imply usually the set up of an Enterprise CA and subordinate RA(s).
Electronic Signature	Electronic data, attached or logically linked to other electronic data and enabling authentication method.
Certipost E-Trust RA Procedures and Guidelines	Procedures and Guidelines that must be strictly followed by Registration Authorities (Central or Local) in the context of the Certipost E-Trust Services.
Certipost E-Trust Certificate Public Registry	The electronic registry used by Certipost E-Trust Services to publish the issued Certificates and Certificate Revocation Lists.
Certificate	An electronic statement that maps the signature verification data to a physical, a moral person or an entity and confirms the identity of this person or entity (subject).
Certificate Holder	A physical or moral person (subject) to which a Certification Service

	Provider has delivered a Certificate.
Certificate Policy	A named set of rules that indicate the applicability of a Certificate to a particular community and/or class of application with common security requirements.
Certificate Public Registry	The repository that hold the publicly available certificates, CRL's and ARL's, issued by the Certipost E-Trust CA's.
Certification Authority (CA)	The entity that issues Certificates by signing Certificate data with its Private Signing Key according to this CPS.
Certification Authority Auditor (CAA)	The Certipost E-Trust Internal CA Auditor that audits the operations of the CA related Entities.
Certification Practice Statement (CPS)	A statement of the practices, which a Certification Service Provider applies for the issuing of Certificates.
Certificate Revocation List (CRL)	A published list of the suspended and revoked Certificates.
Certification Service Provider	Any physical or moral person which delivers and manages Certificates or provides other services related to electronic signatures. In the context of this CPS, the Certification Service Provider is Certipost s.a./n.v., with registered offices in Muntcentrum ,B-1000 Brussels, Belgium.
European Directive(The)	The European Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 ***"on a community framework for electronic signature".***
Lightweight Certificate	A Certificate that is issued according to the requirements of the ETSI technical standard TS 102 042 Lightweight Certificate Policy (LCP), incorporating less demanding policy requirements than the Normalised Certificate and used to support any usage **but** Qualified Electronic Signatures of a cryptographic key pair whose corresponding public key pair is certified. The certified key usage's can be any or any mix of the following usage's: encryption, authentication, non-Qualified signatures, etc.
Normalised Certificate	A Certificate that is issued according to the requirements of the ETSI technical standard TS 102 042 Normalised Certificate Policy (either NCP or NCP+), and used to support any usage **but** Qualified Electronic Signatures of a cryptographic key pair whose corresponding public key pair is certified. The certified key usage's can be any or any mix of the following usage's: encryption, authentication, non-Qualified signatures, etc. The Normalised Certificate Policy offers the same quality as that offer by the Qualified Certificate as defined in ETSI TS 101 456 but without the legal constraints implied by the European Directive, with (NCP+) or without (NCP) requiring use of Secure User Device (signing or decrypting).
Private Key	The private part of an asymmetric key pair used for Public Key encryption techniques. The Private Key is typically used for creating digital signatures or decrypting messages.
Private Signing Key	A Private Key that is exclusively used for signing data.
Public Key	The public part of an asymmetric key pair used for Public Key encryption techniques. The Public Key is typically used for verifying digital signatures or to encrypt messages to the owner of the Private Key.
Registration Authority (RA)	An entity, constituted of as an example, but not limited to a Central Registration Authority (CRA) or Local Registration Authority (LRA), that undertakes to identify and authenticate Subscribers on behalf of a CA.
Qualified Certificate	A Certificate that is used exclusively to support electronic signature and that complies to the requirements of Annex I of the 09 July 2001 Law Annex I and is delivered by a Certification Service Provider that satisfies to the Annex II of the 09 July 2001 Law, and by referencing the technical standard ETS TS 101 456, the technical standard ETSI TS 101 862 ***"Qualified Certificate profile"*** and the RFC 3739 ***"Internet X.509 Public Key Infrastructure Qualified Certificate Profile".***
Qualified Electronic Signature or Qualified Digital Signature	Electronic Signature that satisfies the Article 5.1 of The European Directive and Article 2, 2° of the 09 July 2001 Law.

Relying Party	A person, an organisation or a computer system that is a Subscriber or user of a Certificate but is not a CA or a RA. An end entity is a Subscriber, a relying party, or both.
Secret key	A key used in symmetric encryption where the sender and receiver of encrypted messages use the same secret key.
Secure Signature Creation Device	A software or hardware device that is configured to apply the Signature Creation Data and that satisfies the requirements of the Annex III of the European Directive and of the 09 July 2001 Law.
Secure User Device	Device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Signature Creation Data	Unique data, such as codes or cryptographic Private Keys, used by the signatory to create an advanced electronic signature.
Signature Creation Device	Means configured software or hardware used to implement the Signature Creation Data.
Signature Verification Data	Data, such as codes or cryptographic Public Keys, that are used to verify an Advanced Electronic Signature.
Signature Verification Device	A software or hardware device that is configured to apply the Signature Creation Data
Subject	An entity identified in a Certificate as the holder of the Private Key associated with the Public Key given in the Certificate.
Subscriber	An entity that requests a Certificate and subscribes with a Certification Service Provider (or CA) on behalf of the Subject. The Subscriber may or may not be the Subject (e.g., a physical person, the Subscriber, requesting a Certificate on behalf of a moral person, the Subject).
Suspension and Revocation Authority (SRA)	An Authority that suspends, unsuspends and/or revokes Certificates on behalf of the CA.

ABBREVIATIONS

AES	Advanced Electronic Signature
ARL	Authority Revocation List
CEPRAC	Certipost E-Trust PKI Certification Practices Council
CA	Certification Authority
CAO	Certification Authority Officer
CAA	Certification Authority Auditor
CP	Certificate Policy
CPS	Certification Practice Statement
CRA	Central Registration Authority
CRAO	Central Registration Authority Officer
CRL	Certificate Revocation List
CSP	Certification Service Provider
DAP	Directory Access Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transport Protocol
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
LRAO	Local Registration Authority Officer
NCP	Normalised Certificate Policy
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PKCS	Public Key Certificates Standard
PSE	Personal Security Environment
QCP	Qualified Certificate Policy
RA	Registration Authority
RAO	Registration Authority Officer
RFC	Request For Comments
RSA	A specific Public Key algorithm invented by Rivest, Shamir, and Adleman
SMK	Storage Master Key
SRA	Suspension and Revocation Authority
SRAO	Suspension and Revocation Authority Officer
SSCD	Secure Signature Creation Device
SSL	Secure Socket Layer
SUD	Secure User Device
URL	Uniform Resource Locator

STRUCTURE AND INTERPRETATION OF CERTIPOST E-TRUST CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED & NORMALISED CERTIFICATES (HEREINAFTER REFERRED TO AS "Q&N CPS")

This Q&N CPS is based on the "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework" of the Network Working Group (http://www.ietf.org/html.charters/pkix-charter.html), informational request for comment, RFC 2527, of March 1999.

For the interpretation of the present Q&N CPS, the following guidelines apply:

a) The international standardisation process influences the titles and subtitles of this Q&N CPS. In interpreting this Q&N CPS the text under each title shall be given precedence over the wordings in the titles.

b) Reference of Q&N CPS locations has to be done in the following manner. First the Q&N CPS name has to be provided, followed by the heading numbering and the section/subsection numbering. For instance: Certipost E-Trust Q&N CPS v2.0, section 1.3.2/c3

c) Text parts forming requirements on Certification Service Provider (CSP)'s practices, procedures and responsibilities are numbered from a, b, c etc.

d) As a general rule the CSP, acting in accordance with this Q&N CPS, shall undertake adequate measures to fulfill all requirements in this Q&N CPS. When a section is marked with "Not applicable", it means that this section is not applicable to Certipost E-Trust Services Q&N CPS.

e) Certipost E-Trust presents the current Q&N CPS in such a structure that allows Certipost E-Trust CSP to issue and manage Certificates under more than one Certificate Policy (CP). The document describes the certification practices, which form the basis from which Certipost E-Trust Q&N CSP will issue Certificates under the Qualified, Normalised and Lightweight labels.

1 INTRODUCTION

1.1 Overview

Since 19th December 2003, Certipost sa/nv has taken over the activities and responsibilities of Belgacom (E-Trust) with regards to the activities of Certification Service Provider formally known under the brand name "E-Trust". At the creation of Certipost (23/12/2002), the entire Belgacom E-Trust activity has been transferred to Certipost. Since 19/12/2003, Certipost acts as Certification Service Provider having entirely taken over the Belgacom E-Trust activities; Certipost has thus endorsed all Belgacom E-Trust duties and responsibilities in that matter.

In order to comply with the 9th July 2001 Law, and in order to ensure the business continuity of the E-Trust services to the former Belgacom customers, Certipost takes over the responsibility of Certification Service Provider on the certificates issued under the Belgacom E-Trust CA's before and after the date of 19th December 2003, thus including all certificates that may be issued from that date under this infrastructure.

In other words, any certificate that is issued by an E-Trust CA, either under the brand name Belgacom E-Trust or the brand name Certipost E-Trust, will fall under the responsibility of Certipost sa/nv to the extent of the 9th July 2001 Law.

The Certipost E-Trust Certification Practice Statement for Qualified & Normalised Certificates (hereinafter referred to as "Q&N CPS") aims to describe the practices, which Certification Authorities within the Certipost E-Trust Infrastructure (hereinafter referred to as: "CA's") employ in issuing Qualified digital Certificates, Normalised digital Certificates, or Lightweight digital Certificates.

CA's within the Certipost E-Trust PKI issue a wide range of Certificate types, differing in application field and the community and/or class of application. The set of rules and security requirements that apply to the use of each particular type of Certificate is set forth in a number of associated Certificate Policies (hereinafter referred to as: "CP").

The Certipost E-Trust "Q&N CPS", as well as the associated CP's, shall be reflected in contracts between a CA and Subscribers. Furthermore, a relying party may use the CP in order to determine the level of trustworthiness of the offered Certificate.

The following sub-section describes the Certipost E-Trust PKI architecture.

1.1.1 Certipost E-Trust PKI hierarchy

Certipost E-Trust has a CA hierarchy beginning at the top level with the "Certipost E-Trust Top Root CA", issuing only Primary Sub-CAs' Certificates, and related ARL's. Three Primary CAs are composing this Primary level, respectively the "Certipost E-Trust Primary Qualified CA", the "Certipost E-Trust Primary Normalised CA", and the "Certipost E-Trust Primary Lightweight CA". These Primary CA's are respectively used for issuing only Secondary Sub-CAs' Certificates, and related ARL's. These Secondary CA's are operational CA's issuing end-entities certificates and the related CRL's. This infrastructure is consistent with the PKIX / X.509 standard.

The following figure depicts the current Certipost E-Trust PKI hierarchy:

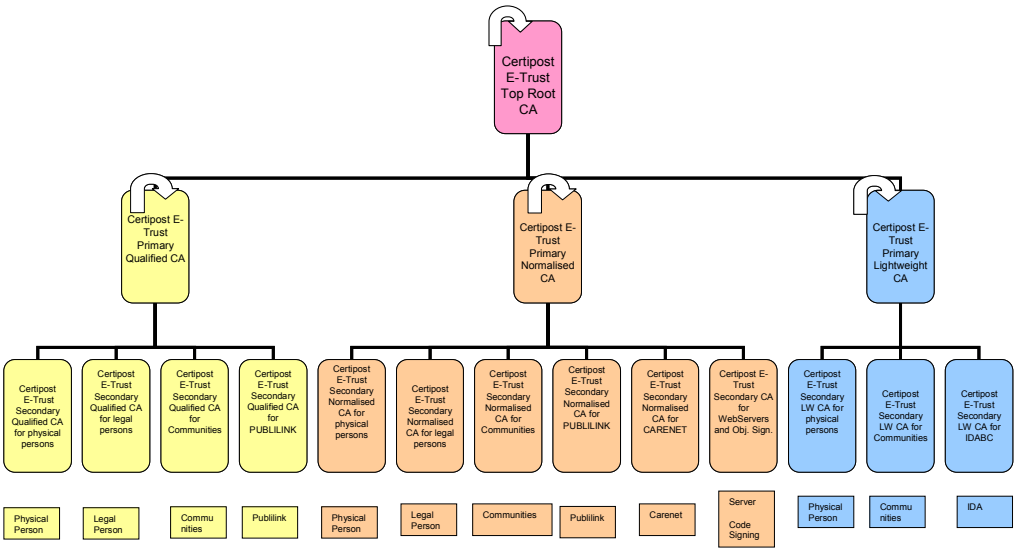

Figure 1: Certipost E-Trust PKI Hierarchy

1.1.1.1 Certipost E-Trust TOP Root CA

This Top Root CA issues new CA Certificates to and only to Primary CA's dedicated either to the issuing of Qualified Certificates, or Normalised Certificates, or Lightweight Certificates. The corresponding Top Root CA Certificate must be included in all certification paths (when possible):

Self-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust TOP Root CA	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust TOP Root CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2025 11:00:00	
Serial number: 04 00 00 00 00 01 05 52 64 c1 95	
Thumbprint (SHA-1): 05 60 a2 c7 38 ff 98 d1 17 2a 94 fe 45 fb 8a 47 d6 65 37 1e	

This infrastructure is consistent with the PKIX / X.509 standard.

As shown on the figure above, there are currently only three Primary Sub-CAs:

- Certipost E-Trust Primary Qualified CA,
- Certipost E-Trust Primary Normalised CA,
- Certipost E-Trust Primary Lightweight CA .

1.1.1.2 Certipost E-Trust Primary CAs

1.1.1.2.1 Certipost E-Trust Primary Qualified CA

The Certipost E-Trust Primary Qualified CA issues new CA Certificates to and only to Secondary Qualified CA's dedicated to the issuing of Qualified Certificates to end-entities..

Self-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Qualified CA	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Qualified CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2020 11:00:00	
Serial number: 04 00 00 00 00 01 05 52 64 c4 25	
Thumbprint (SHA-1) 74 2c df 15 94 04 9c bf 17 a2 04 6c c6 39 bb 38 88 e0 2e 33	

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Qualified CA	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust TOP Root CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2020 11:00:00	
Serial number: 04 00 00 00 00 01 05 52 64 c5 5d	
Thumbprint (SHA-1): 01 06 69 fd f8 f1 5d a4 97 dd fd f8 84 44 6e 47 cf d4 25 81	

1.1.1.2.2 Certipost E-Trust Primary Normalised CA

The Certipost E-Trust Primary Normalised CA issues new CA Certificates to and only to Secondary Normalised CA's dedicated to the issuing of Normalised Certificates to end-entities..

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust TOP Root CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2020 11:00:00	
Serial number: 04 00 00 00 00 01 05 52 64 c8 b9	
Thumbprint (SHA-1): 44 d2 b4 55 54 ff 21 d9 8c 03 2e fa e3 a7 2f 5a 8e 4a 52 90	

Self-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA

Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2020 11:00:00
Serial number: 04 00 00 00 00 01 05 52 64 c7 61
Thumbprint (SHA-1): a5 9c 9b 10 ec 73 57 51 5a bb 66 0c 4d 94 f7 3b 9e 6e 92 72

1.1.1.2.3 Certipost E-Trust Primary Lightweight CA

The Certipost E-Trust Primary Lightweight CA issues new CA Certificates to and only to Secondary Lightweight CA's dedicated to the issuing of Lightweight Certificates to end-entities..

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Lightweight CA	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust TOP Root CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2020 11:00:00	
Serial number: 04 00 00 00 00 01 05 52 64 cb b6	
Thumbprint (SHA-1): 37 fc d7 86 a4 25 10 d0 da 4f 8c 7a e7 93 72 7e bb eb 04 be	

Self-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Lightweight CA	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Lightweight CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2020 11:00:00	
Serial number: 04 00 00 00 00 01 05 52 64 ca 8d	
Thumbprint (SHA-1): 02 17 be 6a 14 c7 86 9b 9e d4 48 ee 02 8e 8f e2 fd b8 cf e9	

1.1.1.3 Certipost E-Trust Secondary Qualified CAs

The Certipost E-Trust Primary Qualified CA issues new CA Certificates to and only to Secondary Qualified CAs. There are four (4) of these Certipost E-Trust Secondary Qualified CAs:

- Secondary Qualified CA for Physical Persons
- Secondary Qualified CA for Legal Persons
- Secondary Qualified CA for Communities
- Secondary Qualified CA for Publilink

These Secondary Qualified CAs issues Qualified Certificates to end-entities.
This infrastructure is consistent with the PKIX / X.509 standard.

1.1.1.3.1 Certipost E-Trust Secondary Qualified CA for Physical Persons

The Certipost E-Trust Secondary Qualified CA for Physical Persons issues Qualified Certificates to and only to physical persons as end-entities.

Root-signed certificate

Subject:	Issuer:

C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Qualified CA for Physical Persons	C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Qualified CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 b6 d3	
Thumbprint (SHA-1): 5f 2d 3e 9b 05 93 66 3c c2 d8 c1 95 e7 4c 95 4d c1 f9 8e ab	

1.1.1.3.2 Certipost E-Trust Secondary Qualified CA for Legal Persons

The Certipost E-Trust Secondary Qualified CA for Legal Persons issues Qualified Certificates to and only to legal persons as end-entities.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Qualified CA for Legal Persons	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Qualified CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 b9 c1	
Thumbprint (SHA-1): f8 e3 d0 3d d6 73 b1 2d b7 c5 98 39 c0 e2 f1 ef 6b 45 6f a1	

1.1.1.3.3 Certipost E-Trust Secondary Qualified CA for Communities

The Certipost E-Trust Secondary Qualified CA for Communities issues Qualified Certificates to and only to physical person end-entities who are part of a Community.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Qualified CA for Communities	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Qualified CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 bb 76	
Thumbprint (SHA-1): 7b b5 76 43 51 9f be 2e 4e a8 2f cd 0c 10 8e dd 74 48 1c dd	

1.1.1.3.4 Certipost E-Trust Secondary Qualified CA for Publilink

The Certipost E-Trust Secondary Qualified CA for Publilink issues Qualified Certificates to and only to physical persons who are part of, or in the context of the Publilink project (http://publilink.gkb-ccb.be/).

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v.	Issuer: C = BE O = Certipost s.a./n.v.

CN = Certipost E-Trust Secondary Qualified CA for Publilink	CN = Certipost E-Trust Primary Qualified CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 bd 99	
Thumbprint (SHA-1): 3f 57 a4 a1 a2 27 11 f9 8b e6 ea 77 65 2d 66 1d ea 59 7a 04	

1.1.1.4 Certipost E-Trust Secondary Normalised CAs

The Certipost E-Trust Primary Normalised CA issues new CA Certificates to and only to Secondary Normalised CAs. There are six (6) of these Certipost E-Trust Secondary Normalised CAs:

- Secondary Normalised CA for Physical Persons
- Secondary Normalised CA for Legal Persons
- Secondary Normalised CA for Communities
- Secondary Normalised CA for Publilink
- Secondary Normalised CA for Carenet
- Secondary Normalised CA for Web-Servers and Object Signing.

These Secondary Normalised CAs issues Normalised Certificates to end-entities.
This infrastructure is consistent with the PKIX / X.509 standard.

1.1.1.4.1 Certipost E-Trust Secondary Normalised CA for Physical Persons

The Certipost E-Trust Secondary Normalised CA for Physical Persons issues Normalised Certificates to and only to physical persons as end-entities.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Normalised CA for Physical Persons	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 c8 96	
Thumbprint (SHA-1): 07 ab cb 99 f4 a8 db 4d ba a0 78 d6 9f 7c 0f 74 3e bf 7e 2d	

1.1.1.4.2 Certipost E-Trust Secondary Normalised CA for Legal Persons

The Certipost E-Trust Secondary Normalised CA for Legal Persons issues Normalised Certificates to and only to legal persons as end-entities.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Normalised CA for Legal Persons	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	

Serial number: 04 00 00 00 00 01 05 53 83 ca 2c
Thumbprint (SHA-1): 48 14 a0 f0 91 36 e0 cf 61 97 c2 f9 12 25 6d 92 6c 82 13 7a

1.1.1.4.3 Certipost E-Trust Secondary Normalised CA for Communities

The Certipost E-Trust Secondary Normalised CA for Communities issues Normalised Certificates to and only to physical person end-entities who are part of a Community.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Normalised CA for Communities	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 cb e1	
Thumbprint (SHA-1): 2a 87 0b f2 b4 55 5f 6c 62 5c e8 62 1f 0f f2 87 29 d4 b5 63	

1.1.1.4.4 Certipost E-Trust Secondary Normalised CA for Publilink

The Certipost E-Trust Secondary Normalised CA for Publilink issues Normalised Certificates to and only to physical persons who are part of, or in the context of the Publilink project (http://publilink.gkb-ccb.be/).

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Normalised CA for Publilink	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 cd 97	
Thumbprint (SHA-1): 60 8f 80 4e e5 cf 79 71 ee 13 37 dd c8 ac 7e 32 06 86 08 67	

1.1.1.4.5 Certipost E-Trust Secondary Normalised CA for Carenet

The Certipost E-Trust Secondary Normalised CA for Carenet issues Normalised Certificates to and only to end-entities who are part of, or in the context of the Carenet project (http://www.carenet.be).

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Normalised CA for Carenet	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 cf 5c	

Thumbprint (SHA-1): 3c 9b 10 6b 35 4f 92 61 6b c8 e9 33 ca e1 c5 f2 86 40 e6 31

1.1.1.4.6 Certipost E-Trust Secondary Normalised CA for Web-Servers and Object Signing

The Certipost E-Trust Secondary Normalised CA for Web-Servers and Object Signing issues Normalised Certificates to and only to web-servers or object signing entities.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Normalised CA for Web-Servers and Object Signing	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Normalised CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 d1 11	
Thumbprint (SHA-1): 39 d6 32 84 4e f5 5d e8 54 ea f9 a0 b2 64 e0 51 a6 7d f9 3c	

1.1.1.5 Certipost E-Trust Secondary Lightweight CAs

The Certipost E-Trust Primary Lightweight CA issues new CA Certificates to and only to Secondary Lightweight CAs. There are three (3) of these Certipost E-Trust Secondary Lightweight CAs:

- Secondary Lightweight CA for Physical Persons
- Secondary Lightweight CA for Communities
- Secondary Lightweight CA for IDABC

These Secondary Lightweight CAs issues Lightweight Certificates to end-entities.
This infrastructure is consistent with the PKIX / X.509 standard.

1.1.1.5.1 Certipost E-Trust Secondary Lightweight CA for Physical Persons

The Certipost E-Trust Secondary Lightweight CA for Physical Persons issues Lightweight Certificates to and only to physical persons as end-entities.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Lightweight CA for Physical Persons	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Lightweight CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 dd a4	
Thumbprint (SHA-1): 70 a5 73 5f 8a 07 b4 e3 69 1a 4a 88 46 de 07 f4 dc d6 15 3d	

1.1.1.5.2 Certipost E-Trust Secondary Lightweight CA for Communities

The Certipost E-Trust Secondary Lightweight CA for Communities issues Lightweight Certificates to and only to physical person end-entities who are part of a Community.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Lightweight CA for Communities	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Lightweight CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 df 79	
Thumbprint (SHA-1): c2 72 51 78 9b 0a 24 7b aa d0 a2 4d 9a 70 cb d3 6c bb b6 e7	

1.1.1.5.3 Certipost E-Trust Secondary Lightweight CA for IDABC

The Certipost E-Trust Secondary Lightweight CA for IDABC issues Lightweight Certificates to and only to end-entities who are part of, or in the context of the IDABC project.

Root-signed certificate

Subject: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Secondary Lightweight CA for Legal Persons	Issuer: C = BE O = Certipost s.a./n.v. CN = Certipost E-Trust Primary Lightweight CA
Valid from : 26 July 2005 11:00:00 Valid to : 26 July 2015 11:00:00	
Serial number: 04 00 00 00 00 01 05 53 83 e1 0f	
Thumbprint (SHA-1): a5 3b 63 54 37 35 13 12 1e f3 d9 e4 44 cc a3 e8 4c a2 92 e9	

1.2 Identification

1.2.1 Identifiers for Certification Practice Statement

Identifiers for the Certipost E-Trust Certification Practice Statement for Qualified & Normalised Certificates are:

Certification Practice Statement Name:

CertipostETrustCertificationPracticeStatementForQualifiedAndNormalisedCertificateVersion2:0

Object Identifier:

0.3.2062.Certipost (7) E-Trust(1).CPS(0).QNCPS(1).Version(2).Sub-version(0)

1.2.2 Identifier for Certificate Policies

Identifiers for Qualified Certificates policies as stated by ETSI TS 101 456 are defined in the next subsections, identifiers for Normalised and Lightweight Certificates policies as stated by ETSI TS 102 042 are defined in the second subsection, while the third subsection describes the additional Certificate Policies used by Certipost E-Trust to rule the issuing of Qualified, Normalised or Lightweight digital Certificates.

1.2.2.1 Qualified Certificate Policies (QCP)

Identifiers for Qualified Certificates policies as stated by ETSI TS 101 456 are defined in the next two subsections.

1.2.2.1.1 QCP public with SSCD (QCP+)

A Certificate policy for Qualified Certificates issued to the public, requiring use of SSCD

Itu-t(0) identified-organization(4) etsi(0) Qualified-Certificate-policies(1456) Policy-identifiers(1) qcp-public-with-sscd(1)

1.2.2.1.2 QCP public

A Certificate policy for Qualified Certificates issued to the public

Itu-t(0) identified-organization(4) etsi(0) Qualified-Certificate-policies(1456) Policy-identifiers(1) qcp-public (2)

1.2.2.2 Normalised and Lightweight Certificate Policies (NCP and LCP)

Identifiers for Normalised and Lightweight Certificates policies as stated by ETSI TS 102 042 are defined in the next two subsections.

1.2.2.2.1 NCP without SSCD (NCP)

A Certificate policy for Normalised Certificate, not requiring use of SSCD

Itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) Policy-identifiers(1) ncp(1)

1.2.2.2.2 NCP with SSCD (NCP+)

A Certificate policy for Normalised Certificate, requiring use of SSCD

Itu-t(0) identified-organization(4) etsi(0) other-certificate-policies (2042) Policy-identifiers(1) ncp+(2)

1.2.2.2.3 LCP

A Certificate Policy for Lightweight Certificates

Itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) Policy-identifiers(1) lcp(3)

1.2.2.3 Current Certipost E-Trust Qualified, Normalised and Lightweight Certificates Policies

The current Certificate Policies used by Certipost E-Trust to rule the issuing of Qualified, Normalised or Lightweight digital Certificates are described in the next subsections, and here below summarised:

- CP used to rule the issuing of digital Qualified, Normalised or Lightweight Certificates for Physical Persons.
- CP used to rule the issuing of digital Qualified or Normalised Certificates for Legal Persons.
- CP used to rule the issuing of digital Qualified, Normalised or Lightweight Certificates for Communities.
- CP used to rule the issuing of digital Qualified or Normalised digital Certificates for the Publilink project .
- CP used to rule the issuing of digital Normalised digital Certificates for the Carenet project (www.carenet.be).
- CP used to rule the issuing of Normalised SSL Webserver digital Certificates
- CP used to rule the issuing of Normalised Code Signing digital Certificates
- CP used to rule the issuing of Lightweight digital Certificates for the IDABC project:

- for the DubliNET CUG functional mailboxes (EC regulation 343/2003)
- for the European Commission (IDA sectoral networks)
- for the Justice and Home affair DG CUG functional mailboxes (EC regulation 2725/2000)

1.2.2.3.1 Certipost E-Trust Qualified, Normalised and Lightweight Certificate Policy for Physical Persons

	Certipost OID[1]	Summary
E-Trust Qualified Certificate for Physical Person with SSCD and Key Generation by CSP (1/2/5 years validity, 1024-bit key size)	Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Certipost OID : **0.3.2062.7.1.1.101.x**	This type of digital Certificates provides a very high degree of assurance about the Certificate holder's personal and, where applicable, professional electronic identity. For a Certificate to be issued, the individual applying for the Certificate must present himself in person during the registration process or must already dispose of a Certificate of a similar level. This Certificate provides a strong guarantee of the link between the personal identity of the Certificate holder (physical person), any professional status (not obligatory), the Public Key and its authorized use. For the application to be validated, the person applying for the Certificate must submit proof of his identity, and any documents valid as proof of his professional status and of any related information requiring certification, as required by the applicable CP (see applicable CP for details). A Public Key certified in this manner may be used solely in one of the following two cases: • A Qualified Digital Signature context: in such a case, the Qualified Certificate satisfies the "**Qualified Certificate"** requirements in the sense of The Directive and its transposition in The 09 July Belgian Law, and of the technical standard ETSI TS 101 456. The Certificate can be used for an Advanced or a Qualified Signature, the latest being automatically equivalent to the handwritten signature ; or (exclusive or) • A context of any usage but Qualified Digital Signature (e.g., normalised digital signature, encryption and/or authentication, or any combination of these, etc.). In such a case, the Normalised Certificate satisfies the "**Normalised Certificate"** requirements in the sense of the technical standard ETSI TS 102 042. The CSP(s) authorized to issue the Certificates under the applicable CP shall specify whether it/they certifies/certify the compliance of these Certificates with this policy and the regulatory documents or whether these Certificates have been certified as complying therewith. The Certification Service Providers (CSPs), authorised to issue Certificates under the applicable CP, indicate whether they claim to comply to the CP and to the relevant regulatory documents or whether they have been certified to be compliant. This Certificate type constitutes a very high level of professional electronic identity that can be used to secure high level security applications such as electronic signature operations or
E-Trust Qualified Certificate for Physical Person without SSCD and Key Generation by CSP (1/2/5 years validity, 1024-bit key size)	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Certipost OID : **0.3.2062.7.1.1.102.x**	
E-Trust Qualified Certificate for Physical Person without SSCD and Key Generation by Owner (1/2/5 years validity, 1024-bit key size)	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Certipost OID : **0.3.2062.7.1.1.103.x**	
E-Trust Normalised Certificate for Physical Person with SSCD and Key Generation by CSP (1/2/5 years validity, 1024-bit key size)	Normalised Certificate with SSCD (OID ETSI 102 042): **0.4.0.2042.1.2** and Certipost OID : **0.3.2062.7.1.1.201.x**	
E-Trust Normalised Certificate for Physical Person without SSCD and Key Generation by CSP (1/2/5 years validity, 1024-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID : **0.3.2062.7.1.1.202.x**	

[1] ***x*** corresponds to the version number of the O.I.D. of the corresponding Certificate Policy.

E-Trust Normalised Certificate for Physical Person without SSCD and Key Generation by Owner (1/2/5 years validity, 1024-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID : **0.3.2062.7.1.1.203.x**	encryption/authentication. These Certificates (and the related Key Pair) used for Qualified Digital Signatures and for Normalised purposes (e.g., encryption and/or authentication) are always distinct (separate key pairs). The Certificates issued under the applicable CP are not exclusively dedicated to be used with a Secure Signature Creation Device (SSCD). The Certificates issued under the applicable CP include one or several CP identifiers that can be used by relying parties in order to determine the applicability and the trustworthiness of the Certificate in relation with a specific application. The Certificates issued under the applicable CP are to be considered as "issued to public" Certificates.
E-Trust Ligthweight Certificate for Physical Person without SSCD and Key Generation by Owner (1 year validity, 1024-bit key size)	Lightweight Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.3** and Certipost OID : **0.3.2062.7.1.1.301.x**	This type of digital Certificates provides a reasonable degree of assurance about the Certificate holder's personal and, where applicable, professional electronic identity. For a Certificate to be issued, the individual applying for the Certificate must **not** present himself in person during the registration process or already dispose of a Certificate of a similar level. This Certificate provides a reasonable guarantee of the link between the personal identity of the Certificate holder (physical person), any professional status (not obligatory), the Public Key and its authorized use. For the application to be validated, the person applying for the Certificate must submit proof of his identity, and any documents valid as proof of his professional status and of any related information requiring certification, as required by the applicable CP (see applicable CP for details). A Public Key certified in this manner may be used solely in a context of any usage but Qualified Digital Signature (e.g., lightweight digital signature, encryption and/or authentication, or any combination of these, etc.). In such a case, the Lightweight Certificate satisfies the "**Lightweight Normalised Certificate"** requirements in the sense of the technical standard ETSI TS 102 042. The CSP(s) authorized to issue the Certificates under the applicable CP shall specify whether it/they certifies/certify the compliance of these Certificates with this policy and the regulatory documents or whether these Certificates have been certified as complying therewith. The Certification Service Providers (CSPs), authorised to issue Certificates under the applicable CP, indicate whether they claim to comply to the CP and to the relevant regulatory documents or whether they have been certified to be compliant. The Certificates issued under the applicable CP include one or several CP identifiers that can be used by relying parties in order to determine the applicability and the trustworthiness of the Certificate in relation with a specific application. The Certificates issued under the applicable CP are to be considered as "issued to public" Certificates.

1.2.2.3.2 Certipost E-Trust Qualified and Normalised Certificate Policy for Legal Persons

	Certipost OID[1]	**Summary**
E-Trust Qualified Certificate for Legal Persons without SSCD and Key Generation by Owner (3 years validity, 1024-bit key size)	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Certipost OID: **0.3.2062.7.1.1.111.x**	This type of digital Certificates provides a very high degree of assurance of a Legal Persons' electronic identity. For a Certificate to be issued, a mandated responsible applying for the Certificate must present himself in person during the registration process. This Certificate provides a strong guarantee of the link between the Legal Persons' electronic identity, the Public Key and its authorized use. For the application to be validated, the person applying for the Certificate must submit proof of his identity, and any documents valid as proof of his mandated responsibility. A Public Key certified in this manner may be used solely in one of the following two cases: • A Qualified Digital Signature context: in such a case, the Qualified Certificate satisfies the "**Qualified Certificate"** requirements in the sense of The Directive and its transposition in The 09 July Belgian Law, and of the technical standard ETSI TS 101 456. The Certificate can be used for an Advanced or a Qualified Signature, the latest being automatically equivalent to the handwritten signature; or (exclusive or) • A context of any usage but Qualified Digital Signature (e.g., normalised digital signature, encryption and/or authentication, or any combination of these, etc.): in such a case, the Normalised Certificate satisfies the "**Normalised Certificate"** requirements in the sense of the technical standard ETSI TS 102 042.
E-Trust Qualified Certificate for Legal Persons with SSCD and Key Generation by CSP (5 years validity, 2048-bit key size)	Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Certipost OID: **0.3.2062.7.1.1.112.x**	

E-Trust Normalised Certificate for Legal Persons without SSCD and Key Generation by Owner (3 years validity, 1024-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID: **0.3.2062.7.1.1.211.x**	The CSP(s) authorized to issue the Certificates under the applicable CP shall specify whether it/they certifies/certify the compliance of these Certificates with this policy and the regulatory documents or whether these Certificates have been certified as complying therewith. This Certificate type constitutes a very high level of professional electronic identity that can be used to secure high level security applications such as electronic signature operations or encryption/authentication. The Certificates (and the related Key Pair) used for Qualified Digital Signatures and for Normalised purposes (e.g., encryption and/or authentication) are always distinct (separate key pairs). The Certificates issued under the applicable CP are not exclusively dedicated to be used with a Secure Signature Creation Device (SSCD). The Certificates issued under the applicable CP include one or several CP identifiers that can be used by relying parties in order to determine the applicability and the trustworthiness of the Certificate in relation with a specific application. The Certificates issued under the applicable CP are to be considered as "issued to public" Certificates.

1.2.2.3.3 Certipost E-Trust Qualified, Normalised or Lightweight Certificate Policy for Communities.

	Certipost OID[1]	**Summary**
E-Trust Qualified Certificate for Communities with SSCD and Key Generation by CSP (1/2/5 years validity, 1024-bit key size)	Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Certipost OID : **0.3.2062.7.1.1.121.x**	This type of digital Certificates provides a very high level of assurance with regard to the electronic personal and professional identity of the Certificate owner in the context or while acting as a member of a specific Community. These certificates are either Qualified or Normalised Certificates for which the issuing is conditioned to the physical presentation during the registration. These Certificates provide a very high level of assurance to guarantee the link between the personal identity, his/her Public Key, its authorised usage and the information related to the professional qualification of the member of a specific Community, who is subject of the Certificate. The validation of the request will demand the provision of the proof of the identity of the applicant as a member of a specific Community and the verification of the pieces guaranteeing his quality(ies) and the related information that

E-Trust Qualified Certificate for Communities without SSCD and Key Generation by Owner (1 year validity, 1024-bit key size)	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Certipost OID : **0.3.2062.7.1.1.122.x**	have to be certified. The so certified Public Key can only be used in one of the two following cases (exclusively): • A Qualified Digital Signature context: in such a case, the Qualified Certificate satisfies the "**Qualified Certificate"** requirements in the sense of The Directive and its transposition in The 09 July Belgian Law, and of the technical standard ETSI TS 101 456. The Certificate can be used for an Advanced or a Qualified Signature, the latest being automatically equivalent to the handwritten signature; or (exclusive or) • A context of any usage but Qualified Digital Signature (e.g., normalised digital signature, encryption and/or authentication, or any combination of these, etc.): in such a case, the Normalised Certificate satisfies the "**Normalised Certificate"** requirements in the sense of the technical standard ETSI TS 102 042. The Certification Service Providers (CSPs), authorised to issue Certificates under this CP, indicate whether they claim to comply to the CP and to the relevant regulatory documents or whether they have been certified to be compliant. This Certificate type constitutes a very high level of professional electronic identity that can be used to secure high level security applications such as electronic signature operations or encryption/authentication performed in the context or in the exercise of the Lawyer's profession. These Certificates (and the related Key Pair) used for Qualified Digital Signatures and for Normalised purposes
E-Trust Normalised Certificate for Communities with SSCD and Key Generation by CSP (1/2/5 years validity, 1024-bit key size)	Normalised Certificate with SSCD (OID ETSI 102 042): **0.4.0.2042.1.2** and Certipost OID : **0.3.2062.7.1.1.221.x**	

E-Trust Normalised Certificate for Communities without SSCD and Key Generation by Owner (1 year validity, 1024-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID : **0.3.2062.7.1.1.222.x**	(e.g., encryption and/or authentication) are always distinct (separate key pairs). The Certificates issued under this CP are not exclusively dedicated to be used with a Secure Signature Creation Device (SSCD). The Certificates issued under this CP include one or several CP identifiers that can be used by relying parties in order to determine the applicability and the trustworthiness of the Certificate in relation with a specific application. This CP satisfies additional requirements compared to the "Certipost E-Trust Qualified of Normalised Digital Certificates for Physical Persons" Certificate Policies : – Obligation for the member of a specific Community applying to be a Certificate owner to visit a Local Registration Authority (LRA) certified and trained by Certipost E-Trust and the Community, if applicable. – Obligation for the member of a specific Community applying to be a Certificate owner to provide Certipost E-Trust, via the certified LRA, the additional identification proofs as required in the CP and related to his quality(ies) related to the Community. – Allowed ability for the Community, via the certified LRAs, to be involved in the revocation/suspension process, in case applicable.

E-Trust Lightweight Certificate for Communities without SSCD and Key Generation by CSP (1/3/5 years validity, 1024-bit key size)	Lightweight Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.3** and Certipost OID : **0.3.2062.7.1.1.311.x**	This type of digital Certificates provides a reasonable level of assurance with regard to the electronic personal and professional identity of the Certificate owner in the context or while acting as a member of a specific Community. These certificates are Lightweight Certificates for which the issuing is **not** conditioned to the physical presentation during the registration. These Certificates provide a reasonable level of assurance to guarantee the link between the personal identity, his/her Public Key, its authorised usage and the information related to the professional qualification of the member of a specific Community, who is subject of the Certificate. The validation of the request will demand the provision of the proof of the identity of the applicant as a member of a specific Community and the verification of the pieces guaranteeing his quality(ies) and the related information that have to be certified. The so certified Public Key can only be used in context of any usage but Qualified Digital Signature (e.g., normalised digital signature, encryption and/or authentication, or any combination of these, etc.). In such a case, the Lightweight Certificate satisfies the "**Lightweight Normalised Certificate"** requirements in the sense of the technical standard ETSI TS 102 042. The Certification Service Providers (CSPs), authorised to issue Certificates under this CP, indicate whether they claim to comply to the CP and to the relevant regulatory documents or whether they have been certified to be compliant. This Certificate type constitutes a reasonable level of professional electronic identity that can be used to secure applications requiring electronic signature operations or encryption/authentication performed in the context of a specific Community. The Certificates issued under this CP include one or several CP identifiers that can be used by relying parties in order to determine the applicability and the trustworthiness of the Certificate in relation with a specific application. This CP satisfies additional requirements compared to the "Certipost E-Trust Lightweight Digital Certificates for Physical Persons" Certificate Policies : – Obligation for the member of a specific Community applying to be a Certificate owner to register through a Registration Authority (RA) certified and trained by Certipost E-Trust and the Community, if applicable. – Obligation for the member of a specific Community applying to be a Certificate owner to provide Certipost E-Trust, via the certified RA, the additional identification proofs as required in the CP and related to his quality(ies) related to the Community. – Allowed ability for the Community, via the certified RAs, to be involved in the revocation/suspension process, in case applicable.

1.2.2.3.4 Certipost E-Trust Qualified and Normalised Certificate Policy for the Publilink project

	Certipost OID[1]	**Summary**
E-Trust Qualified Certificate for Publilink with SSCD and Key Generation by CSP (1 year validity, 1024-bit key size)	Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Certipost OID: **0.3.2062.7.1.1.131.x**	This type of digital Certificates provides a very high level of assurance regarding to the electronic personal and professional identity of the Certificate owner in the context of the Publilink project. These certificates are either Qualified or Normalised Certificates for which the issuing is conditioned to the physical presentation during the registration. These Certificates provide a very high level of assurance to guarantee the link between the personal identity, his/her Public Key, its authorised usage and the information related to the professional qualification of the subject of the Certificate. The Certificate provides the highest level of authentication because the holder of the certificate must : • Either present himself personally with a Local Registration Authority (LRA) in order to be correctly registered before the emission of the certificate by the CSP. • Either dispose already of a Certificate with an equivalent level to be able to proceed to his request The validation of the request will demand the provision of the proof of the identity of the applicant and the verification of the pieces guaranteeing his professional's quality and the related information that have to be certified. The so certified Public Key can only be used in one of the two following cases (exclusively): • A Qualified Digital Signature context: in such a case, the Qualified Certificate satisfies the "**Qualified Certificate"** requirements in the sense of The Directive and its transposition in The 09 July Belgian Law, and of the technical standard ETSI TS 101 456. The Certificate can be used for an Advanced or a Qualified Signature, the latest being automatically equivalent to the handwritten signature; or (exclusive or) • A context of any usage but Qualified Digital Signature (e.g., normalised digital signature, encryption and/or authentication, or any combination of these, etc.): in such a case, the Normalised Certificate satisfies the "**Normalised**
E-Trust Qualified Certificate for Publilink without SSCD and Key Generation by Owner (1 year validity, 1024-bit key size)	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Certipost OID: **0.3.2062.7.1.1.132.x**	
E-Trust Normalised Certificate for Publilink with SSCD and Key Generation by CSP (1 year validity, 1024-bit key size)	Normalised Certificate with SSCD (OID ETSI 102 042): **0.4.0.2042.1.2** and Certipost OID: **0.3.2062.7.1.1.251.x**	

E-Trust Normalised Certificate for Publilink without SSCD and Key Generation by Owner (1 year validity, 1024-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID: **0.3.2062.7.1.1.252.x**	**Certificate"** requirements in the sense of the technical standard ETSI TS 102 042. The Certification Service Providers (CSPs), authorised to issue Certificates under this CP, indicate whether they claim to comply to the CP and to the relevant regulatory documents or whether they have been certified to be compliant. These Certificates (and the related Key Pair) used for Qualified Digital Signatures and for Normalised purposes (e.g., encryption and/or authentication) are always distinct (separate key pairs).

1.2.2.3.5 Certipost E-Trust Normalised Certificate Policy for Carenet

	Certipost OID[1]	**Summary**
E-Trust Normalised Certificate for Carenet (1/3 years validity)	**1.3.6.1.4.1.7727.1.1.1.2.4**	This type of digital Certificates provides a very high degree of assurance of the Certificate holder's personal and professional electronic identity in the framework of the Carenet Project. For a Certificate to be issued, the individual applying for the Certificate must present himself in person during the registration process. This Certificate provides a strong guarantee of the link between the personal identity of the Certificate holder (physical person), and its professional status, the Public Key and its authorized use. For the application to be validated, the person applying for the Certificate must submit proof of his identity, and any documents valid as proof of his professional status and of any related information requiring certification, as required by the applicable CP (see applicable CP for details). The Normalised Certificate for Carenet key usage can either be for signature purposes or (exclusive) for encryption purposes and satisfies the "**Normalised Certificate"** requirements in the sense of the technical standard ETSI TS 102 042.

1.2.2.3.6 Certipost E-Trust Normalised Certificate Policy for (SSL) Webservers

	Certipost OID[1]	**Summary**
E-Trust Normalised Certificate for Web-Servers without SSCD and Key Generation by Owner (1/5 years validity, 1024-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID: **0.3.2062.7.1.1.241.x**	This type of digital Certificates provides a very high level of assurance regarding to the electronic identity of a (web) server. These certificates are Normalised Certificates for which the issuing is conditioned to a physical presentation during the registration of the certificate subscriber. These Certificates provide a very high level of assurance to guarantee the link between the server identity, and its Public Key. The physical person presenting itself at the Local Registration Authority –

E-Trust Normalised Certificate for Web-Servers without SSCD and Key Generation by Owner (5 years validity, 2048-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID: **0.3.2062.7.1.1.243.x**	LRA is the legal representative of the company responsible for or proprietor of the server, or its authorized delegate. The certificate guarantees the server identity (e.g. URL for a web server) and the belonging of the server to a company or an organization. The request validation requires the provision of the proof that the server belongs indeed to the subscribing company or organization.

1.2.2.3.7 Certipost E-Trust Normalised Certificate Policy for Code Signing

	Certipost OID[1]	**Summary**
E-Trust Normalised Certificate for Object-Signing without SSCD and Key Generation by Owner (1/5 years validity, 1024-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID: **0.3.2062.7.1.1.242.x**	This type of digital Certificates provides a very high level of assurance regarding to the electronic identity of an Object Signing entity. These certificates are Normalised Certificates for which the issuing is conditioned to a physical presentation during the registration of the certificate subscriber. These Certificates provide a very high level of assurance to guarantee the link between the Object Signing entity identity, and its Public Key. The physical person presenting itself at the Local Registration Authority – LRA is the legal representative of the company responsible for or proprietor of the Object Signing entity, or its authorized delegate. The certificate guarantees the Object Signing entity identity (e.g. URL for a web server) and its belonging to a company or an organization. This certificate can only be used to sign computer programs (Object code, applets, …).
E-Trust Normalised Certificate for Object-Signing without SSCD and Key Generation by Owner (5 years validity, 2048-bit key size)	Normalised Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.1** and Certipost OID: **0.3.2062.7.1.1.244.x**	

1.2.2.3.8 Certipost E-Trust Lightweight Normalised Certificate Policy for the DubliNET CUG functional mailboxes (EC regulation 343/2003)

	Certipost OID[1]	**Summary**

E-Trust Lightweight Normalised Certificate for IDABC for the DubliNET CUG functional mailboxes (EC regulation 343/2003)	Lightweight Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.3** and Certipost OID: **0.3.2062.7.1.1.323.x**	Medium level Professional digital identity assurance. Remotely requested certificate providing medium level of guarantee for the binding between a Functional Entity and a public key. This certificate guarantees the identity of the Functional Entity and the ownership of this Functional Entity by the Organisation and for which the Organisation is responsible. The validation of the request will require evidence of the identity of the Subscriber and evidence that he/she represents an Organisation identified on the list of authorities identified under Article 22 of EC Regulation 343/2003. This certificate policy is a "lightweight certificate policy" (LCP) as specified by ETSI standard ETSI TS 102 042.

1.2.2.3.9 Certipost E-Trust Lightweight Normalised Certificate Policy for the European Commission (IDA sectoral networks)

	Certipost OID[1]	**Summary**
E-Trust Lightweight Normalised Certificate for IDABC for the European Commission (IDA sectoral networks)	Lightweight Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.3** and Certipost OID: **0.3.2062.7.1.1.322.x**	Medium level Professional digital identity assurance. Remotely requested certificate providing medium level of guarantee for the binding between a Functional Mailbox identity and a public key. This certificate guarantees the identity of the Functional Mailbox and the ownership of the functional mailbox by the Subscriber, who is part of a Company or Organisation. The validation of the request requires evidence of the identity of the Subscriber and evidence that he belongs to the company or organisation. Certificates issued under this policy can only be used in sectoral networks as defined in decisions 1720/1999/EC and 2045/2002/EC of the European Parliament and of the Council. This certificate policy is a "lightweight certificate policy" (LCP) as specified by ETSI standard ETSI TS 102 042.

1.2.2.3.10 Certipost E-Trust Lightweight Normalised Certificate Policy for the Justice and Home affair DG CUG functional mailboxes (EC regulation 2725/2000)

	Certipost OID[1]	**Summary**
E-Trust Lightweight Normalised Certificate for IDABC for the Justice and Home affair DG CUG functional mailboxes (EC regulation 2725/2000)	Lightweight Certificate without SSCD (OID ETSI 102 042): **0.4.0.2042.1.3** and Certipost OID: **0.3.2062.7.1.1.321.x**	Medium level Professional digital identity assurance. Remotely requested certificate providing medium level of guarantee for the binding between a Functional Mailbox identity and a public key. This certificate guarantees the identity of the Functional Mailbox and the ownership of this Functional Mailbox by the Organisation and for which the Organisation is responsible. The validation of the request will require evidence of the identity of the Subscriber and evidence that he/she represents an Organisation identified on the list of authorities identified under Article 15 of EC Regulation 2725/2000. This certificate policy is a "lightweight certificate policy" (LCP) as specified by ETSI standard ETSI TS 102 042.

1.3 Community and Applicability

The Certipost E-Trust Q&N CPS has been designed to provide a statement of the practices that CA's within the Certipost E-Trust PKI employ in issuing Qualified, Normalised or Lightweight Certificates.

The applicability of the Certificates issued by CA's in accordance with this Q&N CPS will be documented in the associated Certificate Policies (CP's).

The CA that issues Certificates in accordance with this Q&N CPS will comply with the current document and with a set of rules for a specific Certificate type. This set of rules is established in an associated CP. This will facilitate different usage and trust assurance levels per Certificate.

The following sub-sections will describe the various communities involved in the certification process (Policy Approval Authority, Certification Authorities, Registration Authorities, end-entities or Subscribers, and relying parties). The latest sub-section will describe the applicability of the Certificates issued under this Q&N CPS according to the specific CP under which the Certificates are issued.

1.3.1 Policy Approval Authorities

a) **Policy Approval Authority within Certipost E-Trust**: The Policy Approval Authority within Certipost E-Trust is called the Certipost E-Trust PKI Certification Practices Council (CePraC). It is the high level management body with final authority and responsibility for

- Specifying and approving the Certipost E-Trust infrastructure and practices.
- Approving the Certipost E-Trust Certification Practice Statement(s) and Certipost E-Trust Certificate Policies and other related documents (General Terms and Conditions, Purchase Orders, sub-contracting agreements, etc.).
- Defining the review and audit process for certification practices and Certificate Policies including responsibilities for maintaining the Certification Practice Statements and Certificate Policies and related documents.
- Defining the review and audit process that ensures that the certificate practices are properly implemented by the CAs and other PKI participants (CRAs, LRAs, SRAs, subcontractors, etc.).
- Defining the review and audit process that ensures that the Certificate Policies are supported by the CAs Certification Practice Statement(s).
- Publication to the Subscribers and relying parties of the Certificates Policies and Certification Practice Statements and their revisions.
- Specifying cross-certification procedures and handling cross-certification requests

b) Policies ruling the membership, the management and the task of the Certipost E-Trust PKI Certification Practices Council as identified in sub a) are provided in internal documents.

1.3.2 Certification Authorities

a) In accordance with the provisions of the Certipost E-Trust Q&N CPS, the following Certification Authorities can be distinguished within the Certipost E-Trust PKI.

- *Certipost E-Trust TOP Root CA*

  The Certipost E-Trust TOP Root CA issues the Certificates of the subordinate E-Trust Primary CAs.

- *Certipost E-Trust Primary Qualified CA*

  The Certipost E-Trust Primary Qualified CA issues Certificates of the subordinate E-Trust

Secondary Qualified CAs. The Secondary Qualified CAs are issuing Qualified Certificates to end-entities.

- Certipost E-Trust Secondary Qualified CA for Physical Persons
- Certipost E-Trust Secondary Qualified CA for Legal Persons
- Certipost E-Trust Secondary Qualified CA for Communities
- Certipost E-Trust Secondary Qualified CA for Publilink

- *Certipost E-Trust Primary Normalised CA*

  The Certipost E-Trust Primary Normalised CA issues Certificates of the subordinate E-Trust Secondary Normalised CAs. The Secondary Normalised CAs are issuing Normalised Certificates to end-entities.

  - Certipost E-Trust Secondary Normalised CA for Physical Persons
  - Certipost E-Trust Secondary Normalised CA for Legal Persons
  - Certipost E-Trust Secondary Normalised CA for Communities
  - Certipost E-Trust Secondary Normalised CA for Publilink
  - Certipost E-Trust Secondary Normalised CA for Carenet
  - Certipost E-Trust Secondary Normalised CA for Web-Servers and Object Signing.

- *Certipost E-Trust Primary Lightweight CA*

  The Certipost E-Trust Primary Lightweight CA issues Certificates of the subordinate E-Trust Secondary Lightweight CAs. The Secondary Lightweight CAs are issuing Lightweight Certificates to end-entities.

  - Certipost E-Trust Secondary Lightweight CA for Physical Persons
  - Certipost E-Trust Secondary Lightweight CA for Communities
  - Certipost E-Trust Secondary Lightweight CA for IDABC

b) Certipost E-Trust allows for cross-certification engagements. Any request for cross-certification engagements by an external CA will have to be submitted to Certipost E-Trust Services. See section 1.4.2 for address details.

c) The E-Trust Secondary Qualified CAs that operates in accordance with this Q&N CPS can issue only Qualified Certificates. A short description of the Qualified Certificates types supported by the E-Trust Secondary Qualified CA is provided above (see section 1.2.2). Every Certificate type is ruled by a specific E-Trust Certificate Policy (CP) document.

d) The E-Trust Secondary Normalised CAs that operates in accordance with this Q&N CPS can issue only Normalised Certificates. A short description of the Normalised Certificates supported by the E-Trust Secondary Normalised CA is provided above (see section 1.2.2). Every Certificate type is ruled by a specific E-Trust Certificate Policy (CP) document.

e) The E-Trust Secondary Lightweight CAs that operates in accordance with this Q&N CPS can issue only Lightweight Certificates. A short description of the Lightweight Certificates supported by the E-Trust Secondary Lightweight CA is provided above (see section 1.2.2). Every Certificate type is ruled by a specific E-Trust Certificate Policy (CP) document.

f) A specific CP will govern the delivery conditions, the usage and the applicability rules and guidelines for each Certificate that is issued under this Certipost E-Trust Q&N CPS. The list mentioned in section 1.2.2 does not exclude any other (future) Certificate type and related CP to refer to the present Q&N CPS provided that each statement in this Q&N CPS is respected.

g) The list of CA's that are allowed to issue a Qualified, Normalised or Lightweight Certificate under the Certipost E-Trust Q&N CPS is stated in the related CP.

h) Certipost E-Trust reserves right to set-up additional E-Trust Primary and Secondary CA's in accordance with the current Certipost E-Trust Q&N CPS.

1.3.3 Registration Authorities

a) In accordance with the provisions of this Q&N CPS, the following Registration Authorities can be distinguished within the Certipost E-Trust Qualified, Normalised and Lightweight PKI.

- *Certipost E-Trust Central RA,*
- *Certipost E-Trust authorised Local RAs as specified in the applicable CP and as ruled by formal contractual agreement between Certipost E-Trust 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 E-Trust and the concerned legal entity acting as Local RA..*
- *European Commissions' Local RA's as specified in the applicable CP and as ruled by formal contractual agreement between Certipost E-Trust and the concerned legal entity acting as Local RA*
- *Contractually bound organisation's Local RA's as specified in the applicable CP and as ruled by formal contractual agreement between Certipost E-Trust and the concerned legal entity acting as Local RA*
- *Carenets' Local RA's as specified in the applicable CP and as ruled by formal contractual agreement between Certipost E-Trust and the concerned legal entity acting as Local RA*

b) Any Registration Authority which operates within the Certipost E-Trust PKI in accordance with this Q&N 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 E-Trust CAs, this approval shall be obtained from the Certipost E-Trust PKI Certification Practices Council).
- Undertake to conform to the stipulations of this Q&N 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 Q&N CPS).

c) The list of Local RA's that are allowed to register requests for a Qualified, Normalised or Lightweight Certificate under the Certipost E-Trust Q&N CPS is stated in the related CP according to the relevant sections of this Q&N CPS.

1.3.4 Subscribers

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

- Any natural person, which can be uniquely identified by a valid piece of identity in accordance with the related CP. Please see applicable CP for details.
- Any legal person, which can be uniquely identified. Please see applicable CP for details.
- Any end-entity other than a natural person or a legal person, which can be uniquely identified. This case is not allowed for issuing of Qualified Certificates. 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:

- Any natural person, which can be uniquely identified by a valid piece of identity in accordance with the related CP. Please see applicable CP for details.

1.3.5 Applicability

a) A Certificate issued by a CA in accordance with this Q&N CPS can be used for different kinds of applications, depending on the CP under which it has been issued.

b) Key usage is indicated in the Certificate Policy: for Qualified Certificate the key usage is exclusively limited for creating Qualified or Advanced Digital Signatures. Any different usage is at the own risk and responsibility of the Subscriber and/or the relying party. For Normalised and Lightweight Certificates, the key usage can be any type of usage but Qualified Digital Signatures and is indicated in the Certificate according to the related CP.

c) Key usage is indicated in the Certificate: for more details see section 7.1.2.

1.3.5.1 Suitable applications

An overview of Certificate applications is shown in the table below according to the current types of Certipost E-Trust Qualified, Normalised or Lightweight Certificate Policies as identified in section 1.2.2.3. See the applicable CP for details. It is however the responsibility of the relying parties to choose for which applications they will use the Certificate.

Certipost E-Trust Qualified, Normalised or Lightweight Certificate for Physical Person				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Qualified Certificate without SSCD and Key Generation by Owner	Advanced Digital Signature only (Key usage extension: nonRepudiation and digitalSignature)	Appropriate for supporting Signatures with legal recognition as provided by art. 4, §5 of the 09 July 2001 Law and art. 5.2 of The European Directive. This means these signatures have a not deniable legal effect.	Electronic personal or professional identity **for advanced electronic signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
E-Trust Qualified Certificate with SSCD and Key Generation by CSP	Qualified Digital Signature only (Key usage extension: nonRepudiation and digitalSignature)	Appropriate for supporting Qualified Signatures (according to art. 4, §4 of the 09 July 2001 Law and art. 5.1 from The European Directive). This means these certificates are supporting digital signatures which have the same value as a handwritten signature.	Electronic personal or professional identity **for qualified digital signature** support in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)

E-Trust Qualified Certificate without SSCD and Key Generation by CSP	Advanced Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Signatures with legal recognition as provided by art. 4, §5 of the 09 July 2001 Law and art. 5.2 from The European Directive. This means these signatures have a not deniable legal effect.	Electronic personal or professional identity **for advanced elecronic signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
E-Trust Normalised Certificate without SSCD and Key Generation by Owner	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	NA except for Normalised digital signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic personal or professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
E-Trust Normalised Certificate with SSCD and Key Generation by CSP	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	NA except for Normalised digital signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic personal or professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
E-Trust Normalised Certificate without SSCD and Key Generation by CSP	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	N.A. except for Normalised digital signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic personal or professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)

E-Trust Lightweight Certificate without SSCD and Key Generation by Owner	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	N.A. except for (normalized digital) electronic signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic personal or professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (medium or low value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)

Certipost E-Trust Qualified and Normalised Certificate for Legal Persons				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Qualified Certificate without SSCD and Key Generation by Owner	Advanced Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Signatures with legal recognition as provided by art. 4, §5 of the 09 July 2001 Law and art. 5.2 of The European Directive. This means these signatures have a not deniable legal effect.	Electronic legal person identity **for advanced electronic signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
E-Trust Qualified Certificate with SSCD and Key Generation by CSP	Qualified Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Qualified Signatures (according to art. 4, §4 of the 09 July 2001 Law and art. 5.1 from The European Directive). This means these certificates are supporting digital signatures which have the same value as a handwritten signature.	Electronic legal person identity **for qualified digital signature** support in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)

E-Trust Normalised Certificate without SSCD and Key Generation by Owner	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	N.A. except for Normalised digital (electronic) signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic legal person identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)

Certipost E-Trust Communities' Qualified, Normalised or Lightweight Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
Communities' Qualified Certificate without SSCD and Key Generation by Owner	Advanced Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Signatures with legal recognition as provided by art. 4, §5 of the 09 July 2001 Law and art. 5.2 from The European Directive. This means these signatures have a not deniable legal effect.	Communities' professional identity **for advanced electronic signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
Communities' Qualified Certificate with SSCD and Key Generation by CSP	Qualified Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Qualified Signatures (according to art. 4, §4 of the 09 July 2001 Law and art. 5.1 from The European Directive). This means these certificates are supporting digital signatures which have the same value as a handwritten signature.	Communities' professional identity **for qualified digital signature** support in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
Lawyers' Normalised Certificate without SSCD and Key Generation by Owner	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	NA except for Normalised digital signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic Lawyer's professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage** : The certificate can only be used by its owner in the context or in the exercise of its profession of Lawyer. **No limit on transaction value**.

Communities' Normalised Certificate with SSCD and Key Generation by CSP	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	N.A. except for Normalised digital (electronic) signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Communities' professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
Communities' Normalised Certificate without SSCD and Key Generation by Owner	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	N.A. except for Normalised digital (electronic) signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Communities' professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
Communities' Lightweight Certificate without SSCD and Key Generation by CSP	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	N.A. except for electronic signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Communities' professional identity for **any usage but Qualified Digital Signature** (e.g., lightweight digital signature, digital authentication and encryption) in (medium or low value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)

Certipost E-Trust Publilink Qualified and Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
Publilink Qualified Certificate with SSCD and Key Generation by CSP	Qualified Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Qualified Signatures (according to art. 4, §4 of the 09 July 2001 Law and art. 5.1 from The European Directive). This means these certificates are supporting digital signatures which have the same value as a handwritten signature.	Publilink related professional identity **for qualified digital signature** support in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
Publilink Qualified Certificate without SSCD and Key Generation by Owner	Advanced Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Signatures with legal recognition as provided by art. 4, §5 of the 09 July 2001 Law and art. 5.2 from The European Directive. This means these signatures have a not deniable legal effect.	Publilink related professional identity **for advanced electronic signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)
Publilink Normalised Certificate without SSCD and Key Generation by Owner	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	N.A. except for Normalised digital (electronic) signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Publilink related professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)

Publilink Normalised Certificate with SSCD and Key Generation by CSP	Any usage but Qualified Digital Signature (Key usage extension: see 7.1.2)	N.A. except for Normalised digital (electronic) signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Publilink related professional identity for **any usage but Qualified Digital Signature** (e.g., normalised digital signature, digital authentication and encryption) in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: As indicated by Subscriber (when applicable)

Certipost E-Trust Dublinet CUG functional mailboxes (EC regulation 343/2003) Lightweight Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Lightweight Certificate	(Key usage extension: see 7.1.2)	N.A. except for Lightweight digital signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic functional identity **for any usage but Qualified Digital Signature** (e.g., digital signature, digital authentication and encryption) in commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: The certificate can only be used by its owner in the context of the functional identity, which is owned by an Organisation that is identified on the list of authorities identified under Article 22 of EC Regulation 343/2003. **No limit on transaction value**.

Certipost E-Trust IDA sectoral networks Lightweight Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Lightweight Certificate	(Key usage extension: see 7.1.2)	NA except for Lightweight digital signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic functional identity **for any usage but Qualified Digital Signature** (e.g., digital signature, digital authentication and encryption) in commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: The certificate can only be used by its owner in the context of sectoral networks, as defined in decisions 1720/1999/EC and 2045/2002/EC of the European Parliament and the Council. **No limit on transaction value**.

Certipost E-Trust Justice and Home affair DG CUG functional mailboxes (EC regulation 2725/2000) Lightweight Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Lightweight Certificate	(Key usage extension: see 7.1.2)	NA except for Lightweight digital signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic functional identity **for any usage but Qualified Digital Signature** (e.g., digital signature, digital authentication and encryption) in commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: The certificate can only be used by its owner in the context of the functional identity, which is owned by an Organisation that is identified on the list of authorities identified under Article 15 of EC Regulation 2725/2000. **No limit on transaction value**.

Certipost E-Trust SSL WebServer Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Normalised Certificate for (web-) servers	(Key usage extension: see 7.1.2)	N.A. except for Normalised digital (electronic) signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic identity **for any usage but Qualified Digital Signature** (e.g., digital signature, digital authentication and encryption) in commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: The certificate can only be used in the context of guaranteeing the URL of a SSL WebServer and in a context of encryption of the connection to a SSL WebServer. **No limit on transaction value**.

Certipost E-Trust Object Signing Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Normalised Certificate for Object Signing	(Key usage extension: see 7.1.2)	N.A. except for Normalised digital (electronic) signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic identity **for any usage but Qualified Digital Signature** (e.g., digital signature, digital authentication and encryption) in commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: The certificate can only be used in the context of signing computer programs (object code, applets,…). **No limit on transaction value**.

Certipost E-Trust Carenet Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Normalised Certificate for Carenet	(Key usage extension: see 7.1.2)	N.A. except for Normalised digital (electronic) signatures according to art. 1322 Belgian Civil Code. This means these signatures have a not deniable legal effect.	Electronic identity **for any usage but Qualified Digital Signature** (e.g., digital signature, digital authentication and encryption) in commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage**: The certificate can only be used in the context of the Carenet application. **No limit on transaction value**.

1.3.5.2 Approved applications

See the applicable CP.

1.3.5.3 Prohibited applications

It is recommended not to use Certificates issued in accordance with this Q&N CPS for another purpose than as defined for that Certificate type in the list of suitable applications (section 1.3.5.1) or in the applicable CP. The set of rules set forth in the applicable CP also applies.

1.4 Contact Details

1.4.1 Specification administration organisation

Certipost E-Trust Services administer this Q&N CPS. CPS administration is done in accordance with section 8 of this CPS.

1.4.2 Contact person

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

Contact persons:
Certipost E-Trust Services
Certipost E-Trust PKI Certification Practices Council
C/o Bart Callens
Ref.: CPS Administration
Muntcentrum
B-1000 Brussels
Belgium

http://www.e-trust.be
info@e-trust.be

Fax: +32 (53) 601 151

1.4.3 Person determining CPS suitability for the policy

a) Certipost E-Trust PKI Certification Practices Council (see section 1.3.1) is responsible for determining Certipost E-Trust Q&N CPS suitability for Certipost E-Trust CP.

b) Certipost E-Trust PKI Certification Practices Council is responsible for determining and issuing the CP's, determining their suitability to Q&N CPS and to authorize (Local) RA's to register Certificate requests and CA's to issue Certificates under a particular Certipost E-Trust CP and this Q&N CPS.

c) The Certipost E-Trust PKI Certification Practices Council is responsible for initiating audits as stated in section 2.7.1.

d) To contact the Certipost E-Trust PKI Certification Practices Council, please use the contact information as stated in section 1.4.2.

2 GENERAL PROVISIONS

2.1 Obligations

The following are the obligations of Certipost E-Trust Services:

a) **Infrastructure** -- Certipost E-Trust Services is obliged to maintain the Certipost E-Trust PKI Infrastructure in accordance with this Q&N CPS.

b) **Maintenance of an Electronic Registry for Certificates and Certificate Revocation Lists** -- Certipost E-Trust Services is obliged to maintain an electronic registry, permanently available to anybody in an electronic way. This registry is called the Certipost E-Trust Certificate Public Registry. This electronic registry will at least contain:

- **a)** The Certificates that have been delivered by a CA in accordance with this Q&N CPS and the applicable CP; and
- **b)** The Certificate Revocation List published in accordance with this Q&N CPS and with the applicable CP.
- **c)** The CA Certificates of the CAs that are part of the Certipost E-Trust PKI.

c) **Electronic Registry Protection --** Certipost E-Trust Services is obliged to provide its best effort to protect the Certipost E-Trust Certificate Public Registry against unauthorized modifications.

d) **Agreements** -- Certipost E-Trust Services is responsible for drawing up one or more contractual agreements with:

- The prospective Subscriber in a way that clearly indicates the rights and obligations of both parties. This contractual agreement is referring to the applicable Certificate Policy and the CPS, and in particular to this section. This agreement will at least state:
  - The acknowledgement of the Subscriber on the recommended applications of a Certificate and the correctness of the information provided;
  - The Subscriber will only use the key pair for the intended usage and with any other limitations notified to the Subscriber;
  - The acceptance of the rules and conditions associated with usage of the storage media used to store the Private Key, including the responsibility to safe-guard the Private Key, the storage media and its PIN (or pass phrase);
  - The immediate report of the loss of either or both (Private Key and or its pin), as well as report any suspicion of misuse, breach of confidentiality or integrity flaw;
  - The system of suspension and revocation of Certificates.
- All RA's, operating on behalf of a CA, in a way that clearly indicates the rights and obligations of both parties.
- The RA Officer (Local or Central), operating on behalf of an RA, in a way that clearly indicates the rights and obligations of both parties. This agreement may be part of the contractual agreement between Certipost E-Trust Services and the RA.

2.1.1 CA obligations

The following are the obligations of any CA within the Certipost E-Trust PKI Infrastructure:

a) **Standards compliance** -- Certipost E-Trust shall ensure that all requirements on CA, as detailed in sections 2.3 to 8.3, are implemented as applicable respectively

- for Qualified CAs to the ETSI Technical Standard TS 101.456 and in particular, when relevant, to the certificate policies QCP public with SSCD and to QCP public;
- for Normalised CAs to the ETSI Technical Standard TS 102 042 (Normalised level);

- for Lightweight CAs to the ETSI Technical Standard TS 102 042 (Lightweight level)

b) **Accuracy of representations** -- The CA guarantees to all who reasonably rely on the information contained in the Certificate issued under this Q&N CPS, that it has issued the Certificate to the named Subscriber, in accordance with the provisions in this Q&N CPS and in the applicable CP.

c) **Required controls provision** -- The CA shall provide all its certification services consistent with this Q&N CPS.

d) **Certificate Issuance** – The CA within the Certipost E-Trust Qualified and Normalised PKI segment from the Certipost E-Trust PKI Infrastructure, issuing Certificates under this Q&N CPS, is obliged to issue Certificates in accordance with section 4.1.

e) **Notification of Certificate issuance** -- The CA is obliged to ensure that the Subscriber who is the subject of the Certificate or not and others who reasonably rely on that Certificate are notified of the Certificate issuance in accordance with section 2.6.1 of this CPS.

f) **Certificate suspension and revocation by the CA** -- Certificate suspension and revocation by the CA are ruled by sections 3.4. and 4.4.

g) **Notification of revocation or suspension of a Certificate** -- The CA is obliged to ensure that the Subscriber who is the subject of the Certificate or who is responsible of the Certificate and others who reasonably rely on that Certificate are notified of the Certificate revocation or suspension in accordance with sections 4.4.10 of this CPS.

h) **Maintain Certificate information** -- The CA is obliged to maintain records necessary to support requests concerning its operation, including audit files and archives.

i) **Notification to the Subscriber of the necessary information to correctly and safely use the CA services** --

a) The CA is obliged to ensure that the Subscriber (who may or may not be the Subject of the Certificate) is notified of his obligations in accordance with section 2.1.3 of this CPS.

b) The CA is obliged to inform the Subscriber about the requirements regarding the protection of Private Key.

c) The CA is obliged to inform the Subscriber about the precise guarantees that are offered by the CA services in accordance with this CPS and relevant CP.

j) **Data Privacy** -- The CA is authorized to collect the personal data that is necessary to perform its services. These personal data can only be used in the context of the certification services provision. The collection of information from third parties can only be achieved with prior approval of the Subscriber. The data privacy protection is done in accordance with respect to the Belgian law on privacy issues. In order to carry out its tasks in an efficient manner, Certipost E-Trust uses databases with these personal data. In this regard, Certipost E-Trust must respect the privacy of the persons concerned and therefore attaches utmost importance and caution to the processing of personal data. The personal data which the Subscriber supplies to Certipost E-Trust are incorporated in the files of CERTIPOST s.a./n.v., Centre Monnaie, - 1000 Brussels. The data will only be used for the provisioning of the Certipost E-Trust services. The Subscriber has the right to access and correct this data.

k) **Protection of issuing CA's Private Key** -- The CA is obliged to protect its Private Key in accordance with the provisions of sections 4 through 6 of this CPS.

l) **Restriction on issuing CA's Private Key use** -- The CA's shall ensure that CA's Private Signing Keys are not used inappropriately. In particular, CA's Private Signing Key used for generating Certificates and/or issuing revocation status information and other adequate information consistent with the Certificate issuance under this Q&N CPS and the applicable CP shall not be used for any other purpose. See section 6.1.9.1 for more details on the usage of the usage of the CA's Private Keys.

2.1.2 RA obligations

2.1.2.1 CRA obligations

The following are the minimum obligations of any RA within the Certipost E-Trust Infrastructure:

a) **Accurate dealing of the requests** -- The RA is obliged to accurately represent the information it prepares for a CA, to process request and responses timely and securely in accordance with section 3 through 6 of this Q&N CPS, the applicable CP and the Certipost E-Trust RA Procedures and Guidelines.

b) **Maintain Certificate application information** -- The RA is obliged to keep, for **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 this Q&N CPS.

c) **Q&N CPS, CP's and Certipost E-Trust RA Procedures and Guidelines provisions compliance** -- The RA is obliged to comply with all provisions in this Q&N CPS, the applicable CP's and the Certipost E-Trust RA Procedures and Guidelines.

d) **Protection of RA's PSE** -- The RA is obliged to protect its Private Key in accordance with the provisions of sections 4 through 6 of this CPS.

e) **Restriction on RA PSE use** -- The RA can only use his Private Key for purposes associated with its RA function, as defined in this Q&N CPS, the applicable CP's and the Certipost E-Trust RA Procedures and Guidelines.

f) **Quality of the Key Pair Generation** – If the CRA generates the Subscribers' keys: to generate their cryptographic key pairs, and to use them properly, the CRA is 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 CRA is obliged to generate the Subscribers' keys using a key generation algorithm, a key length, and a signature algorithm recognized as being fit for the purposes of certificate usage. If the CP requires use of an SSCD and the CRA generates its keys, then the key shall be created within an SSCD.

2.1.2.2 LRA obligations

See specific CP for specific requirements related to the Certificate type for which registration is requested by a Subscriber.

The LRA is under a contractual obligation to scrupulously follow the registration procedures described in the CSP's CPS.

The LRA shall guarantee that:

a) Certificate Holders are correctly identified and authenticated, with respect both to their personal identity as natural persons and to any mentions of their professional status.

b) Applications for Certificates submitted to the CSP are complete, accurate, valid and duly authorized.

In particular:

c) The registration officer shall inform the Certificate Holder of the terms and conditions for the use of the Certificate. These are set out in the Order Form and the General Terms and Conditions to be signed by the Certificate Holder (paper or notarized electronic format).

d) The registration officer shall check the identity of the Certificate Holder on the basis of valid ID papers recognized under Belgian law. These papers shall indicate, inter alia, the full name (last name and first names), date and place of birth, and the postal address at which the Certificate Holder can be contacted.

e) The registration officer shall also verify any information relating to the Certificate Holder's professional status for the purposes of certification.

f) If the Certificate Holder is an affiliate of a legal person, the registration officer shall validate the documentation supplied as proof of the existence of this relationship.

g) The registration officer shall store one copy of the information provided during registration procedure by the Certificate holder and sent, in its entirety, to the CSP, and in particular:

- A copy 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.
- A copy of the contractual agreement signed by the Certificate Holder, including the latter's agreement to all obligations incumbent on him.
- The above information is archived for a period of 30 years after the expiry of the last Certificate, corresponding to this registration.

h) If the key pair is not generated by the CSP or the LRA, the validation procedure used by the registration officer for electronic Certificate applications shall guarantee that the Certificate Holder is in possession of the Private Key linked to the Public Key to be certified.

i) Compliance with the requirements on the protection of personal data in connection with registration procedures shall be enforced.

j) The LRA has a contractual obligation to take clear and appropriate measures vis-à-vis:

- The physical security of the information and, where appropriate, of the systems;
- The logical access to any software;
- The employees in charge of registration.

k) The classification of and responsibilities for this data are of crucial importance and shall be handled in accordance by the LRA. This covers the following:

- The data itself; in paper format (registration data, guidelines and procedures, etc.) and, where applicable, in electronic format;
- The software applications used and their configuration.
- Hardware equipment (e.g. PC's, telecommunications equipment, etc.) and their configuration.
- Physical access to the data (buildings, safes, access controls and conditional access to software such as smartcards, etc.).

l) The LRA shall ensure these items (2.1.2.2 k) are managed and stored in such a way as to avoid any impact as a result of a loss of confidentiality, integrity or even availability of this data.

m) Quality of the Subscribers' key pair generation: If the LRA generates Subscribers' keys: to generate their cryptographic key pairs, and to use them properly, the LRA is 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 unauthorised usage of a Private Key. In particular, the LRA is obliged to generate Subscribers' 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 LRA generates its keys, then the key shall be created within a SSCD.

2.1.3 Subscriber obligations

The following are the obligations of any Subscriber to services within the Certipost E-Trust PKI Infrastructure:

a) Accuracy in Certificate applications -- 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.

b) Quality of the key pair generation – 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 unauthorised 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.

c) Protection of Subscriber's Private Key -- Subscribers are obliged to protect their Private Key at all times, against loss, disclosure, modification and unauthorised 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 pass phrase, used to protect against unauthorised 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 pass phrase has been entered). Subscribers shall securely archive their Private Key after the validity period of his certificate.

d) Strict compliance with the Certificate deliverance rules and procedures -- Subscribers are obliged to strictly follow the conditions and procedures to be followed in order to request a Certificate in accordance with the CPS and the applicable CP. If the CP requires use of an SSCD, the Subscriber shall only use the certificate with electronic signatures created using such a device.

e) Certificate Acceptance and verification -- The Certificate is deemed accepted by the Subscriber within 8 days from the issuance or at the moment of its first use, whichever is the earliest. If the Subscriber notices an inconsistency between the contractual agreement information and the content of his/her Certificate, he/she must inform Certipost E-Trust without any delay. Certipost E-Trust will then revoke the Certificate and take the appropriate measures either to refund the Certificate price to the Subscriber or to reissue a Certificate. This will be the Subscriber's sole remedy for any acceptance refusal.

f) Notification of CA upon Private Key compromise -- Subscribers are obliged to notify without any delay, up to the end of the validity period indicated in their certificate, the CA that issued their Certificate by sending a Certificate suspension or revocation request:

- upon suspicion that the Subscriber's Private Key is potentially compromised
- the Subscriber's Private Key has been lost or stolen
- Control over the Subscriber's Private Key has been lost due to compromise of activation data (e.g. PIN code or pass phrase) or other reasons

The CA that issued the concerned certificate will immediately revoke this certificate.

g) Notification of CA upon any change in their Certificate content -- The Subscribers are obliged to notify immediately the CA that issued their Certificates upon any inaccuracy or change in the content of their Certificates by means of a Certificate revocation request.

h) Proper use of a Certificate -- Subscribers are obliged to comply with all restrictions or limitations to the use of their Private Keys and Certificates. The Subscriber will only use the key pair for intended use as written in the Certificate and related CP and in accordance with any other limitations notified to the Subscriber. Furthermore, when a Certificate has expired, been suspended or been revoked, the Certificate becomes immediately invalid and the Subscriber shall immediately and permanently stop the use of the corresponding Private Key (e.g., to generate a digital signature or to request a Certificate for the corresponding key pair to another Certification Authority).

i) Sanctions -- A Subscriber who is found to have acted in a manner counter to these obligations will have its Certificate revoked, and will have no claim against Certipost E-Trust in the event of a dispute. Certipost E-Trust reserves the rights to prosecute the fraudulent Subscriber in accordance to the applicable law. The Subscriber will respond to the direct and indirect damages as a result of the non-execution of the obligations that are imposed by this CPS, the related CP, and the contract or by the applicable law. Certipost E-Trust is not liable for any consequence due to the violation by

the Subscriber of his obligations included in the present section.

j) Relying Party Information -- The Subscriber is obliged to inform the relying parties of the issues stated in section 2.1.4.

For possible additional specific obligations see specific CP.

2.1.4 Relying party information

The following are the Relying Parties' obligations:

a) Proper use of Certificates -- Relying Parties are obliged to use the Certificate for the purpose for which it was issued, notably the limitations of use or, in the case of transactions, the limitations of the value of the transactions, in accordance with the corresponding CP and if necessary with the current Q&N CPS.

b) Revocation or suspension checking responsibilities – Prior to its use, Relying Parties are obliged to verify the validity, suspension or revocation of the Certificate using current revocation status information through the Certipost E-Trust Certificate Public Registry.

c) Digital Signature verification responsibilities -- Relying Parties are obliged to verify the Digital Signature of a received digitally signed message and to verify the digital signature of the CA who issued the Certificate used for the verification purpose.

d) Establishing trust in CA -- Relying Parties are obliged to establish trust in the CA who issued the Certificate they are about to use by verifying the chain of Certificates at the root of which a trusted CA exists. The path processing should be based on the guidelines set by the X.509 standard.

e) A Relying Party shall take **any other precautions** prescribed in agreements or elsewhere.

f) A Relying Party who is **found to have acted in a manner inconsistent** with these obligations will have no valid claim against Certipost E-Trust in the event of a dispute. Certipost E-Trust is not liable for any consequence due to the violation by a relying party of his obligations included in section 2.1.4.

2.1.5 Repository obligations

a) Certipost E-Trust Services is obliged to timely provide publication of Qualified, Normalised or Lightweight Certificates and the related Certificate Revocation List as detailed in 4.4.6.

b) Certipost E-Trust Services will make use of a Public Registry to publish issued digital Certificates and Certificate Revocation Lists, except when otherwise agreed with the Subscriber in the applicable CP.

2.2 Liability

2.2.1 Warranties and limitations on warranties

a) CA's warrant only that their procedures are implemented in accordance with their published Q&N CPS, and that any Certificates issued that assert a policy OID defined in this document were issued in accordance with the stipulations of this Q&N CPS and the corresponding CP for that level of assurance. In addition other warranties may be implied in this Q&N CPS definition by operation of law.

b) By signing a Certificate containing a policy OID which indicates the use of the corresponding CP, a CA certifies to all who reasonably rely on the information contained in the Certificate, that it has checked the information in the Certificate according to the procedures laid down in that CP and in the present Q&N CPS, that the information was correct at the time of issuance of the Certificate, that the Subscriber possessed the data for the creation of the signature conform to the Certificate's verification data at the time of issuance of the Certificate and that the data relating to the creation

and verification of the signature can be used complementarily.

c) RA's warrant that they perform their duties in accordance with applicable sections of this Q&N CPS, the corresponding CP to which they are subject and the internal procedures and guidelines. The CA shall undertake liability for all RA services provided on behalf of the CA. RA liabilities are therefore primarily handled between the CA and the RA. The CA shall synchronise its contract with the RA to this policy.

2.2.2 Damages covered and disclaimers

Except as expressly provided in section 2.2.1 and in the applicable legislation, Certipost E-Trust disclaim all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaim any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties. Certipost E-Trust does not warrant "non repudiation" of any Certificate or message. Certipost E-Trust does not warrant any software.

2.2.3 Loss limitations

To the extent permitted by law, Certipost E-Trust makes the following exclusions or limitations of liability:

a) In no event shall Certipost E-Trust be liable for any indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates, Digital Signatures, or other transactions or services offered or contemplated by this Q&N CPS even if Certipost E-Trust has been advised of the possibility of such damages.

b) In no event shall Certipost E-Trust be liable for any direct, indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use or the reliance of a suspended, revoked or expired Certificate.

c) The aggregate liability of Certipost E-Trust to all parties, including but not limited to Subscribers, applicants, recipients or relying parties, shall not exceed, if and to the extent permitted under applicable law, the applicable liability cap for such Certificate set forth below. The combined aggregate liability of Certipost E-Trust to any and all persons concerning a specific Certificate shall be limited to an amount not to exceed the following, for the aggregate of all digital signatures and transactions related to such Certificate:

- Liability cap for Qualified or Normalised Certificates: 25.000 EUR.
- Liability cap for Lightweight Certificates: 250 EUR

If and to the extent such limitations are not permitted under applicable law, than the liability of Certipost shall be limited to the maximum extent permitted under applicable law.
This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary, or incidental damages, incurred by any person, including without limitation a Subscriber, an applicant, a recipient, or a Relying Party, that are caused by reliance on or use of a Certificate Certipost E-Trust issues, manages, uses, suspends or revokes, or such a Certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim. The liability cap on each Certificate shall be the same regardless of the number of Digital Signatures, transactions, or claims related to such Certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court or competent jurisdiction. In no event shall Certipost E-Trust be obligated to pay more than the aggregate liability cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the

liability cap.

d) By accepting a Certificate, the Subscriber agrees to indemnify and hold Certipost E-Trust and his agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, that Certipost E-Trust and its agents and contractors may incur, that are caused by the use or publication of a Certificate and that arises from:

- Falsehood or misrepresentation of fact by the Subscriber;
- Failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive Certipost E-Trust or any person receiving or relying on the Certificate;
- Failure to protect the Subscribers Private Key, to use a trustworthy system, or to otherwise, take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorised use of the Subscriber's Private Key.

2.2.4 Other exclusions

Not applicable.

2.3 Financial responsibility

2.3.1 Indemnification by relying parties

Certipost E-Trust assumes no financial responsibility for improperly used Certificates.

2.3.2 Fiduciary relationships

Issuance of Certificates in accordance with this Q&N CPS and the corresponding CP does not make the CA, or any RA within the Certipost E-Trust Infrastructure an agent, fiduciary, trustee, or other representative of Subscribers or relying parties.

2.3.3 Administrative processes

Not applicable.

2.4 Interpretation and Enforcement

2.4.1 Governing law

The laws of Belgium shall govern the enforceability, construction, interpretation, and validity of this Q&N CPS, of the related CP's and of the related contracts. See applicable CP and applicable related contractual agreements (Purchase Order, General Conditions) for more details about policies and procedures for complaints and disputes resolution.

2.4.2 Severability, survival, merger, notice

2.4.2.1 Severability

a) The titles and subtitles of this Q&N CPS are influenced by the international standardisation process. In interpreting this Q&N CPS the text under each title shall be given precedence over the wordings in the titles.

b) The Q&N CPS validity shall not be affected by one of its clauses being declared null and void; insofar as is possible, the clause that is declared null and void shall be replaced by a clause which best defines the intention of the clause declared null and void.

2.4.2.2 Survival

Any provision of this Q&N CPS that, in order to fulfill the purposes of such provision, needs to survive the termination or expiration of this Q&N CPS, shall be deemed to survive for as long as necessary to fulfill such purposes.

2.4.2.3 Merger

In case of a merger, Certipost E-Trust shall ensure the continuity and stability of the CA operation with all reasonable means.

2.4.2.4 Notice

All notices and other communications which may or are required to be given, served or sent pursuant to this Q&N CPS shall be in writing and shall be sent, except provided explicitly in the Q&N CPS, either by (i) registered mail, return receipt requested, postage prepaid, (ii) an internationally recognised "overnight" or express courier service, (iii) hand delivery (iv) facsimile transmission, deemed received upon actual delivery or completed facsimile, or (v) an advanced electronic signature based on a Qualified Certificate and a secure signature creation device (SSCD).

2.4.3 Dispute resolution procedures

a) Any dispute that cannot be resolved, amicably, shall be subject to a final decision by arbitration conforming the CEPANI rules. Arbitration shall take place in Brussels. The language of the procedure shall be French or Dutch.

b) However, taking in account article 14 of the law of 21 march 1991 relating to the reform of certain public economic companies, if the Subscriber is a natural person, any dispute which cannot be resolved amicably, shall be subject to a sole decision by the Brussels Courts, unless the Subscriber agrees to arbitration after the dispute has risen.

2.5 Fees

Public fees for Certipost E-Trust Services are established and published on the following URL **http://www.e-trust.be/**

2.5.1 Certificate issuance or renewal fees

a) *Qualified, Normalised or Lightweight Certificate fees* are provided by Certipost E-Trust in the corresponding purchase orders, available on http://www.e-trust.be.

b) *Renewal fees*:

- not applicable for certificate renewal, because certificate renewal is not allowed.
- for certificate rekey, the same fee (and procedure) as the first issuance is applicable, unless otherwise stipulated

2.5.2 Certificate access fees

Access to Certificates on the Certipost E-Trust Certificate Public Registry is free of charge excluded communication costs.

2.5.3 Revocation or status information access fees

Access to Certificate Revocation Lists on the Certipost E-Trust Certificate Public Registry is free of charge excluded communication costs.

2.5.4 Fees for other services such as policy information

a) Fees are provided by Certipost E-Trust 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 on-line or physical media copies of this Q&N CPS or for supplying on-line copies of a CP supported by this Q&N CPS, or as stated in section 4.6.7 b) (non exhaustive list) .

2.5.5 Refund policy

Not applicable, except if a specific agreement is made, in particular in case of non acceptance of certificate by subscriber, see section 4.3 b) for further details.

2.6 Publication and Repository

2.6.1 Publication of CA information

a) CA's within the Certipost E-Trust PKI shall make publicly available, in their repositories:

- The Certipost E-Trust Services Q&N CPS;
- The public applicable CP's under which Certificates are issued according to this Q&N CPS;
- Certification Revocation Lists;
- Authority Revocation Lists;
- All CA-Certificates issued by the CA, self signed CA-Certificate and cross Certificates for cross certified CA's;
- Public purchase orders and general conditions;
- All Certificates issued by the CA in conformance with this Q&N CPS

CRL's and Certificates shall be available on the public repository all days, 24 hours per day, except in case of Force Majeure. Certipost E-Trust will do its best efforts to obtain an uptime of **99 %** for its public repository service.

Information objects in Certificates issued under this Q&N CPS and applicable CP's are regarded as personal data of the Subscriber. In order to carry out its tasks in an efficient manner, Certipost E-Trust uses databases with these personal data. In this regard, Certipost E-Trust respects the privacy of the persons concerned. The Subscriber authorises Certipost E-Trust to publish such personal data on its repositories.

b) Certipost E-Trust shall publish a copy of issued Certificates in publicly available repositories, after the Certificate has been issued by Certipost E-Trust.

c) The Subscriber is responsible to check the correctness of the published information and act as specified in section 2.1.3 (e)

d) Certipost E-Trust shall provide relevant information about issued Certificates when necessary to aid in dispute resolution concerning, for example, digital signatures.

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

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

2.6.2 Frequency of publication

a) CRL publication shall be in accordance with section 4.4.9.

b) CPS publication shall be in accordance with section 8.

2.6.3 Access controls

a) There shall be no access controls on the reading of the public CP or of the public Q&N CPS. Everybody has read access.

b) Access controls on Certificates are optional at the discretion of the CA and may be part of a specific rule of a particular CP.

c) There shall be appropriate access controls controlling who can write or modify all items in the electronic repository concerned by (sub(a) and sub(b)). The Certipost E-Trust Certificate Public Registry, the CP's and Q&N CPS are protected against any unauthorised modification.

2.6.4 Repositories

Certipost E-Trust Services will use the Certipost E-Trust Certificate Public Registry to publish the issued Certificates and the CRL's. All the CA's issuing Certificates according with this Q&N CPS will make use of this registry unless expressly stipulated otherwise in the corresponding CP. In that case the chosen electronic repository can be one appropriate to the Certificate using community, and shall comply with the constraints expressed in the current Q&N CPS as a minimum requirement, in accordance to the total security requirements. Such repository may be operated by the CA or by a separate organisation.

2.7 Compliance audit

a) CA's issuing Certificates make a statement to those who reasonably rely on the information in the Certificate that their practices fully comply with this Q&N CPS.

b) It is strictly prohibited for any person or organisation to falsely claim compliance with this Q&N CPS. Certipost E-Trust will take legal actions against any person or organisation disregarding this prohibition.

2.7.1 Frequency of entity compliance audit

a) The Certipost E-Trust PKI Certification Practices Council, 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 Q&N CPS, in the appropriate CP's and in internal documents.

b) CA's operating under this Q&N CPS shall be audited regularly for conformance with the present

Q&N CPS and the appropriate CP's.

c) The Certipost E-Trust PKI Certification Practices Council 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 Q&N CPS, in the appropriate CP's and in internal documents.

2.7.2 Identity/qualifications of auditor

a) 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 Q&N CPS. The auditor shall be named in the Revision Status of the Q&N CPS and, if relevant, the appropriate CP's.

b) The auditor and CA shall have a contractual relationship for the performance of the audit, and be sufficiently organisationally 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.

2.7.3 Auditor's relationship to audited party

As stated in section 2.7.2 of this CPS.

2.7.4 Topics covered by audit

a) The audit only compares the practices laid down in this Q&N CPS and the appropriate CP's with the on site CA's implementation. All aspects of the CA's operation as specified in this Q&N 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 Q&N CPS meets the requirements in this Q&N CPS, or to trust the statement of compliance by the CA.

2.7.5 Actions taken as a result of deficiency

a) Any discrepancies between a CA's operation and a stipulation of its CP's /Q&N CPS must be noted and immediately notified to the Certipost E-Trust PKI Certification Practices Council. The CEPRAC will determine a remedy, including a time for completion.

Certipost E-Trust Services PKI Certification Practices Council C/o Bart Callens Muntcentrum B-1000 Brussels Belgium	http://www.e-trust.be Fax: +32 (53) 601 151 e-mail : info@e-trust.be

b) 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.

c) 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.

d) 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.

e) 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.

2.7.6 Communication of results

a) Conclusive results of the audits shall be distributed to the audited RA, the audited CA, and to the Certipost E-Trust PKI Certification Practices Council. 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 Q&N 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 E-Trust PKI Certification Practices Council. A special audit may be required to confirm the implementation of the effectiveness of the remedy.

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

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 E-Trust 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., Centre Monnaie - Munt Centrum, 1000 Brussels. The data will be used for the provisioning of the Certipost E-Trust 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[2], 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 Q&N CPS are to be kept

[2] And if applicable without prior consent of the subscriber's employer.

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 section 4.6.7 of this Q&N CPS.

2.8.2 Types of information not considered confidential

a) Certificates, CRL's, revocation/suspension information and any information available on http://www.e-trust.be are not considered confidential.

b) Identification information or other personal or corporate information appearing on Certificates is not considered confidential.

2.8.3 Disclosure of Certificate revocation/suspension information

As Certificate revocation/suspension information is not considered confidential, it is disclosed.

2.8.4 Release to law enforcement officials

Release to law enforcement officials is in accordance with the applicable laws and regulations.

2.8.5 Release as part of civil discovery

Not applicable.

2.8.6 Disclosure upon owner's request

As stated in section 2.8.1.

2.8.7 Other information release circumstances

Not applicable.

2.9 Intellectual Property Rights

The present Q&N CPS and the applicable CP's are the property of Certipost E-Trust and are protected by intellectual property rights, unless otherwise agreed. Any use not allowed by the Q&N CPS and the applicable CP's may entail civil and criminal proceedings.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names for Qualified, Normalised and Lightweight Certificates

Attribute	Necessity	Comments
Country (C)	Mandatory	**Physical person**: Nationality of the Subscriber as it appears on the Subscriber's identity card. **Legal person**: Country in which the organisation has its social siege (as stated in the Articles - Statutes of organisation). **Other entities**: Country of location.
State/Province (ST)	Optional	**Physical person**: Not applicable, unless stated otherwise in the applicable CP. **Legal person**: Not applicable, unless stated otherwise in the applicable CP. **Other entities**: State/Province of location, unless stated otherwise in the applicable CP.
Locality (L)	Mandatory if no Organisation is present.	**Physical person**: Place of Birth of the Subscriber as it appears on the Subscriber's identity card. **Legal person**: Locality in which the organisation has its social siege (as stated in the Articles - Statutes of organisation). **Other entities**: Locality of location.
Organisation (O)	Mandatory if no Locality is present.	**Physical person**: - For private person: Not applicable, unless stated otherwise in the applicable CP. - For employees/administrator/manager: official name of the Company employing the Subscriber (published in the Company Articles of association), unless stated otherwise in the applicable CP. - For independents: official name of the Company employing the Subscriber (published in the Company Articles of organisation), unless stated otherwise in the applicable CP. **Legal Person**: Official name of the legal entity as it appears in its official statutes or articles of association.
Organisation unit or Department (OU)	Optional, and allowed only if Organisation is present	**Physical person**: – For private person: Not applicable, unless stated otherwise in the applicable CP. – For employees/administrator/manager: unit or department in the Company employing the Subscriber – For independents: unit or department in the Company employing the Subscriber.
Common Name (CN)	Mandatory	**Physical person**: Family name, first names and initials of additional first names of the Subscriber as it is on his valid identity card. **Legal Person**: Official name of the legal entity as it appears in its official statutes. This should include the legal form of the legal entity. **Other entities**: Unique name identifying the entity.

The above table represents however the **minimal** set of attributes. Other attributes can be added by Certipost E-Trust, see applicable CP.

3.1.2 Need for names to be meaningful

a) In case of Subscribers, the information in the Certipost E-Trust Certificate Public Registry (directory) and in the Certificate can be matched with the information on the official identity card.

b) The use of a pseudonym is not allowed by Certipost E-Trust.

c) In case of legal person (organizational entities), the naming information must match the legal characteristics (legal name) that have been registered in accordance with applicable laws and regulations.

d) All other information (attributes) shall be consistent with internationally accepted standards and guidelines.

3.1.3 Rules for interpreting various name forms

See section 3.1.1 and 3.1.2.

3.1.4 Uniqueness of names

In fact, the combination of country, locality/organisation and common name (family name, first names and the initials of additional first names) will uniquely identify the Certificate's owner.

3.1.5 Name claim dispute resolution procedure

a) In case of any name claim dispute, the requester will contact Certipost E-Trust Services (see contact information in section 1.4.2. Certipost E-Trust Services will investigate the grounds on which the name claim dispute is based.

b) Any entity acting within the Certipost E-Trust PKI Infrastructure is obliged to give appropriate and sufficient co-operation to an investigation mentioned in section 3.1.5a).

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

d) 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 E-Trust reserves the right to terminate the contract(s) immediately, to revoke the Certificate and to refuse to continue any collaboration with that person. Furthermore Certipost E-Trust reserves the right to undertake legal actions.

3.1.6 Recognition, authentication and role of trademarks

a) Certipost E-Trust can not guarantee that the names issued will contain the requested trademark.

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

c) Section 3.1.5 is also applicable.

3.1.7 Method to prove possession of Private Key

a) 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 standard). This will enable the RA to verify the user's Private Key possession.

b) Additional measures can be taken on a per Certificate type basis (see related CP), such as Registration Authentication PIN (RAP), call backs, etc.

3.1.8 Authentication of organisation's identity

a) The RAs within the Certipost E-Trust 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 organisation identity.

b) For the Certipost E-Trust Qualified, Normalised or Lightweight Certificate the authentication of an organisation entity will require the appropriate documents as specified in the applicable CP (see applicable CP for details).

3.1.9 Authentication of individual identity

a) The RA within the Certipost E-Trust 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.

b) The authentication of an individual entity will require the appropriate documents as specified in the applicable CP (see applicable CP for details).

3.2 Routine Rekey

Same process as initial registration shall be performed.

3.3 Rekey after Revocation

Same process as initial registration shall be performed.

3.4 Revocation Request

3.4.1 Revocation, Suspension and Unsuspension Request

A Certificate Holder (physical or legal person), the legal representative (or his duly appointed proxy) of the organisation if the Certificate Holder (physical person) has had the professional part of the Certificate certified, the LRA or Certipost E-Trust may apply for suspension, unsuspension or revocation of the Certificate. The Certificate Holder and, where applicable, the legal representative (or his duly appointed proxy) shall be notified of the suspension, unsuspension or revocation of the Certificate. The CSP shall make a form for the suspension/unsuspension/revocation of the Certificate available to the parties concerned. The applications and reports linked to a suspension, unsuspension following suspension or revocation shall be processed on receipt, and authenticated and confirmed in the following manner (minimal requirements):

In the case of **suspension**:

a) The applicant shall notify, either by phone, by e-mail or by fax, the Suspension and Revocation Authority (SRA) of the CSP which issued the concerned Certificate.
b) The SRA shall then immediately suspend the Certificate, as from the date on which the application is received. The form shall be sent by fax or by post to the CSP within 14 working days, failing which the Certificate will be unsuspended.
c) When confirmed, the suspension of a Certificate shall be so for an unlimited period of time.

In the case of **unsuspension**:

a) To obtain the form required for unsuspension, the applicant shall contact the Suspension and Revocation Authority of the CSP which issued the Certificate.
b) The applicant shall make an appointment with the LRA approved by the CSP and present himself in person with the duly completed form and a (double-sided) signed copy of his identity card.
c) The LRAO shall then verify the documents submitted and the identity of the applicant. If the request is validated, the LRAO shall immediately transmit it to the SRA.
d) The SRA shall then reinstate the Certificate within 24 hours of receiving the application.

In the case of **revocation**, the applicant shall:

a) Request the suspension of the Certificate (see above);
b) Contact the SRA to ask for a certificate revocation application form.
c) The applicant shall make an appointment with the LRA approved by the CSP and present himself in person with the duly completed form and a (double-sided) signed copy of his identity card.
d) The LRAO shall then verify the documents submitted and the identity of the applicant. If the request is validated, the LRAO shall immediately transmit it to the SRA.
e) The SRA shall suspend the Certificate, as from the date on which the application is

received. The Certificate shall be revoked (or unsuspended) after a period of investigation of a maximum of 10 working days.

Revocation of a Certificate shall be definitive.

a) In case of suspension, the CA will also identify the requester by verifying the challenge password. This challenge password is the one requested in the Subscriber contract (see the corresponding CP, and contractual agreements).

b) In case a Subscriber, a legal representative or the authorised delegate of the legal representative requests a revocation, the authentication of the request will require the following documents:

- The Subscriber: the revocation form duly filled in and signed, a signed copy (recto/verso) of his valid piece of identity;
- The legal representative: the revocation form duly filled in and signed, a signed copy (recto/verso) of his valid piece of identity and the current articles of association of his organisation;
- The authorised delegate of the legal representative: the revocation form duly filled in and signed, a signed copy (recto/verso) of his valid piece of identity, the valid articles of association of his organisation and proof of his ability to represent the legal representative.

For more details, see applicable CP.

c) The above process and requirements are minimal requirements; more strict requirements can be specified in the applicable CP.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

In order to apply for a Certificate, the following steps need to be undertaken:

a) The Procedures described in the applicable CP and in the applicable contractual agreement (purchase order, general terms and conditions and CP) have to be followed by the requester.

b) Requester will initiate the generation of a Public/Private Key pair.

c) In case the Public/Private Key pair is generated by CSP (e.g., at RA premises), the secret key is given solely to the requester who must also provide a passphrase to protect his Private Key once in its possession (this passphrase is introduced by the requester to protect his key without revealing it).

d) Requester will provide an electronic Certificate request in accordance with the three previous points and with the applicable CP (see applicable CP for details).

e) Requester will sign 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 authorise the creation and the publication of the obtained Certificate in the Certipost E-Trust Certificate Public Registry.

4.2 Certificate Issuance

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

a) The issuing CA performs Certificate issuance and for this ensures that new and rekeyed Certificates are issued securely.

b) The procedure of issuing the Certificates is securely linked to the associated registration, certificate rekeys, including the provision of any subscriber generated public key. In particular, prior to 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. The information provided in the signed contractual agreement prevails on the electronic information.
   - If the Subscriber takes care of the key generation, the RA checks the self-signed request (e.g., PKCS#10 request).
   - RA archives all the information (paper and electronic).
   - RA sends the request securely to the CA.
   - The CA will generate the Certificate and publish it in the Certipost E-Trust Certificate Public Registry
   - The Subscriber is notified by the CA that the Certificate was issued. A copy of the Certificate is sent directly to the requester. For more details, see applicable CP.
   - In case the key generation is done by the CSP before the complete authentication (face to face identification), the certificate will be immediately temporarily suspended by the CSP right after issuance and publication of the certificate and before the delivery of the certificate to the Subscriber. After the complete authentication (face to face identification) and delivery of the key pair, the certificate is unsuspended by the CSP.

c) The Qualified Certificates are generated and issued in accordance with annex I of The European Directive. See applicable CP for details on Certificate content

d) If the issuing CA (CSP) generated the Subscriber's key, then

- The procedure of issuing the Certificate is securely linked to the generation of the key pair by the CA (CSP).
- The Private Key is securely passed to the registered Certificate owner (subscriber).

e) The issuing CA ensures over time the uniqueness of the distinguished name assigned to the subscriber within the domain of the CA, as described in 3.1.4.

f) The confidentiality and integrity of registration data shall be protected especially when exchanged with the Subscriber or between distributed CA system components.

4.3 Certificate Acceptance

a) The Certificate owner accepts that his Certificate is published immediately after its generation in the Certipost E-Trust Certificate Public Registry, unless specified otherwise in the CP.

b) The Certificate is deemed accepted by the Subscriber within 8 days from the issuance or at the moment of its first use by the Certificate Holder, whichever is the earliest. If the Subscriber notices an inconsistency between the contractual agreement information and the content of his/her Certificate, he/she must inform Certipost E-Trust without any delay. Certipost E-Trust will then revoke the Certificate and take the appropriate measures either to refund the Certificate Price to the Subscriber or to reissue a Certificate. This will be the Subscriber's sole remedy for any acceptance refusal.

4.4 Certificate Suspension and Revocation

a) The suspension and revocation procedures that are set forth in this Q&N CPS and the applicable CP will be in accordance with the applicable law. The Subscriber and, if applicable, the legal representative of the Organisation (or his authorised delegate) will be notified of the revocation or the suspension.

b) 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 provisions of section 4.2 are applicable.

c) The request for suspension / revocation and the related documents shall be recorded and archived.

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

e) The CRL issuance frequency shall be at least every twenty-four (24) hours**.** Additionally, a new CRL shall be published immediately when a Certificate has been suspended, unsuspended or revoked.

f) Suspension / 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.

g) Suspension / 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.

h) 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.

i) Suspension / Revocation status information is publicly and internationally available on ldap://ldap.e-trust.be as CRL attribute of the Certipost E-Trust TOP Root CA, Primary CAs and Secondary CAs. OCSP (Online Certificate Status Protocol) services may be additionally provided, see applicable CP and Certificate content for details.

4.4.1 Circumstances for suspension / revocation

Revocation occurs on decision of the Suspension and Revocation Authority (SRA):

a) Upon request by and after authentication of the Subscriber, the legal representative (or his authorised representative), Certipost E-Trust authorised representatives or entities, or authorities in accordance with the applicable law;

b) When serious and motivated reasons exist to establish that:

- The Certificate has been delivered from wrong or falsified information.
- The certified information is not valid any more.
- The confidentiality of the Private Key is no more ensured or has been compromised.
- The Certificate has not been paid in respect with the contractual provisions.

c) When the CA stops its activities without another CA overtaking its activities;

d) In this case: (i) the Subscribers will be informed at least 2 months before revocation, and (ii) all relevant information about the Certificate will stay registered for a period of 30 years.

4.4.2 Who can request suspension / revocation?

a) Revocation can be requested by

- The Subscriber.
- The legal representative of the Organisation or his authorised delegate, when the Organisation of the Subscriber is certified in the Subscriber's Certificate.
- The Certipost E-Trust PKI Certification Practices Council.
- (Local) Registration Authorities having taken part in the registration of the concerned Certificate.
- An authorised legal authority.

4.4.3 Procedure for suspension / revocation request

a) Revocation can be asked by

- Filling in the revocation form that can be found in the general conditions as part of the contractual agreement (available on the following web site: http://www.e-trust.be/CPS/QNCerts).
- Calling Certipost E-Trust Services.
- Going in person to a RA.

The possibility to use any of the above mentioned methods for requesting revocation is governed by the related CP.

b) The Certificate is immediately suspended according to the following procedure. The Certificate will be suspended in real time. During this suspension period, the SRA will as soon as possible investigate the revocation request (see section 3.4 of the present CPS and applicable CP). If the revocation request is authenticated and validated, the SRA will revoke the Certificate.

c) Revoked Certificates cannot be unrevoked. Revocation is an irreversible process.

d) The requests and reports linked to a suspension, unsuspension or revocation will be processed and treated as from the moment of receipt, authenticated and confirmed as specified in the applicable CP (see also section 3.4.1 of the present document).

e) In case of suspension, the CA will also identify the requester by verifying the challenge password. This challenge password is the one requested in the Subscriber contract (see the corresponding CP, and contractual agreements).

4.4.4 Revocation request grace period

Not applicable.

4.4.5 Limits on suspension period

a) Revocation request: a Certificate is suspended for maximum 10 working days following the revocation request (day of the request, if it is a working day, included), duration of the investigation period after which the Certificate is either revoked or unsuspended depending on the investigation results;

b) Suspension request: a Certificate can be suspended for an unlimited period of time.

4.4.6 CRL issuance frequency (if applicable)

The CRL issuance frequency shall be at least every twenty-four (24) hours**.** Additionally, a new CRL shall be published immediately when a Certificate has been suspended, unsuspended or revoked.

4.4.7 CRL checking requirements

a) The CRL is checked at the Certificate Relying Party's own responsibility. This particularly refers to the CRL lookup frequency, which is the sole responsibility of the Relying Party.

b) The CRL can be checked with appropriated software accessing the Certipost E-Trust Certificate Public Registry (e.g. DAP, LDAP or HTML protocols). See the Certipost E-Trust web site (http://www.certipost.be/en/X500.php3) and section 4.4 i) for more details.

4.4.8 On-line revocation status checking availability

OCSP (Online Certificate Status Protocol) services may be additionally provided, see applicable CP and Certificate content for details.

4.4.9 On-line revocation status checking requirements

OCSP (Online Certificate Status Protocol) services may be additionally provided, see applicable CP and Certificate content for details.

4.4.10 Other forms of revocation advertisements available

The Certificate owner is always notified of the revocation of his Certificate either by phone, by mail, by fax or by E-mail.

4.4.11 Checking requirements for other forms of revocation advertisements

Not applicable.

4.4.12 Special requirements re key compromise

See section 4.8 of this Q&N CPS.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

The following types of events are recorded in the whole Certipost E-Trust PKI:

a) *System Log File*: The operating systems record in their own system log files the following events (non-exhaustive) :

- Start-up and shutdown of the servers
- Tasks performed by users, fulfilling the trusted roles as defined in 5.2.1, and applications

b) *Security System Log File:* For extending the system logging, dedicated software is used to keep track of the security and any significant changes that were done on the system level. The events that are recorded that way are centrally monitored and analysed. These event recordings include (non-exhaustive) :

- Tracking of the Operating System security patch level.
- Tracking of the integrity of critical system files.
- Tracking of installations of new software.
- Tracking of security parameters, such as users and password policies.
- Tracking of the findings of malicious files.
- Tracking on back-up parameters.

c) *Application log:* Created by one of the Certipost E-Trust PKI Infrastructure components that logs each and every operation. This last information is stored and (digitally) signed. This information is not alterable. Furthermore these log files are physically protected like the other parts of the PKI and not accessible from the outside of the Certipost E-Trust PKI Infrastructure. These event recordings include (non-limitative) :

- The creation of the Certipost E-Trust Certificate Public Registry-entries.
- 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.

d) These log files are regularly archived and stored securely.

4.5.2 Frequency of processing log

a) All the information that is mentioned in section 4.5.1 of this CPS is processed on-line.

b) The log files are analyzed regularly in order to detect any dysfunction or malicious action.

4.5.3 Retention period for audit log

Audit logs will be retained for a period of **30 years**.

4.5.4 Protection of audit log

a) Logs created by the CA/RA components from the Certipost E-Trust PKI Infrastructure are digitally signed.

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

c) Access control is restricted to the database access to which only security officers have access. There is no encryption of these logs.

4.5.5 Audit log backup procedures

a) The back-up of the application audit log files is done daily, using a highly secured and encrypted link to the back-up location.

b) The back-up location is protected with similar security level measures than the principal location.

4.5.6 Audit collection system (internal vs external)

Both are used.

4.5.7 Notification to event-causing subject

Not applicable.

4.5.8 Vulnerability assessments

a) The audit logs are analysed by Operators (see section 4.5.2 of this Q&N CPS)

b) Network vulnerability assessments are carried out on a regular basis to ensure that the servers on the Certipost E-Trust PKI segment are secured appropriately.

4.6 Records Archival

Beside the information, listed in 4.5, all information published in Certipost E-Trust Certificate Public Registry and all information exchange between the user and the different elements of the Certipost E-Trust PKI segment are recorded.

4.6.1 Types of event recorded

a) Electronic Certificate requests.

b) Signed registration forms (contractual agreements) from Subscribers' applications for Certificates.

c) Contents of issued Certificates.

d) Records on CA rekeying including key identifiers and cross Certificates.

e) Records on cross certification including the inquiry for cross certification and the performed actions.

f) Revocation / Suspension / Unsuspension requests and all recorded messages exchanged with the originator of the request and/or the Subscriber and other relevant revocation / suspension / unsuspension checking information.

g) CRL's.

h) Audit results.

i) Current and former contractual agreements and CPS's.

4.6.2 Retention period for archive

The retention period for archives is **30 years**.

4.6.3 Protection of archive

a) Electronic forms archives (stored in e.g. databases and/or tapes): the same protection as for audit log files applies (see section 4.5.4 of this CPS). All data are signed by the Certipost E-Trust PKI concerned elements. All the published data (in Certipost E-Trust Certificate Public Registry) are signed by the issuing CA. This ensures the authenticity and integrity of an electronic record in order to guarantee their authenticity and integrity towards ages. Only dedicated and authorised internal Certipost E-Trust staff members and /or duly (sub-)contracted authorized and qualified personnel are allowed to manipulate these files.

b) When Certipost E-Trust operates this task, the electronic communications are secured following PKIX-recommendations. Paper form transports are under the responsibility of Certipost E-Trust.

4.6.4 Archive backup procedures

The same procedure as for the previous points applies (see sections 4.5.5 and 4.6.3 of the present Q&N CPS).

4.6.5 Requirements for time-stamping of records

As these records are signed; they are time stamped, since all data signed by the PKI encompasses time information.

4.6.6 Archive collection system (internal or external)

Both are used.

4.6.7 Procedures to obtain and verify archive information

a) Normally all the data that is published (or that has been published), is available in the Certipost E-Trust Certificate Public Registry.

b) Depending on the policy used to enroll the Subscriber (e.g. copy of identity card), additional purely personal Subscribers' data or records of individual transactions may be released upon request by any of the entities involved in the transaction, or their authorised representatives. These data are stored in a separate database (not the Certipost E-Trust Certificate Public Registry) only accessible under very restricted conditions and in compliance with requirements regarding confidentiality and privacy stated in section 2.8. On a per case studied basis some information can be made accessible only to the Subscriber or the authorised people. A reasonable handling fee may be asked to cover the cost of record retrieval.

c) CA's shall make available on request, produced documentation of the CA's compliance with the applicable Q&N CPS according section 2.7 of this CPS.

d) The CA shall ensure availability of the archive and that archived information is stored in a readable format during its retention period.

4.7 Key changeover

4.7.1 CA keys

a) A new CA root key generation process is initiated. (see section 6.1.1 of the present Q&N CPS);

b) 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.

4.7.2 User keys

a) The Subscriber is automatically warned by e-mail one month before the end of the validity date of its certificate, provided his e-mail address is correctly communicated to Certipost E-Trust. A new Certificate is not automatically rebuilt from the previous data.

b) The user must request a new Certificate. It is imposed that a new Certificate also means a new pair of keys (rekey) as the validity period of the Certificate was introduced for security reasons.

c) If the user wants the same security level (Qualified, Normalised or Lightweight) as before, in case of face to face registration, he must :

- If neither the Certificate nor the Private Key has been compromised and are still valid : request a new certificate electronically following the procedure described in the applicable CP,
- Otherwise: presents himself again to verify that the information that is related to him is still valid.

4.7.3 Cross-certification keys

a) Cross-certified CA's, as any other users, are warned by Certipost E-Trust that a changeover occurs.

b) The same procedure has to be performed as for the initial cross-certification.

4.8 Compromise and Disaster Recovery

A detailed Contingency and Disaster Recovery Plan is ruling the operations described in the section 4.8 of the present Q&N CPS. This document is an internal confidential document.

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

a) The impacted PKI components are brought down and reset with new clean components (in case of key compromise, see related section of this Q&N CPS). After the problems and the resolution are analyzed, the disaster recovery site takes over from the main-one if it has not been impacted by the same compromise/disaster.

b) Users are warned by the most appropriate and reliable means and if necessary via press.

c) All Certificates issued during the compromise are revoked and then re-keyed.

4.8.2 Entity Public Key is revoked

Not applicable.

4.8.3 Entity key is compromised

4.8.3.1 E-Trust TOP Root CA, Primary CA(s) and Secondary CA(s) Keys

a) The key is immediately revoked according to section 4.4 of the present Q&N CPS.

b) All cross certificates issued for this CA, are revoked by the respective other CA's. The ARL's and CRL's are updated and published.

c) The CA production machine is deactivated.

d) An inquiry is performed in order to identify the cause of compromising and to exclude it from the new set-up.

e) A new CA key generation procedure occurs (see section 6.1.1 of this Q&N CPS).

f) As far as possible, all Certificates issued under this compromised CA are revoked.

g) Users are warned by the most appropriate and reliable means.

h) The appropriate measures as described in 4.8.1 apply.

4.8.3.2 Users' Keys

See section 4.4 of this Q&N CPS on revocation. If the Certificate is revoked due to Certipost E-Trust CA compromising or operator errors, Certipost E-Trust will provide, free of charge, a new equivalent Certificate to the user, based on a rekey procedure (see section 3.3). If the user reveals to be a defrauder, Certipost E-Trust reserves rights to terminate any contract with him.

In case the user key is compromised, the user is obliged to follow the applicable suspension and revocation procedures. The suspension and revocation procedure will be followed in accordance with section 4.4 of this Q&N CPS.

4.8.4 Secure facility after a natural or other type of disaster

In the event of any natural or other type of disaster, the disaster recovery site will take over from the main site.

4.8.5 Contingency and Disaster Recovery Plan

A detailed Contingency and Disaster Recovery Plan is ruling the operations described in the section 4.8 of the present Q&N CPS. This document is an internal confidential document.

4.9 CA Termination

a) Transfer of services from one organisation to another organisation, 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 E-Trust shall send notification to all Subscribers to ensure the continuous 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.
- Realise 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 Q&N CPS.
- Terminate all authorisations 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.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This section describes non-technical security controls used in the context of the completion of all tasks regarding the Certipost E-Trust Services. All the components of the Certipost E-Trust PKI are protected against unauthorised use.

5.1 Physical Controls

This concerns all the sites where the Certipost E-Trust PKI components from the Certipost E-Trust PKI are operated, including the CAs, CAOs, RAs, RAOs, LRAs, LRAOs, the Certipost E-Trust on-line request service, Certificate Public Registry and the Certipost E-Trust website.

5.1.1 Site location and construction

a) The following high level security sites are identified within the Certipost E-Trust PKI:

- PKI Security Rooms: In these rooms reside the services for the Certipost E-Trust TOP Root, Primary and Secondary CAs, the Certipost E-Trust on-line request, Certificate Public Registry, Online Revocation Status Service, and the Certipost E-Trust web site. These rooms have a very high level of security.
- Disaster Recovery PKI Security Rooms: these rooms are the back-up and disaster recovery sites for the PKI Security Rooms. The same very high level of security applies to this disaster recovery site.
- PKI Operations Management Rooms: In these rooms resides the overall management of all the other Certipost E-Trust services, as well as the Certipost E-Trust CRAO and the Certipost E-Trust SRAO service. These rooms have a high level of security.
- PKI LRAO Rooms: In these rooms reside the components for the Certipost E-Trust LRAO Services. These rooms have a level of security as contractually imposed on the LRA and/or LRAO's.

b) Furthermore, all documents and other items (like smart cards) that need to be stored securely are stored in burglary and fire resistant safes.

5.1.2 Physical access

a) The E-Trust CA's sites shall be regularly inspected to verify that the access control system is always operational and running.

b) For the PKI Security Rooms and the Disaster Recovery PKI Security Rooms, as defined in 5.1.1 : These areas are protected against unauthorised access by at least 3 perimeters protections. The first and the second consist, as the minimum, of a badge system and the third of a badge system combined with a biometrics authentication system, as a minimum. All accesses are logged. The access is furthermore only possible via a sas. The sas is composed of a double fireproof door and is burglary resistant. It allows access for only one person at a time.
Alarm systems, which can only be deactivated by PIN codes known only to the persons having access to these areas, protect against physical intrusion.

c) For the high level Security Rooms, other than the PKI Security Rooms and the PKI Disaster Recovery Security Rooms: these areas are protected against unauthorised access by at least 2 perimeter protections.

d) The Certipost E-Trust authorized staff members and/or the duly (sub-)contracted authorized and qualified personnel must follow the fully documented procedure to access the rooms. Each

Certipost E-Trust staff member and/or the duly (sub-)contracted authorized and qualified personnel as well as their respective backup are identified. The access rights to the various PKI locations are clearly identified for each Certipost E-Trust staff member and/or the duly (sub-)contracted authorized and qualified personnel and their backups. Giving access to a new Certipost E-Trust staff member and/or to a duly (sub-)contracted authorized and qualified personnel requires very strict verifications. The access right of a Certipost E-Trust staff member who quits Certipost or who is subject to a security-screening is immediately removed. The access rights of a duly (sub-)contracted authorized and qualified personnel who quits the (sub-)contracted legal entity or who is subject to a security-screening is immediately removed.

e) Detailed description of the protection of these areas and Access Control Security Policies are provided in internal documents.

5.1.3 Power and air conditioning

a) The power supply of the Certipost E-Trust PKI elements is protected against a main network power supply interruption.

b) An air conditioning system is installed to have a reliable operational environment. It is nevertheless implemented in such a way that it will not reduce the physical security to the room nor compromise the functioning of the hardware/software in case of its dysfunction.

5.1.4 Water exposures

This is namely addressed by the disaster recovery site.

5.1.5 Fire prevention and protection

Every wall and every door of the Certipost E-Trust Very High Level Security Rooms are fire protected.

5.1.6 Media storage

All the media are memorised and stored at one site and replicated in another site with the same degree of physical protection to be able, even in case of site disaster, to be fully available after a short time.

5.1.7 Waste disposal

Standard office waste are removed and destroyed on the standard Certipost procedure. Either dedicated closed trash boxes are used for confidential data for which the content is destroyed immediately when removed, or a paper destruction machine is used to destroy immediately any disposal including confidential data. All the other very high secure PKI components like access cards to hardware/software are physically destroyed.

5.1.8 Off-site backup

An advanced replication mechanism ensures that the electronic data from the PKI Security Room is automatically replicated to the Disaster Recovery PKI Security Room. Furthermore, servers and other appliances are installed and configured in exactly the same way as the back-up site (except for network settings). Additionally, procedures are in place to ensure that changes in software versions on the PKI Security Room are also applied in the Disaster Recovery PKI Security Room. Back-ups of smart cards of the operational components of the Certipost E-Trust PKI are located in safes in the Disaster Recovery PKI Security Room.

5.2 Procedural Controls

a) The various tasks to be accomplished in the Certipost E-Trust PKI are clearly defined in internal documents.

b) The Certipost E-Trust Staff Members are either employees of Certipost s.a./n.v., or authorized and qualified employees of sub-contractual entities or contracted LRAOs in accordance with section 1.3.3, and with the other applicable provisions of the present document.

5.2.1 Trusted roles

a) Following roles are identified as the trusted roles within the Certipost E-Trust PKI:

Security Officers: Persons who fulfill this role have an overall responsibility for administering the implementation of the security practices.

System Administrators: Persons who fulfill this role are authorized to install, configure and maintain the PKI trustworthy systems for support for registration, Certificate generation, Subscriber (secure) device provision and revocation management. They are authorized to perform system backup and recovery.

System Auditors: Persons who fulfill this role are authorized to view and maintain archives and audit logs of the PKI trustworthy systems.

Certification Authority Auditor (CAA): Persons who fulfill this role have the responsibility to perform the a posteriori audit and check of the correct and authorized issuing of the Certificates issued by the CA.

Central Registration Authority Operator (CRAO): Persons who fulfill this role have the responsibility to perform the central registration and issuing the approved Certificate request to the CA.

Local Registration Authority Operator (LRAO): Persons who fulfill this role have the responsibility to do the local registration and, dependant on the CP, issuing the approved Certificate request to the CA.

Suspension and Registration Authority Operator (SRAO): Persons, who fulfill this role, have the responsibility for the suspension, revocation and unsuspension of the Certificates.

Certipost E-Trust PKI Certification Practices Council: Persons, who fulfill this role, have the responsibilities, as described in section 1.3.1 and section 8 of this CPS.

b) The security roles and responsibilities and the occupancy of above roles are described in job descriptions and in internal fully documented procedures. The job descriptions are defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness, and differentiating between general functions and CA specific functions.

c) The occupancy of the roles is such that the possibility of fraud is minimised.

d) The administrative and management procedures and processes exercised by the trusted roles personnel are in line with the Certipost E-Trust information security management procedures.

e) Managerial personnel possess expertise in the electronic signature and information security technology and familiarity with security procedures for personnel with security responsibilities.

f) All personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations.

g) CA personnel are formally appointed to trusted roles by senior management responsible for security.

h) The CA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offense which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

5.2.2 Number of persons required per task

Each task may be carried out by at least two persons for availability reasons. Moreover, a CAA performs an additional check (a posteriori) on the issuing of each Certificate.

For certain sensitive tasks (e.g. Wedding Ceremony), several persons are required for security and dual control reasons.

5.2.3 Identification and authentication for each role

The identification and authentication for each role are determined in internal documents (e.g., job descriptions, contractual agreement).

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

a) The Certipost E-Trust Staff Members are either employees of Certipost s.a./n.v., or authorized and qualified employees of sub-contractual entities or contracted LRAOs in accordance with section 1.3.3, and with the other applicable provisions of the present document.

b) The Certipost E-Trust Staff Members are selected following an appropriate procedure as described in internal documents.

c) The Certipost E-Trust Staff Members have been assigned with a specific job function (see section 5.2.1) and have the required expert knowledge, experience and qualification for the offered services and as appropriate to their job function.

5.3.2 Background check procedures

Each Certipost E-Trust Staff Member must be background checked independently and individually. Certipost s.a./n.v. employees or any physical person who are not Certipost E-Trust Staff Members may have only a temporary access to the PKI-locations, must always be accompanied by at least one Certipost E-Trust Staff Member and must sign a non-disclosure agreement.

5.3.3 Training requirements

a) Following formal trainings and accreditations are necessary to fulfill the following trusted roles:

- LRAO training for LRAO operations
- CRAO training for CRAO operations
- SRAO training for SRAO operations

b) Only after having successfully followed this formal training and having signed a dedicated LRAO, CRAO or SRAO contract, one can fulfill the respective trusted role.

c) A training plan is included in the job description of each trusted role.

5.3.4 Retraining frequency and requirements

The retraining frequency and requirements are described in internal documents.

5.3.5 Job rotation frequency and sequence

The job rotation frequency and sequence are described in internal documents.

5.3.6 Sanctions for unauthorised actions

A Certipost E-Trust Staff Member who operates in violation of the policies and procedures stated here and in the PKI internal processes and procedures, whether through negligence or with malicious intent, will have his/hers privileges revoked and will be subject to administrative discipline and possibly criminal pursuit.

5.3.7 Contracting personnel requirements

Standard Certipost S.A. contract following the Belgian legislation plus a special Non Disclosure Agreement are used. For LRAOs or subcontracted employees, not employed by Certipost s.a./n.v., a formal contractual agreement, compliant with the applicable provisions stated in the present document, is signed between the LRAO and/or the legal company employing the LRAO or the trusted personnel and Certipost s.a./n.v. (E-Trust).

5.3.8 Documentation supplied to personnel

Each Certipost E-Trust Staff Member, any authorized and qualified employees of sub-contractual entities and any external LRAO accredited to serve a particular CP receives the appropriate documents defining the work to be done, including the procedure.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

Key pair generation concerns 2 different kinds of entities:

- The PKI management components included in the Certipost E-Trust PKI. The various components are the CA's, RA's and all other related software/hardware.
- The software/hardware at the Subscriber (end-user) side.

6.1.1 Key pair generation

6.1.1.1 PKI components key pair generation

a) CA (whether TOP Root, Primary or Secondary) key pair generation is ruled by a fully documented procedure called "Wedding ceremony" (internal confidential document).

b) For the Certipost E-Trust CAs' keys' generation, several CA Wedding Ceremony Security Officers must be present to enable the key generation process in a Hardware Security Module (HSM). 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, granted physical access controls to these CA Wedding Ceremony Security Officers is deactivated and can only be made active again by a specific written demand to the Certipost E-Trust PKI Certification Practices Council.

c) RA, SRA, CAA key generation is done by a Security Officer in the presence of the corresponding operator under dual control.

6.1.1.2 Subscriber key pair generation

a) If the Subscriber's key pair generation is done by the Certification Service Provider (e.g., at the (Local) RA), the Private Key is, only stored permanently on the user's pin and/or password protected storage media or SSCD, unless key escrow is applicable (see applicable section in the present document).

b) If key generation is done by the Subscriber and the Certificate request send to the CSP, Certipost E-Trust give no guarantee on the key generation. Minimal key size (for RSA) must be 1024 bits (e.g. for personal residential and enterprise usage) and 2048 for high security usage (e.g. military usage). The pass phrase protecting the Private Key is strictly personal and must never be written down; its minimal size should be 8 alphanumerical characters. The Private Key should never be stored on a shared hard disk. The minimum acceptable solution for storing the Private Key is a floppy disk or a hard disk, but the best solution remains a SSCD (e.g. smart card).

c) See specific CP for more details and requirements regarding the usage of SSCD and the key generation by the CSP or by the Subscriber.

6.1.2 Private Key delivery to entity

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

- Floppy-disk: The Private Key shall be stored in an encrypted way using a pass phrase of at least 8 characters.
- SSCD: This provides a higher security level with higher reliability. The SSCD access shall be PIN protected.

b) CA provided subscriber key management services: The CA shall ensure that any subscriber keys, that it generates, are generated securely and the privacy of the subscriber's private key is assured.

c) Certificate generation

- If the CA generates the subscriber keys:
  - CA-generated Subscriber keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures.
  - CA-generated Subscriber keys shall be of a key length and for use with a public key algorithm which is recognized as being fit for the purposes of Qualified Electronic signatures.
  - CA-generated Subscriber keys shall be generated and stored securely before delivery to the Subscriber.
  - The Subscriber's private key shall be delivered to the subscriber in a manner such that the privacy of the key is not compromised and on delivery only the Subscriber has access to its Private Key.

d) Secure Signature Creation Device (SSCD) preparation

- The CA shall ensure that if it issues SSCD this is carried out securely.
- In particular, if the CA issues a SSCD:
  - secure-signature-creation device preparation shall be securely controlled by the service provider;
  - secure-signature-creation device shall be securely stored and distributed;
  - secure-signature-creation device deactivation and reactivation shall be securely controlled;
  - where the secure-signature device 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.

6.1.3 Public Key delivery to Certificate Issuer

Three (3) types of Certificate requests are possible; all based on PKCS#10 requests in DER or PEM format. These requests are signed by the corresponding Private Key and verified by the CSP:

- A floppy-disk at the LRA.
- 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 electronic rekey possibility (see section 3.2 of the present Q&N CPS) and when authorized in the applicable CP.

6.1.4 CA Public Key delivery to users

The CA Public Keys are published on the Certipost E-Trust Certificate Public Registry and Certipost E-Trust Web-site. This information is also available on simple request to info@e-trust.be or by a verification of the hash by telephone (see section 8 for contact details of Certipost E-Trust).

6.1.5 Key sizes

- All CA Certificates have a key size (RSA) of 2048 bits. The key size of other PKI components in the Certipost E-Trust PKI is of minimum 1024 bits.
- Minimum accepted Subscriber key size is (RSA) 1024 bits.

6.1.6 Public Key parameters generation

a) For all the Certipost E-Trust applications, Public Key RSA exponents are chosen secure (e.g. Fermat 4).

b) The Public Key module generation is done with state of the art parameter generation technology (e.g. Blum Blum Shub)

6.1.7 Parameter quality checking

Parameter generation is implemented using state of the art technology and shall be regularly re-evaluated regarding new advances in cryptology.

6.1.8 Hardware/software key generation

CA components of the Certipost E-Trust 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 clear. HSM devices used by Certipost E-Trust are FIPS 140-1 level 3.

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

6.1.9.1 PKI components Public Key

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.

6.1.9.2 Subscriber's Public Key

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.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

a) The HSM's that are used by the CA components of the Certipost E-Trust Qualified and Normalised PKI segment are FIPS 140-1 Level 3.

The signing engines are based on the FIPS 140-1 Level 3 compliant devices. Thanks to its design, the device can 'virtually' host an unlimited number of signing key pairs (roots) per device. A strong encryption key that is split-up over smart cards that are protected with multiple pass phrases (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. Multiple engines can host identical roots in order to cope with high availability and scalability. The signing engine supports for public key ciphers RSA (tested up to 16.384 bit keys, performing at least up to 100 signature / second) and DSA.
Each engine hosts (depending on the configuration) three sub engines: the certificate, the CRL and the OCSP engine. All three perform signing operations, however on different data structures and according to different policies.

b) Recommended cryptographic modules for user are SSCD. See appropriate CP for more details on requirements for SSCD usage.

6.2.2 Private Key multi-person control

The Private Keys of the Certipost E-Trust 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 pass phrases (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.

For the other Certipost E-Trust components, one double passphrase protected smartcard is required.

6.2.3 Private Key escrow

a) PKI components: The Private Keys of the Certipost E-Trust CA's are never exported under unencrypted form from the HSM, holding the Private Keys of Certipost E-Trust CA's.

b) Subscriber's Private Keys are never escrowed unless otherwise stated in the applicable CP. However only encryption private keys are eligible for Key escrow.

6.2.4 Private Key backup

a) PKI components: At the same time of generating the Private Keys of the Certipost E-Trust CA's in the HSM, the Private Keys, encrypted by the SMK, are exported on smartcards. Thereafter, the Private Keys, encrypted by the SMK, are imported in a HSM, which is located in the Disaster Recovery Secure PKI Room.

b) Subscriber's Private Keys: There is no backup in the Certipost E-Trust infrastructure of the Private Key of the Subscribers.

6.2.5 Private Key archival

This is described in internal documents.

6.2.6 Private Key entry into cryptographic module

In case the Private Key has to be put in the HSM again or in a new HSM, several components have to be used (see section 6.2.2 and 6.2.3 of this Q&N CPS).

6.2.7 Method of activating Private Key

The Private Keys of the Certipost E-Trust CA's are activated, using 3 passphrases protected smartcards, hold by 3 different security officers.

Additionally, two double-passphrase protected smartcards, hold by 3 different Security Officers, are needed, as well as a PIN code to access the HSM for starting the Certipost E-Trust CA softwares.

6.2.8 Method of deactivating Private Key

The Private Keys can be deactivated at least in the following cases:

- When the software, accessing the Certipost E-Trust CA Keys, is shut downed by a Security Officer.
- When the HSM is manually stopped by a Security Officer.
- When the HSM detects a physical breach
- When the HSM is operated outside the standard temperature range

- When there is a power failure.

6.2.9 Method of destroying Private Key

a) The Private Keys of the Certipost E-Trust CA's are destroyed when the HSM detects a physical breach, the HSM is operated outside the standard temperature range, or when there is a power failure.

b) The Private Keys of the Certipost E-Trust CA's can be destroyed by the Security Officers by destroying the HSM, the back-up HSM and the smartcards, containing the SMK and the Private Keys, encrypted by the SMK.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key archival

Public Keys stored in the internal CA database are archived for a period of 30 years. As Certipost E-Trust Certificate Public Registry retains all Certificates, it stores also the corresponding Public Keys.

6.3.2 Usage periods for the Public and Private Keys

a) PKI components

- TOP Root CA: The validity period is twenty (20) years.
- Primary CAs: The validity period is fifteen (15) years.
- Secondary CAs: The validity period of the key for the issuing of end-entity Certificates is ten (10) years.

b) The validity period of the user key is CP dependent.

c) Public Keys must always be retrievable after the expiration date of the corresponding Certificate in order to be able to verify Digital Signatures applied before this expiration date.

6.4 Activation Data

6.4.1 Activation data generation and installation

a) PKI components: Activation data refers to the combination of PIN and pass phrase to access all the Certipost E-Trust PKI components via smart cards, or HSM.

b) Subscriber's activation data: PIN code is minimum required.

6.4.2 Activation data protection

a) *PKI components:* The passphrase PIN should never be stored nor written somewhere. A second backup is usable as well for hardware failure as for a passphrase that has been forgotten. The pass phrases may not be shared.

b) *Subscriber:* In accordance with the present CPS and with the applicable CP, the Certificate Holder shall protect the Private Key at all times against loss, disclosure, alteration or unauthorized use. Once the private and public key pair has been created, the Certificate Holder shall be personally responsible for maintaining the key pair's integrity and confidentiality. The Certificate Holder shall be deemed the sole user of the Private Key. The PIN code (Personal Identity Number) or the password, employed for preventing unauthorized use of the Private Key, shall never be stored in the same place as the Private Key itself, nor alongside its storage medium. Nor shall it be stored without

protection: it shall always be adequately protected. The Certificate Holder shall never leave his Private Key unsupervised when it is not locked (e.g., leave it unsupervised in a work station when the PIN code or password has been entered). The Certificate Holder shall have sole liability for the use of his Private Key; the CSP shall not liable for the use made of the key pair belonging to the Certificate Holder.

6.4.3 Other aspects of activation data

It is recommended to change the pass phrases every month to diminish the probability for it being compromised.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

a) All Certipost E-Trust PKI computer components are configured in a maximum self-protecting mode. For each type of operating system check list procedures apply to regularly verify the conformance to such criteria.

b) Certipost E-Trust will do all its best to guarantee the highest possible level of security of its PKI infrastructure.

c) Penetration tests are regularly carried-out on the Certipost E-Trust PKI computers to check any flaws and problems in the security.

6.5.2 Computer security rating

This information is described in Certipost E-Trust internal documents.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

a) The development is carried out in a controlled secure environment requiring a high level of clearance.

b) Methods and software are first tested within the Certipost E-Trust PKI Testing Environment before being used in the Certipost E-Trust PKI production environment. Change management and configuration management follow the operational procedures commonly used within Certipost E-Trust PKI. Both change and configuration management ultimately are the responsibility of the members of the Certipost E-Trust PKI Certification Practices Council.

c) Production and development environments are totally uncoupled.

6.6.2 Security management controls

Configuration, integrity and penetration tests are regularly carried-out on the Certipost E-Trust PKI computers to check any flaws and problems in the security.

6.6.3 Life cycle security ratings

Internal Certipost procedures will be strictly followed.

6.7 Network Security Controls

The Certipost E-Trust Network uses the state of the art firewall technology, as well as intrusion detection technology.

6.8 Cryptographic Module Engineering Controls

The HSM's containing the Certipost E-Trust CA's Private Keys, are FIPS 140-1 level 3.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

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

b) Inclusion of data elements in Certificates shall be consistent with this Q&N CPS and the applicable CP.

c) Content of the Certificates are given in the applicable CP's.

7.1.1 Version number(s)

Certificates issued under this CPS are X.509 version 3 Certificates. The version field of the Certificates issued under this CPS shall then be set to 2, indicating that the version is v3.

7.1.2 Certificate extensions

7.1.2.1 CA Certificate extensions

The following profile is provided as an example for a Root-signed CA (either Primary or Secondary) and is similar for the TOP Root CA.

Attribute	Field	IN [3]	CR [4]	PO [5]	CO [6]	Value
Extensions						
Authority Properties						
issuerAltName						
	Rfc822Name					
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of Certipost E-Trust issuing CA public Key (either TOP Root or Primary CA)
	authorityCertIssuer					
	authorityCertSerialNumber					
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.e-trust.be/<issuing CA name>.crl
	nameRelativeToCRLIssuer					
	cRLIssuer					
Subject Properties						
subjectAltName						
	Rfc822Name					
subjectKeyIdentifier						
	keyIdentifier	✓				SHA-1 Hash of Certipost E-Trust certified CA public Key
Policy Properties						

[3] IN = Included: Attribute / field included within the certificate profile.
[4] CR = Critical extension.
[5] PO = Policy: content to be supplied via the Certificate Signing Request (O = Optional, M = Mandatory).
[6] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

KeyUsage		✓	True			As defined in section 6.1.9.1.
	digitalSignature					True
	nonRepudiation					True
	keyEncipherment					
	dataEncipherment					
	keyAgreement					
	keyCertSign	✓				
	crlSign	✓				
	encipherOnly					
	decipherOnly					
CertificatePolicies						
	PolicyIdentifier	✓			S	0.3.2062.7.1.0.1.2.0
	policyQualifierID	✓			S	CPS
	qualifier	✓			S	http://www.e-trust.be/CPS/QNcerts
	policyQualifierID					
	noticeNumbers					
	DisplayText					
BasicConstraints		✓	True			
	cA	✓				True
	pathLenConstraint	✓				Primary: None (-1) Secondary: pathlength=0
NetscapeCertificateType						
	SSL Client					
	SSL Server					
	S/MIME					
	Object Signing					
	Reserved					
	SSL CA	✓				True
	S/MIME CA	✓				True
	Object Signing CA	✓				True

7.1.2.2 End-entities Certificate extensions

The following end-entities Certificate extensions profile is provided as an example for end-entity Certificate issued by Secondary CA:

Attribute	Field	IN [7]	CR [8]	PO [9]	CO [10]	Value
Extensions						
Authority Properties						
issuerAltName						
	Rfc822Name					*Not used*
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the Certipost E-Trust Secondary issuing CA
authorityInfoAccess						
	AccessMethod	✓				Id-ad-2 (Certification Authority Issuer (1.3.6.1.5.5.7.48.2))
	accessLocation	✓				http://ca.e-trust.be/<issuing CA nickname>.crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	

[7] IN = Included: Attribute / field included within the certificate profile.
[8] CR = Critical extension.
[9] PO = Policy: content to be supplied via the Certificate Signing Request (O = Optional, M = Mandatory).
[10] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

	fullName	✓				"http://crl.e-trust.be/<issuing CA nickname.crl"
	nameRelativeToCRLIssuer					Not used
	cRLIssuer					Not used
Subject Properties						
subjectAltName						
	Rfc822Name	✓		M	D	Certificate Holder's email address

subjectKeyIdentifier						
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature					**Qualified Certificates**: nonRepudiation and digitalSignature. **Normalised & Lightweight Certificates**: as defined in the corresponding CP (usually a combination of digitalSignature, keyEncipherment, and dataEncipherment).
	nonRepudiation					
	keyEncipherment					
	dataEncipherment					
	keyAgreement					
	keyCertSign					
	crlSign					
	encipherOnly					
	decipherOnly					

certificatePolicies		✓				
	PolicyIdentifier	✓			S	As defined in section 1.2.2. (Certipost OID)
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	http:// www.e-trust.be/CPS/QNCerts
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓			S	As defined in the corresponding CP. Example: "E-Trust Certificate Policy for Qualified Certificates for Physical Persons. Supported by SSCD, Key Generation by CSP. GTC, CP and CPS: www.e-trust.be/CPS/QNCerts"
	PolicyIdentifier	✓			S	As defined in section 1.2.2. (ETSI OID)
QualifiedCertificateStat						
	QcCompliance	✓		M		*QcCompliance oid*
	QcLimitValue					Not used
	QCRetentionPeriod					Not used

Netscape Proprietary						
NetscapeCertificateType						Not used unless specified in applicable CP
	SSL Client					
	SSL Server					
	S/MIME					
	Object Signing					
	Reserved					
	SSL CA					
	S/MIME CA					
	Object Signing CA					

7.1.3 Signature algorithm object identifiers

Certificates under this CPS will use the following OIDs for signatures:

OID = "1.2.840.113549.1.1.5" - SHA-1 with RSA Encryption.

7.1.4 Use of name fields

See subsection 3.1.1of this Q&N CPS.

7.1.5 Name constraints

Certipost E-Trust will fully follow the structure described in the X.500 standards. No name constraints are used, unless explicitly stated by the corresponding CP.

7.1.6 Certificate policy Object Identifier

See section 1.2.2 of the present Q&N CPS.

7.1.7 Usage of Policy Constraints extension

No Policy Constraints extensions are used.

7.1.8 Policy qualifiers syntax and semantics

Not applicable.

7.1.9 Processing semantics for the critical Certificate policy extension

Not applicable.

7.2 CRL Profile

7.2.1 Version number(s)

a) The CA will support X.509 version 2 CRL's, retrievable by LDAP on the Certipost E-Trust Certificate Public Registry.

b) As an alternative to CRL's the CA may provide Web based or "other" revocation checking service.

7.2.2 CRL and CRL entry extensions populated and their criticality

a) authorityKeyIdentifier: non critical. See also section 7.1.2 for the values of this extension.

b) cRLNumber: non critical.

c) reasonCode: non critical.

8 SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

a) The only changes that Certipost E-Trust Services 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 1.4 of this Q&N 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 E-Trust PKI Certification Practices Council shall accept, modify or reject the proposed change after completion of the review period.

d) All CPS changes under consideration by the Certipost E-Trust PKI Certification Practices Council shall be disseminated to interested parties (see section 8.2 of this Q&N CPS) for a period of minimum 14 days. Proposed changes to the present Q&N CPS will be disseminated to interested parties by publishing the new document on the http://www.e-trust.be/CPS/QNcerts web site. The date of publication and the effective date are indicated on the title page of the Q&N CPS. The effective date will be at least 14 days later then the date of publication.

e) All changes to the Q&N CPS or CP, other then editorial or typographical corrections, or changes to the contact details, will be subject to a new Object Identifier for the Q&N CPS or CP.

8.2 Publication and notification policies

8.2.1 Items not published in the CPS

Not applicable.

8.2.2 Distribution of Certificate Policy definition and CPS

The only valid current version of the Certipost E-Trust Q&N CPS, the corresponding CP's, general conditions and purchase orders are the one that are published by the Certipost E-Trust PKI Certification Practices Council on http://www.e-trust.be/CPS/QNcerts . The only valid previous versions of these documents are published by the Certipost E-Trust PKI Certificate Practices Council on http://www.e-trust.be/CPS/QNcerts

8.3 CPS approval procedures

Certipost E-Trust PKI Certification Practices Council is responsible for CPS approval.