VALIDITY: 12/09/2003-03/11/2004

Belgacom E-Trust Services

Certification Practice Statement for Qualified & Normalised Certificates

OUTDATED

O.I.D. 0.3.2062.9.6.0.2.2.1

Version 2.1

Start date of application : September 2003

OUTDATED

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	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.
Belgacom or Belgacom E-Trust	Belgacom SA/NV of public law, with registered offices in 1030 Brussels, Bd. du Roi Albert II, 27.
Belgacom E-Trust Infrastructure	The Belgacom Public Key Infrastructure that is deployed by Belgacom to provide the Belgacom E-Trust Certification Services.
Belgacom E-Trust PKI Certification Practices Council	The Policy Authority within Belgacom E-Trust is called the Belgacom E-Trust PKI Certification Practices Council (BEC). It is the high level management body with final authority and responsibility for – Specifying and approving the Belgacom E-Trust infrastructure and practices. – Approving the Belgacom E-Trust Certification Practice Statement(s) and Belgacom 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.
Belgacom E-Trust Services	The Belgacom Certification services.
Belgacom E-Trust Enterprise Program	This program consists in providing corporate customers with a dedicated *Belgacom E-Trust sub-Infrastructure*. This will imply usually the set up of an Enterprise CA and subordinate RA.
Electronic Signature	Electronic data, attached or logically linked to other electronic data and enabling authentication method.
Belgacom 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 Belgacom E-Trust Services.
Belgacom E-Trust Certificate Public Registry	The electronic registry used by Belgacom E-Trust Services to publish the issued Certificates and Certificate Revocation Lists.
Belgacom E-Trust Services Root CA	The Belgacom E-Trust Root CA is the original Certificate and his infrastructure. It is only able to issue Certificate(s) of subordinate E-Trust Primary CA's and E-Trust Enterprise Program CA's.
Certificate	An electronic statement that maps the signature verification data to a physical or moral person and confirms the identity of this person.
Certificate Holder	A physical or moral person 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. [ABA]
Certificate Public Registry	The repository that hold the publicly available certificates, CRL's and ARL's, issued by the Belgacom E-Trust Primary and Root Qualified and Normalised 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 Belgacom 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 authority 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.
European Directive(The)	The European Directive 1999/93/CE of the European Parliament and the Council of 13 December 1999 ***"on a community framework for electronic signature".***
Normalised Certificate	A Certificate that is 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. A Normalised Certificate is issued according to the requirements of the ETSI technical standard TS 102 042.
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, such as, 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 European Directive and is delivered by a Certification Service Provider that satisfies to the Annex II of The European Directive, and by referencing The 09 July 2001 Law, the technical standard ETS TS 101 456, the technical standard ETSI TS 101 862 ***"Qualified Certificate profile"*** and the RFC 3039 ***"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.
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 whose identity and Public Key is certified in a Public Key Certificate.
Subscriber	An entity that requests a Certificate 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
BEC	Belgacom 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
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
URL	Uniform Resource Locator


OUTDATED

STRUCTURE AND INTERPRETATION OF BELGACOM 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: Belgacom E-Trust Q&N CPS v1.0, 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 fulfil all requirements in this Q&N CPS. When a section is marked with "Not applicable", it means that this section is not applicable to Belgacom E-Trust Services Q&N CPS.

e) Belgacom E-Trust present the current Q&N CPS in such a structure that allows Belgacom 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 Belgacom E-Trust Q&N CSP will issue Certificates under the Qualified and Normalised labels.

1. INTRODUCTION

1.1 Overview

The Belgacom 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 Belgacom E-Trust Infrastructure (hereinafter referred to as: "CA's") employ in issuing Qualified digital Certificates or Normalised digital Certificates.

CA's within the Belgacom E-Trust Qualified & Normalised Infrastructure 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 Belgacom 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 uses the CP in order to determine the level of trustworthiness of the offered Certificate.

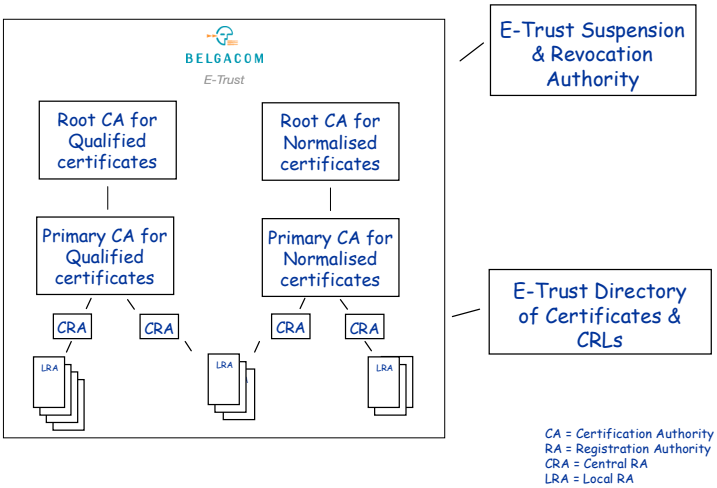
The following sub-section describes the Belgacom E-Trust Qualified & Normalised PKI segment from the complete Belgacom E-Trust PKI.

1.1.1 Belgacom E-Trust Qualified & Normalised CA hierarchy

Belgacom E-Trust has a Qualified & Normalised CA hierarchy beginning at the top level with two Root CAs, one for Qualified Certificates and the second for the Normalised Certificates, issuing only Sub-CAs' Certificates, respectively for Qualified Certificates and for Normalised Certificates. This infrastructure is consistent with the PKIX / X.509 standard.

The following figure depicts the current Belgacom E-Trust Qualified & Normalised PKI segment:

Belgacom E-Trust PKI segment for Qualified and Normalised Certificates



1.1.1.1 Belgacom E-Trust Root CA for Qualified Certificates

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

Subject: C=be O=Belgacom CN=Belgacom E-Trust Root CA for Qualified Certificates	Issuer: C=be O=Belgacom CN=Belgacom E-Trust Root CA for Qualified Certificates
Valid from : Fri Aug 10 10:34:46 GMT+02:00 2001 Valid to : Tue Aug 10 09:34:46 GMT+02:00 2021	
Serial number: 3B739C9D	
Thumbprint (SHA-1): 939A AC10 8CF2 5537 1F48 9062 A97C EC64 7DA3 0FE6	

The Belgacom E-Trust Root CA for Qualified Certificates issues only Sub-CAs' Certificates for CAs that are eligible to issue Qualified Certificates in the sense of the European Directive and the 9 July 2001 Law, and in the sense of the ETSI technical standard TS 101 456.

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

For the moment, as shown on the figure above, there is only one Sub-CA (Belgacom E-Trust Primary CA for Qualified Certificates) issuing all end-users Qualified Certificates.

1.1.1.2 Belgacom E-Trust Primary CA for Qualified Certificates

The Belgacom E-Trust Primary CA for Qualified Certificates issues only Qualified Certificates in the sense of the European Directive and the 9 July 2001 Law, and in the sense of the ETSI technical standard TS 101 456.

Subject: C=be O=Belgacom CN=Belgacom E-Trust Primary CA for Qualified Certificates	Issuer: C=be O=Belgacom CN=Belgacom E-Trust Root CA for Qualified Certificates
Valid from: Mon Nov 05 14:07:53 GMT+01:00 2001 Valid to: Fri Nov 05 14:07:53 GMT+01:00 2010	
Serial Number: 3BE68F29	
Thumbprint (SHA-1): C88E C9DE DED8 381D B4F0 AED0 DAF3 B0BD 894B C921	

1.1.1.3 Belgacom E-Trust Root CA for Normalised Certificates

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

Subject: C=be O=Belgacom CN=Belgacom E-Trust Root CA for Normalised Certificates	Issuer: C=be O=Belgacom CN=Belgacom E-Trust Root CA for Normalised Certificates
Valid from: Mon Nov 05 16:29:02 GMT+01:00 2001 Valid to: Fri Nov 05 16:29:02 GMT+01:00 2021	
Serial number: 3BE6B035	
Thumbprint (SHA-1): BF1C FE00 D9D6 CD98 8829 FFCA 6D2A 9850 92C0 177B	

The Belgacom E-Trust Root CA for Normalised Certificates issues only Sub-CAs' Certificates for CAs that are eligible to issue Normalised Certificates in the sense of the ETSI technical standard TS 102 042.

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

For the moment, as shown on the figure, there is only one Sub-CA (Belgacom E-Trust Primary CA for Normalised Certificates) issuing all end-users Normalised Certificates.

1.1.1.4 Belgacom E-Trust Primary CA for Normalised Certificates

The Belgacom E-Trust Primary CA for Normalised Certificates issues only Normalised Certificates in the sense of the ETSI technical standard TS 102 042.

Subject: C=be O=Belgacom CN=Belgacom E-Trust Primary CA for Normalised Certificates	Issuer: C=be O=Belgacom CN=Belgacom E-Trust Root CA for Normalised Certificates
Valid from: Tue Nov 06 10:44:58 GMT+01:00 2001 Valid to: Sat Nov 06 10:44:58 GMT+01:00 2010	
Serial number: 3BE7B11A	
Thumbprint (SHA-1): 7F62 0A1A FCCD 71BC 0177 C4B8 CD3D 7606 F1E1 94FA	

1.2 Identification

1.2.1 Identifiers for Certification Practice Statement

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

Certification Practice Statement Name:

BelgacomETrustCertificationPracticeStatementForQualifiedAndNormalisedCertificateVersion1:0

Object Identifier:

0.3.2062.9.BelgacomE-Trust(6).CPS(0).QNCPS(2).Version(2).Sub-version(1)

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 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 Belgacom E-Trust to rule the issuing of Qualified or Normalised 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

A Certificate policy for Qualified Certificate 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 Certificate Policies

Identifiers for Normalised 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)

1.2.2.3 Current Belgacom E-Trust Qualified & Normalised Certificates Policies

The current Certificate Policies used by Belgacom E-Trust to rule the issuing of Qualified or Normalised digital Certificates are described in the next three subsections. The first subsection describes the CP used to rule the issuing of digital Qualified or Normalised certificates to lawyers from the "Ordre français des avocats du barreau de Bruxelles", the Brussels Bar Association. While the second subsection describes the CP used to rule the issuing of digital Qualified or Normalised Certificates to the public. The third subsection described the CP used to rule the issuing of digital Qualified or Normalised digital Certificates for the FRNB (Fédération Royale du Notariat Belge)

1.2.2.3.1 Lawyer's Qualified or Normalised Digital Certificate Policy

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 or while acting as a lawyer. 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 lawyer, subject of the Certificate.

The validation of the request will demand the provision of the proof of the identity of the applicant Lawyer and the verification of the pieces guaranteeing his lawyer'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 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 TO1 456 ; 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 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 Qualified Digital 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.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 "Belgacom E-Trust Qualified of Normalised Digital Certificates" Certificate Policies :

- Obligation for the Lawyer applying to be a Certificate owner to visit a Local Registration Authority (LRA) certified and trained by Belgacom E-Trust and the « Ordre français des avocats du barreau de Bruxelles » (OFBB).
- Obligation for the Lawyer applying to be a Certificate owner to provide Belgacom E-Trust, via the certified LRA, the additional identification proofs as required in the CP and related to his quality of Lawyer.
- Allowed ability for the OFBB, via the certified LRAs, to be involved in the revocation/suspension process.

The Lawyer's Qualified or Normalised CP is a global CP encompassing several certificate policies whose identifiers are provided in the following Table 1.

Lawyer's Qualified Certificate for Qualified Digital Signature Only		Lawyer's Normalised Certificate	
	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key Generation by Owner : **0.3.2062.9.6.1.15.2.x**		Normalised Certificate without SSCD **0.4.0.2042.1.1** and Key Generation by Owner: **0.3.2062.9.6.1.15.6.x**
Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Key Generation by CSP: **0.3.2062.9.6.1.15.3.x**	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key Generation by CSP: **0.3.2062.9.6.1.15.4.x**	Normalised Certificate with SSCD **0.4.0.2042.1.2** and Key Generation by CSP : **0.3.2062.9.6.1.15.7.x**	Normalised Certificate without SSCD **0.4.0.2042.1.1** and Key Generation by CSP : **0.3.2062.9.6.1.15.8.x**

Table 1. Identification of the "Lawyer's Qualified or Normalised Certificate Policy"

(CSP = Certification Service Provider; x= version number)

1.2.2.3.2 Belgacom E-Trust Qualified or Normalised Digital Certificates

This type of digital Certificates provides a very high degree of assurance of the Certificate holder's personal (physical or legal person) 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. This Certificate provides a strong guarantee of the link between either the personal identity of the Certificate holder (physical person), any professional status (not obligatory), the Public Key and its authorized use, or the identity of the Certificate holder (legal person), 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 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 101 456 ; 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 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 (see Section D1.5 of this document).

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 Qualified Digital Signature operations or

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. Certificates issued under this general CP for CSP Qualified or Normalised Certificates include one or more CP identifiers. These can be used by third parties to determine the applicability and trustworthiness of a Certificate for a particular application.

The Certificates issued under the applicable CP are to be considered as "issued to public" Certificates.

The identifiers for the Certificate Policies for Belgacom E-Trust Qualified or Normalised Certificates set out in this document are listed in Table 2 (physical person), Table 2bis (legal persons), and Table 2ter (physical person in the context of Certipost application) below.

Belagcom E-Trust Qualified Certificate for Qualified Signature Only		Belgacom E-Trust Normalised Certificate	
	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by owner : **0.3.2062.9.6.1.19.2.x**		Normalised Certificate without SSCD **0.4.0.2042.1.1** and Key generation by owner : **0.3.2062.9.6.1.19.6.x**
Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Key generation by CSP: **0.3.2062.9.6.1.19.3.x**	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by CSP: **0.3.2062.9.6.1.19.4.x**	Normalised Certificate with SSCD **0.4.0.2042.1.2** and Key generation by CSP: **0.3.2062.9.6.1.19.7.x**	Normalised Certificate without SSCD **0.4.0.2042.1.1** and Key generation by CSP: **0.3.2062.9.6.1.19.8.x**

Table 2. Identification of the Belgacom E-Trust Qualified or Normalised CP

(CSP = Certification Service Provider; x= version number)

Belgacom E-Trust Qualified Certificate For Legal Persons (for Qualified Signature Only)	
	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key Generation by owner: **0.3.2062.9.6.1.25.2.x**
Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Key Generation by CSP: **0.3.2062.9.6.1.25.3.x**	Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key Generation by CSP : **0.3.2062.9.6.1.25.4.x**

Belgacom E-Trust Normalised Certificate For Legal Persons	
	Qualified Certificate without SSCD (OID ETSI 102 042) **0.4.0.2042.1.1** and Key Generation by owner : **0.3.2062.9.6.1.25.6.x**
Qualified Certificate with SSCD (OID ETSI 102 042) **0.4.0.2042.1.2** and Key Generation by CSP : **0.3.2062.9.6.1.25.7.x**	Qualified Certificate without SSCD (OID ETSI 102 042) **0.4.0.2042.1.1** and Key Generation by CSP : **0.3.2062.9.6.1.25.8.x**

Tableau 2bis. Identification of the Belgacom E-Trust Qualified or Normalised CP for Legal persons (CSP = Certification Service Provider, x = version number).

Belgacom E-Trust Qualified Certificate
For Qualified Signature only, and in the context of the Certipost application

Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key Generation by the owner: **0.3.2062.9.6.1.23.2.x**

Tableau 2ter. Identification of the Belgacom E-Trust Qualified Certificate in the context of the Certipost application (x = version number)

1.2.2.3.3 FRNB Qualified or Normalised Digital Certificate Policy

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 or while acting as a notary, a candidate notary or a collaborator of the Notary. 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 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 101 456 ; 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 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.

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).

1.3 Community and Applicability

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

The applicability of the Certificates issued by CA's in accordance with this Q&N CPS will be documented in the associated 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 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 Authorities

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

- Specifying and approving the Belgacom E-Trust infrastructure and practices.
- Approving the Belgacom E-Trust Certification Practice Statement(s) and Belgacom 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

b) Policies ruling the membership, the management and the task of the Belgacom 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 Belgacom E-Trust Q&N CPS, the following Certification Authorities can be distinguished within the Belgacom E-Trust Qualified and Normalised PKI segment.

- *Belgacom E-Trust Root CA for Qualified Certificates*

The Belgacom E-Trust Root CA issues the Certificate(s) of the subordinate Belgacom E-Trust Primary CA for Qualified Certificates.

- *Belgacom E-Trust Primary CA for Qualified Certificates*

The Belgacom E-Trust Primary CA for Qualified Certificates may issue Qualified Certificates that are identified in the related Belgacom Qualified CP's.

- *Belgacom E-Trust Root CA for Normalised Certificates*

The Belgacom E-Trust Root CA for Normalised Certificates issues the Certificate(s) of the subordinate E-Trust Primary CA for Normalised Certificates.

- *Belgacom E-Trust Primary CA for Normalised Certificates*

The Belgacom E-Trust Primary CA for Normalised Certificates may issue Normalised Certificates that are identified in the related Belgacom Normalised CP's.

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

c) The Belgacom E-Trust Primary CA for Qualified Certificates 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 Primary Qualified CA is provided above (see section 1.2.2). Every Certificate type is ruled by a specific Belgacom E-Trust Certificate Policy (CP) document.

d) The Belgacom E-Trust Primary CA for Normalised Certificates 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 Primary Normalised CA is provided above (see section 1.2.2). Every Certificate type is ruled by a specific Belgacom E-Trust Certificate Policy (CP) document.

e) A specific CP will govern the delivery conditions, the usage and the applicability rules and guidelines for each Certificate that is issued under this Belgacom 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.

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

g) Belgacom E-Trust reserves right to set-up additional E-Trust Primary CA's in accordance with the

current Belgacom 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 Belgacom E-Trust Qualified and Normalised PKI segment.

- *Belgacom E-Trust Central RA,*
- *Belgacom E-Trust authorised Local RAs as specified in the applicable CP and as ruled by formal contractual agreement between Belgacom E-Trust and the concerned legal entity acting as Local RA,*
- *OFBB Local RA and Lawyers member of OFBB acting as Local RA as specified in the applicable CP and as ruled by formal contractual agreement between Belgacom E-Trust and the concerned legal entity acting as Local RA.*
- *FRNB Local RA's as specified in the applicable CP and as ruled by formal contractual agreement between Belgacom E-Trust and the concerned legal entity acting as Local RA.*

b) Any Registration Authority which operates within the Belgacom E-Trust Qualified and Normalised PKI segment 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 Belgacom E-Trust CAs, this approval shall be obtained from the Belgacom 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 or Normalised Certificate under the Belgacom 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 Digital Signatures. Any usage different from creating Qualified Digital Signature is at the own risk and responsibility of the Subscriber and/or the relying party. For Normalised 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 Belgacom E-Trust Qualified and Normalised 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.

Belgacom E-Trust Qualified and Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Qualified Certificate without SSCD (0.4.0.1456.1.2) and Key Generation by Owner (0.3.2062.9.6.1.19.2.x)	Qualified 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.	Electronic personal or professional identity **for legal value digital signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage** : As indicated by Subscriber. **Limit on transaction value**: As indicated by Subscriber.
E-Trust Qualified Certificate with SSCD (0.4.0.1456.1.1) and Key Generation by CSP (0.3.2062.9.6.1.19.3.x)	Qualified Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Legal Qualified Signatures (according to art. 4, §4 of the 09 July 2001 Law and art. 5.1 from The European Directive).	Electronic personal or professional identity **for legal value digital signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage** : As indicated by Subscriber. **Limit on transaction value**: As indicated by Subscriber.
E-Trust Qualified Certificate without SSCD (0.4.0.1456.1.2) and Key Generation by CSP (0.3.2062.9.6.1.19.4.x)	Qualified 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.	Electronic personal or professional identity **for legal value digital signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage** : As indicated by Subscriber. **Limit on transaction value**: As indicated by Subscriber.
E-Trust Normalised Certificate without SSCD and Key Generation by Owner (0.3.2062.9.6.1.19.6.x)	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	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. **Limit on transaction value**: As indicated by Subscriber.

E-Trust Normalised Certificate with SSCD and Key Generation by CSP (0.3.2062.9.6.1.19.7.x)	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	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. **Limit on transaction value**: As indicated by Subscriber.
E-Trust Normalised Certificate without SSCD and Key Generation by CSP (0.3.2062.9.6.1.19.8.x)	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	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. **Limit on transaction value**: As indicated by Subscriber.

Belgacom E-Trust Qualified Certificate for Qualified Signature only, and in the context of Certipost application				
	Key Usage	Legal value	Type of applications	Restriction of usage
E-Trust Qualified Certificate without SSCD (0.4.0.1456.1.2) and Key Generation by Owner (0.3.2062.9.6.1.23.2.x)	Qualified Digital Signature only (Key usage extension: nonRepudiation,)	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.	Electronic personal or professional identity **for legal value digital signature** in the context of Certipost application only.	**Limit of usage** : As indicated by Subscriber. **Limit on transaction value**: As indicated by Subscriber.

Belgacom 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 (0.4.0.1456.1.2) and Key Generation by Owner (0.3.2062.9.6.1.25.2.x)	Qualified 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.	Electronic legal person identity **for legal value digital signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage** : As indicated by Subscriber. **Limit on transaction value**: As indicated by Subscriber.

E-Trust Qualified Certificate with SSCD (0.4.0.1456.1.1) and Key Generation by CSP (0.3.2062.9.6.1.25.3.x)	Qualified Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Legal Qualified Signatures (according to art. 4, §4 of the 09 July 2001 Law and art. 5.1 from The European Directive).	Electronic legal person identity **for legal value digital signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage** : As indicated by Subscriber. **Limit on transaction value**: As indicated by Subscriber.
E-Trust Qualified Certificate without SSCD (0.4.0.1456.1.2) and Key Generation by CSP (0.3.2062.9.6.1.25.4.x)	Qualified 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.	Electronic legal person identity **for legal value digital signature** in (high value) commercial transactions, contract signing, banking transactions, interactions with Public Institutions, etc.	**Limit of usage** : As indicated by Subscriber. **Limit on transaction value**: As indicated by Subscriber.
E-Trust Normalised Certificate without SSCD and Key Generation by Owner (0.3.2062.9.6.1.25.6.x)	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	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. **Limit on transaction value**: As indicated by Subscriber.
E-Trust Normalised Certificate with SSCD and Key Generation by CSP (0.3.2062.9.6.1.25.7.x)	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	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. **Limit on transaction value**: As indicated by Subscriber.
E-Trust Normalised Certificate without SSCD and Key Generation by CSP (0.3.2062.9.6.1.25.8.x)	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	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. **Limit on transaction value**: As indicated by Subscriber.

Belgacom E-Trust Lawyer's Qualified and Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
Lawyers' Qualified Certificate without SSCD (0.4.0.1456.1.2) and Key Generation by Owner (0.3.2062.9.6.1.15.2.x)	Qualified 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.	Electronic Lawyer's professional identity **for legal value digital signature** 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**.
Lawyers' Qualified Certificate with SSCD (0.4.0.1456.1.1) and Key Generation by CSP (0.3.2062.9.6.1.15.3.x)	Qualified Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Legal Qualified Signatures (according to art. 4, §4 of the 09 July 2001 Law and art. 5.1 from The European Directive).	Electronic Lawyer's professional identity **for legal value digital signature** 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**.
Lawyers' Qualified Certificate without SSCD (0.4.0.1456.1.2) and Key Generation by CSP (0.3.2062.9.6.1.15.4.x)	Qualified 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.	Electronic Lawyer's professional identity **for legal value digital signature** 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**.
Lawyers' Normalised Certificate without SSCD and Key Generation by Owner (0.3.2062.9.6.1.15.6.x)	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	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**.

Lawyers' Normalised Certificate with SSCD and Key Generation by CSP (0.3.2062.9.6.1.15.7.x)	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	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**.
Lawyers' Normalised Certificate without SSCD and Key Generation by CSP (0.3.2062.9.6.1.15.8.x)	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	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**.

Belgacom E-Trust FRNB Qualified and Normalised Certificate				
	Key Usage	Legal value	Type of applications	Restriction of usage
FRNB Qualified Certificate with SSCD (0.4.0.1456.1.1) and Key Generation by CSP (0.3.2062.9.6.1.26.3.x)	Qualified Digital Signature only (Key usage extension: nonRepudiation, and digitalSignature)	Appropriate for supporting Legal Qualified Signatures (according to art. 4, §4 of the 09 July 2001 Law and art. 5.1 from The European Directive).	Electronic notarial professional identity **for legal value digital signature** 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 notarial profession. **No limit on transaction value**.
FRNB Normalised Certificate with SSCD and Key Generation by CSP (0.3.2062.9.6.1.26.7.x)	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	Electronic notarial 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 notarial profession. **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

Belgacom 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:
Belgacom E-Trust Services — http://www.e-trust.be
Belgacom E-Trust PKI Certification Practices Council
C/o Veerle Vandenabeele — Fax: +32 (2) 201 56 50
Ref.: CPS Administration
Koning Albert II-laan, 27
B-1030 Brussels
Belgium

1.4.3 Person determining CPS suitability for the policy

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

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

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

d) To contact the Belgacom 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 Belgacom E-Trust Services:

Infrastructure -- Belgacom E-Trust Services is obliged to maintain the Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom E-Trust PKI Infrastructure in accordance with this Q&N CPS.

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

- The Certificates that have been delivered by a CA in accordance with this Q&N CPS and the applicable CP; and
- The Certificate Revocation List published in accordance with this Q&N CPS and with the applicable CP.
- The CA Certificates of the CAs that are part of the Belgacom E-Trust Qualified and Normalised PKI segment.

Electronic Registry Protection -- Belgacom E-Trust Services is obliged to provide its best effort to protect the Belgacom E-Trust Certificate Public Registry against unauthorised modifications.

Agreements -- Belgacom 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 Belgacom E-Trust Services and the RA.

2.1.1 CA obligations

The following are the obligations of any CA within the Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom E-Trust PKI Infrastructure:

a) **Standards compliance** -- Belgacom 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).

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 Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom 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** --

1. 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 policy.
2. The CA is obliged to inform the Subscriber about the requirements regarding the protection of Private Key.
3. 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 authorised 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, Belgacom E-Trust uses databases with these personal data. In this regard, Belgacom 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 Belgacom E-Trust are incorporated in the files of BELGACOM S.A. of public law, Boulevard du Roi Albert II, 27, 1030 Brussels. The data will only be used for the provisioning of the Belgacom 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 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 Belgacom 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 Belgacom E-Trust RA Procedures and Guidelines.

b) **Maintain Certificate application information** -- The RA is obliged to keep, for 30 years after expiricy of the corresponding certificates, 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 Belgacom 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 Belgacom 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 Belgacom 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 unauthorised 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 recognised 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 lawyer holding the Certificate (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.

h) The above information 2.1.2.2 g) are archived for a period of 30 years.

i) 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.

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

k) 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.

l) 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.).

m) The LRA shall ensure these items (2.1.2.2 l))) 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.

n) 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 Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom 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 7 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 Belgacom E-Trust without any delay. Belgacom 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 Belgacom E-Trust in the event of a dispute. Belgacom 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. Belgacom 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.

k) For possible additional specific obligations see specific CP.

2.1.4 Relying party information

The following are the relying parties' issues:

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

b) Belgacom 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, Belgacom 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. Belgacom E-Trust does not warrant "non repudiation" of any Certificate or message. Belgacom E-Trust does not warrant any software.

2.2.3 Loss limitations

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

a) In no event shall Belgacom 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 Belgacom E-Trust has been advised of the possibility of such damages.

b) In no event shall Belgacom 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) In no event will the aggregate liability of Belgacom E-Trust to all parties, including but not limited to Subscribers, applicants, recipients or relying parties, exceed the applicable liability cap for such Certificate set forth below. The combined aggregate liability of Belgacom 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: 25000 EUR.

   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 Belgacom 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 Belgacom 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 Belgacom 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 Belgacom 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 Belgacom 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

Belgacom 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 Belgacom 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 fulfil 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 fulfil such purposes.

2.4.2.3 Merger

In case of a merger, Belgacom 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 Belgacom 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 or Normalised Certificate fees* is provided by Belgacom E-Trust on a regularly updated pricing sheet.

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.

2.5.2 Certificate access fees

Access to Certificates on the Belgacom 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 Belgacom 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 Belgacom 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.

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 Belgacom E-Trust Qualified and Normalised PKI segment shall make publicly available, in their repositories:

- The Belgacom 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 whith 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. Belgacom E-Trust will do its best efforts to obtain an up99 %limit such unavailability period of time.

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, Belgacom E-Trust uses databases with these personal data. In this regard, Belgacom E-Trust respects the privacy of the persons concerned. The Subscriber authorises Belgacom E-Trust to publish such personal data on its repositories.

b) Belgacom E-Trust shall publish a copy of issued Certificates in publicly available repositories, after the Certificate has been issued by Belgacom 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) Belgacom 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) Belgacom E-Trust will make available the CA-Certificates for all public CA-keys in the Belgacom 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 Belgacom E-Trust Certificate Public Registry, the CP's and Q&N CPS are protected against any unauthorised modification.

2.6.4 Repositories

Belgacom E-Trust Services will use the Belgacom 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. Belgacom E-Trust will take legal actions against any person or organisation disregarding this prohibition.

2.7.1 Frequency of entity compliance audit

a) The Belgacom 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 Belgacom 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 CA's practice laid down in its Q&N CPS and the appropriate CP's with the on site implementation. All aspects of the CA's operation as specified in its 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 Belgacom E-Trust PKI Certification Practices Council. The BEC will determine a remedy, including a time for completion.

Belgacom E-Trust Services PKI Certification Practices Council C/o Veerle Vandenabeele Bd du Roi Albert II, 27 B-1030 Brussels Belgium	http://www.e-trust.be Fax: +32 (2) 201 56 50

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 Belgacom 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 judgement 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 Belgacom 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) Belgacom 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 Belgacom 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 BELGACOM S.A. of public law, Boulevard du Roi Albert II, 27, 1030 Brussels. The data will be used for the provisioning of the Belgacom 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[1], 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.

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

e) All Private Keys used and handled within the CA operation under this CPS are to be kept confidential.

f) Audit logs and records shall not be made available as a whole, except as required by law. Only records of individual transactions may be released according to 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 Belgacom 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 and Normalised 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 association). **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 association). **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 association),), unless stated otherwise in the applicable CP.
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 name 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. **Other entities**: Unique name identifying the entity.

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

3.1.2 Need for names to be meaningful

a) In case of Subscribers, the information in the Belgacom 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 Belgacom E-Trust.

c) In case of legal person (organisational 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 name 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 Belgacom E-Trust Services (see contact information in section 1.4.2. Belgacom E-Trust Services will investigate the grounds on which the name claim dispute is based.

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

c) In case the name claim dispute is due to an error of Belgacom E-Trust Services, Belgacom 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, Belgacom 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 Belgacom E-Trust reserves the right to undertake legal actions.

3.1.6 Recognition, authentication and role of trademarks

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

b) No RA, or any CA within the Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom E-Trust PKI Infrastructure is obliged to perform any trademark infringement investigation at the time the Naming information is provided by an entity. Belgacom 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 users Private Key possession.

b) Additional measures are 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 identity

a) The RAs within the Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom 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 Belgacom E-Trust Qualified or Normalised 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 Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom 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 Belgacom 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**:

- 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.
- 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.
- When confirmed, the suspension of a Certificate shall be so for an unlimited period of time.

In the case of **unsuspension** :

- To obtain the form required for Unsuspension, the applicant shall contact the Suspension and Revocation Authority of the CSP which issued the Certificate.
- 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.
- 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.
- The SRA shall then reinstate the Certificate within 24 hours of receiving the application.

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

- Request the suspension of the Certificate (see above);
- Contact the SRA to ask for a certificate revocation application form.

- 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.
- 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.
- 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. 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).

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

d) 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 Belgacom 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 rekey, 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 Subcriber 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 Belgacom 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 Belgacom E-Trust Certificate Public Registry, unless specified otherwise in the CP.

b) The Certificate is deemed accepted by the Subscriber within 7 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 Belgacom E-Trust without any delay. Belgacom 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 one (1) hour**.** 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 endeavours 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 endeavours 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://baobab.e-trust.be:389 and on ldap://baobab1.e-trust.be:389 as CRL attribute of the Belgacom E-Trust Root CA for Qualified Certificates, the Belgacom E-Trust Primary CA for Qualified Certificates, the Belgacom E-Trust Root CA for Normalised Certificates and the Belgacom E-Trust Primary CA for Normalised Certificates. 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), Belgacom 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 Belgacom 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 Belgacom 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, authentified and confirmed as specifed 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 one (1) hour**.** 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 Belgacom E-Trust Certificate Public Registry (e.g. DAP, LDAP or HTML protocols). See the Belgacom E-Trust web site (www.e-trust.be/en/x500) 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 Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom E-Trust PKI:

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

- 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-exhaustif) :

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

c) *Application log :* Created by one of the Belgacom E-Trust Qualified and Normalised PKI segment 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 Belgacom E-Trust PKI Infrastructure. These event recordings include (non-limitatif) :

- The creation of the Belgacom 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 wasn't 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 analysed 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 Belgacom E-Trust Qualified and Normalised PKI segment Infrastructure are digitally signed.

b) Only dedicated internal Belgacom E-Trust qualified staff members 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 an 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

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

Network vulnerability assessments are carried out on a regular basis to ensure that the servers on the Belgacom E-Trust Qualified and Normalised PKI segment are secured appropriately.

4.6 Records Archival

Beside the information, listed in 4.5, all information published in Belgacom E-Trust Certificate Public Registry and all information exchange between the user and the different elements of the Belgacom E-Trust Qualified and Normalised 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 Belgacom E-Trust Qualified and Normalised PKI segment elements. All the published data (in Belgacom 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 Belgacom E-Trust staff members are allowed to manipulate these files.

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

b) Depending on the policy used to enrol 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 recognised representatives. These data are stored in a separate database (not the Belgacom 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 Belgacom E-Trust. A new Certificate is not automatically rebuild 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 or Normalised) 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 himself is still valid.

4.7.3 Cross-certification keys

a) Cross-certified CA's, as any other users, are warned by Belgacom 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 section of this Q&N CPS). After the problems and the resolution are analysed, 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 Belgacom E-Trust Qualified and Normalised Root and Primary CA 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 Belgacom E-Trust CA compromising or operator errors, Belgacom E-Trust will provide, for free, a new equivalent Certificate to the user, based on a rekey procedure (see section 3.3). If the user reveals to be a defrauder, Belgacom 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, Belgacom 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 4.4.10 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 fulfil 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 to perform all the tasks regarding the Belgacom E-Trust Services. All the components of the Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom E-Trust PKI are protected against unauthorised use.

5.1 Physical Controls

This concerns all the sites where the Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom E-Trust PKI, including the CAs, CAOs, RAs, RAOs, LRAs, LRAOs, the Belgacom E-Trust on-line request service, Certificate Public Registry and the Belgacom E-Trust website.

5.1.1 Site location and construction

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

- PKI Security Rooms: In these rooms reside the services for the Belgacom E-Trust Root and Primary CAs for Qualified and for Normalised Certificates, the Belgacom E-Trust Primary RAs for Qualified and for Normalised Certificates, the Belgacom E-Trust on-line request, Certificate Public Registry, Online Revocation Status Service, and the Belgacom 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 Belgacom E-Trust services, as well as the Belgacom E-Trust CRAO and the Belgacom E-Trust SRAO service. These rooms have a high level of security.
- PKI SRAO Room : In this room resides the Belgacom E-Trust Primary SRAO for Qualified and for Normalised Certificates services. This room has a high level of security.
- PKI LRAO Rooms : In these rooms resides the components for the Belgacom E-Trust LRAO Services. These rooms has 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 a) : These areas are protected against unauthorised access by at least 3 perimeters protections. The first and the second consist of a badge system and the third of a badge system combined with a biometrics authentication system. 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 then 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 Belgacom E-Trust staff members must follow the fully documented procedure to access the rooms. Each Belgacom E-Trust staff member as well as his/her backup are identified. The access rights to the various PKI locations are clearly identified for each Belgacom E-Trust staff member and his/her backup. Giving access to a new Belgacom E-Trust staff member requires very strict verifications. The access right of a Belgacom E-Trust staff member who quits Belgacom or who is subject to a security-screening is immediately removed.

e) Detailed description of the protection of these areas (5.1.2 b) and 5.1.2 c)) and Access Control Security Policies are provided in internal documents.

5.1.3 Power and air conditioning

a) The power supply of the Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom E-Trust PKI 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 Belgacom E-Trust Very High Security Rooms are fire protected.

5.1.6 Media storage

All the media are memorised and stored at one site with the same degree of physical protection and replicated in another site 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 Belgacom procedure. Dedicated closed trash boxes are used for confidential data. The content is destroyed immediately when removed. 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 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 Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom E-Trust PKI are clearly defined in internal documents.

b) The Belgacom E-Trust Staff Members are either employees of Belgacom sa, or employees of Certipost sa (an affiliate company of Belgacom and The Belgian Post), 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 Belgacom E-Trust Infrastructure :

- **Security Officers**: Persons who fulfil this role have an overall responsibility for administering the implementation of the security practices.
- **System Administrators** : Persons who fulfil this role are authorised to install, configure and maintain the PKI trustworthy systems for support for registration, Certificate generation, Subscriber device provision and revocation management. They are authorised to perform system backup and recovery.
- **System Auditors**: Persons who fulfil this role are authorised to view and maintain archives and audit logs of the PKI trustworthy systems.
- **Certification Authority Auditor (CAA)** : Persons who fulfil this role have the responsibility to perform the a posteriori audit and check of the correct and authorised issuing of the Certificates issued by the CA.
- **Central Registration Authority Operator (CRAO)** : Persons who fulfil 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 fulfils 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 fulfil this role, have the responsibility for the suspension, revocation and unsuspension of the Certificates.
- **Belgacom E-Trust PKI Certification Practices Council** : Persons who fulfil 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 is in line with the Belgacom 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.

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 Belgacom E-Trust Staff Members are either employees of Belgacom sa, or employees of Certipost sa (an affiliate company of Belgacom and The Belgian Post), or contracted LRAOs in accordance with section 1.3.3, and with the other applicable provisions of the present document.

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

c) The Belgacom 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 Belgacom E-Trust Staff Member must be background checked independently and individually. Belgacom sa employees or any physical person who are not Belgacom E-Trust Staff Members have only a temporary access to the PKI-locations, must always be accompanied by at least one Belgacom 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 fulfil 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 fulfil 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 Belgacom 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 Belgacom sa, Certipost sa contract following the Belgian legislation plus a special Non Disclosure Agreement are used. For LRAOs not employed by Belgacom sa or Certipost sa, 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 and Belgacom E-Trust.

5.3.8 Documentation supplied to personnel

Each Belgacom E-Trust Staff Member 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 Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom 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 Root or not) key pair generation is ruled by a fully documented procedure called "Wedding ceremony" (internal confidential document).

b) For the Belgacom E-Trust Primary and Root Qualified and Normalised 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 initialisation, 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 Belgacom 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 floppy-disk 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, Belgacom 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

Two (2) 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 sent by email at request@e-trust.be, 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 section3.2 of the present Q&N CPS) and when authorised in the applicable CP.

6.1.4 CA Public Key delivery to users

The CA Public Keys are published on the Belgacom E-Trust Certificate Public Registry and Belgacom 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 Belgacom E-Trust).

6.1.5 Key sizes

a) The (Root) CA Certificates have a key size (RSA) of 2048 bits. The key size of other PKI components in the Belgacom E-Trust Qualified and Normalised PKI segment is of minimum 1024 bits.

b) Minimum accepted Subscriber key size is (RSA) 1024 bits.

6.1.6 Public Key parameters generation

a) For all the Belgacom 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 Belgacom E-Trust Qualified and Normalised PKI segment from the Belgacom 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 Belgacom E-Trust are FIPS 140-1 level 4 certified.

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

6.1.9.1 PKI components Public Key

a) The CA has 2 key pairs :

- One 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, as defined in section 7.3.3 of ETSI 101 456, within physically secure premises.
- The other key pair is not used for signing Certificates and CRL's and has the key usage digital signature, non repudiation, key encryption, data encryption and key agreement enabled in the corresponding certificate.

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 Belgacom E-Trust Qualified and Normalised PKI segment are FIPS 140-1 Level 4 certified.

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 Belgacom E-Trust Qualified and Normalised CA's, are encrypted by a Storage Master Key (SMK). This SMK is split and written onto 8 smartcards. These 8 smartcards are given to 4 persons, holding each 2 smartcards. For the recovery of the Storage Master Key, at least 3 smartcards needs to be combined.

For the other Belgacom E-Trust components, one double pass phased protected smart card is required.

6.2.3 Private Key escrow

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

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

6.2.4 Private Key backup

a) PKI components: At the same time of generating the Private Keys of the Belgacom E-Trust Qualified and Normalised 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 Belgacom 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 Belgacom E-Trust Qualified and Normalised CA's are activated, using 2 passphrase protected smartcards, hold by 2 different security officers.

Additionally, two double passphrase protected smartcards, hold by 2 different security officers, are needed, as well as a PIN code to access the HSM for starting the Belgacom E-Trust Qualified and Normalised 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 Belgacom E-Trust Qualified and Normalised CA Keys is shutdowned 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

The Private Keys of the Belgacom E-Trust Qualified and Normalised 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.

The Private Keys of the Belgacom E-Trust Qualified and Normalised 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 Belgacom 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:
   - Root CAs: The validity period is twenty (20) years.
   - Primary CAs: The validity period of the key for the issuing of Qualified or Normalised Certificates is nine (9) 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 Belgacom 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 must not be shared.

   - Subscriber: In accordance with the CPS currently in effect and with this 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 Belgacom 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) Belgacom E-Trust will do all its best to guarantee the highest possible level of security of its infrastructure.

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

6.5.2 Computer security rating

This information is described in Belgacom 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 Belgacom E-Trust Testing Environment before being used in the Belgacom E-Trust production environment. Change management and configuration management follow the operational procedures commonly used within Belgacom. Both change and configuration management ultimately are the responsibility of the members of the Belgacom 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 Belgacom E-Trust PKI computers to check any flaws and problems in the security.

6.6.3 Life cycle security ratings

Internal Belgacom procedures will be strictly followed.

6.7 Network Security Controls

The Belgacom 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 Belgacom E-Trust Qualified and Normalised CA's Private Keys, are FIPS 140-1 level 4 compliant.

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

	X509 v3 extensions	
KeyUsage	Mandatory	– For the Belgacom E-Trust Root and Primary CA Certificates : as defined in section 6.1.9.1. – For the Certificates, issued by the Belgacom E-Trust Primary CA's : – Qualified Certificates : non-repudiation and digitalSignature. – Normalised Certificates: as defined in the corresponding CP.
CertificatePolicies	– Not used for the Belgacom E-Trust Primary and Root Q&N CA Certificates. – Mandatory for the Certificates, issued by the Belgacom E-Trust Primary Q&N CA's.	– policyIdentifier : as defined in section 1.2.2. – policyQualifiers : userNotice : as defined in the corresponding CP's. Example: "<Qualified or Normalised> E-Trust certificate for digital signature; <Qualified or Normalised> certificate <with or without> SSCD; Key generation by <the owner or the CSP>. General conditions O.I.D.: 0.3.2062.9.6.w.x.y.z"
basicConstraints	– Mandatory for the Belgacom E-Trust Primary and Root Q&N CA Certificates. – Not used for the Certificates, issued by the Belgacom E-Trust Primary Q&N CA's, unless specified in the corresponding CP.	– For the Belgacom E-Trust Qualified and Normalised Root CA Certificates : o cA: TRUE o PathLenConstraint: 5 – For the Belgacom E-Trust Qualified and Normalised Primary CA's : o cA: TRUE o PathLenConstraint: 2

authorityInfoAccess	– Mandatory for the Belgacom E-Trust Primary and Root Q&N CA Certificates. – Not used for the Certificates, issued by the Belgacom E-Trust Primary Q&N CA's.	accessMethod : On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.e-trust.be
authorityKeyIdentifier	– Mandatory for the Belgacom E-Trust Primary Q&N CA Certificates. – Not used for the Certificates, issued by the Belgacom E-Trust Primary Q&N CA's, unless specified in the corresponding CP.	– For the Belgacom E-Trust Root and Primary Normalised CA Certificates : – keyIdentifier: 95E1 1594 E795 3E25 6DCA F6BF 7558 A2FC 6191 D56F – authorityCertIssuer: Directory Address: – CN=Belgacom E-Trust Root CA for normalised certificates – OU=E-Trust – O=Belgacom – C=BE – authorityCertSerialNumber: 3BE6 B035 – For the Belgacom E-Trust Root and Primary Qualified CA Certificates : – KeyIdentifier: 6FC0 4354 7292 F7DB 2CA8 ADB8 03BF D0A3 5209 E5A5 – Certificate Issuer: Directory Address: – CN=Belgacom E-Trust Root CA for qualified certificates – OU=E-Trust – O=Belgacom – C=BE – authorityCertSerialNumber=3B73 9C9D
subjectKeyIdentifier	– Mandatory for the Belgacom E-Trust Primary Q&N CA Certificates. – Not used for the Certificates, issued by the Belgacom E-Trust Primary Q&N CA's, unless specified in the corresponding CP.	– For the Belgacom E-Trust Primary Qualified CA Certificate: 486B A7D3 A75D 8E93 AC96 00DC 5C17 A391 4843 C558 – For the Belgacom E-Trust Root Qualified CA Certificate: – 6FC0 4354 7292 F7DB 2CA8 ADB8 03BF D0A3 5209 E5A5 – For the Belgacom E-Trust Primary Normalised CA Certificate: – 06EB 4E0A 0E78 7B56 AFC2 B453 3B95 5768 3A2E 4C21 – For the Belgacom E-Trust Root Normalised CA Certificate: – 95E1 1594 E795 3E25 6DCA F6BF 7558 A2FC 6191 D56F

netscapeCertType	– Mandatory for the Belgacom E-Trust Primary Q&N CA Certificates. – Not used for the Certificates, issued by the Belgacom E-Trust Primary Q&N CA's, unless specified in the corresponding CP.	For the Belgacom E-Trust Root and Primary Q&N CA Certifcates : SSL CA , SMIME CA , Signature CA(07)

Other extensions may be used according to relevant CP.

7.1.3 Signature algorithm object identifiers

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

sha1WithRSAEncryption : iso(1).member body(2).USA(840).RSADSI(113549).PKCS(1).PKCS-1(1)

7.1.4 Use of name fields

See subsection 3.1.1of this Q&N CPS.

7.1.5 Name constraints

Belgacom E-Trust will fully follow the structure described in the X500 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 Belgacom 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 Belgacom 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 Belgacom 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 Belgacom E-Trust PKI Certification Practices Council shall be disseminated to interested parties (see section 8.2of 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 Belgacom E-Trust Q&N CPS, the corresponding CP's, general conditions and purchase orders are the one that are published by the Belgacom 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 Belgacom E-Trust Management Board on http://www.e-trust.be/CPS/QNcerts

8.3 CPS approval procedures

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