

Certificate Policy for **Normalised** **E-Trust Certificates**

Version 1.0

Date published: 1 January 2007

Certificate Policy for Normalised E-Trust Certificates

This document describes the applications for which certificates, in the form of a Normalised E-Trust Certificate (hereinafter referred to as the “Certificate”) issued by the Certification Service Provider (CSP) under this Certificate Policy (CP), may be used, as well as the procedures to be followed and the responsibilities of the parties involved, in accordance with the CSP’s Certification Practice Statements (CPS). This CP applies to Normalised Certificates that meet the following criteria.

Section		Ref. RFC 2527
A	<i>Detail of the Certificate Policy for Normalised E-Trust Certificates</i>	1.1
	<p>This type of Certificate provides a very high degree of assurance of the electronic personal and professional identity of a physical person or a Legal Entity. It guarantees proper authentication given that the Customer must be present in person when his/her application is registered by a Registration Authority (RA). The Customer is an employee of a legal entity, a legal representative of the Legal Entity or a duly authorized representative thereof. The link between the physical person or the Legal Entity and the public key is certified.</p> <p>The Certificate provides the highest degree of assurance of proper authentication since the person applying for the Certificate must go to a RA in person for official registration before a Normalised Certificate can be issued by the Certification Service Provider.</p> <p>For applications to be validated the person applying for the Certificate must present, for verification, his/her identity card and proof of his/her professional status, together with any supporting information to be certified and documents linking his identity to the company (organization).</p> <p>The private key corresponding to the public key certified in this way can be used for all usage except a Qualified Digital Signature (e.g. Normalised digital signature, encryption and/or authentication, and any combination of these except a qualified digital signature) in which case the certificate is specified by the criteria for “Normalised Certificates” as specified by technical standard ETSI 102 042.</p> <p>The Certification Service Provider authorized to issue Certificates under this CP specifies whether it complies with this CP and with the regulatory texts or whether the Certificates are certified in accordance with the CP (see Section D1(5) of this document).</p>	
B	<i>Identification of the Certificate Policy for Normalised E-Trust Certificates</i>	
	<p>A CP is a specific set of rules that indicate a Certificate's applicability to a particular community and/or type of application that shares the same security requirements.</p> <p>This document sets out and identifies the E-Trust Certificate Policy for Normalised Certificates. These Certificates are compatible with, and meet the requirements laid down in, ETSI TS 102 042.</p> <p>The CSP, on behalf of the Certificate Holder is responsible for the generation of the Private Key and Public Key.</p>	

Section		Ref. RFC 2527			
	<p>The Certificates issued under this Normalised Certificate Policy have a CP identifier. This can be used by third parties to determine the applicability and trustworthiness of the Certificate for a particular application. This Identifier is as specified in the table below .</p> <p style="text-align: center;">Normalised E-Trust Certificate</p> <table><tr><td>Normalised Certificate with SSCD OID ETSI 102 042: 0.4.0.2042.1.2 Key generation by CSP: 0.3.2062.7.1.1.201.x</td></tr><tr><td>Normalised Certificate without SSCD OID ETSI 102 042: 0.4.0.2042.1.1 Key generation by CSP: 0.3.2062.7.1.1.202.x</td></tr></table> <p style="text-align: center;">Normalised E-Trust-certificaat voor Legal Persons</p> <table><tr><td>Normalised Certificate without SSCD OID ETSI 102 042: 0.4.0.2042.1.1 Key generation by owner: 0.3.2062.7.1.1.211.x</td></tr></table> <p style="text-align: center;">Tabel 1. Identification of E-Trust Certificate Policy for Normalised Certificates</p>	Normalised Certificate with SSCD OID ETSI 102 042: 0.4.0.2042.1.2 Key generation by CSP: 0.3.2062.7.1.1.201.x	Normalised Certificate without SSCD OID ETSI 102 042: 0.4.0.2042.1.1 Key generation by CSP: 0.3.2062.7.1.1.202.x	Normalised Certificate without SSCD OID ETSI 102 042: 0.4.0.2042.1.1 Key generation by owner: 0.3.2062.7.1.1.211.x	
Normalised Certificate with SSCD OID ETSI 102 042: 0.4.0.2042.1.2 Key generation by CSP: 0.3.2062.7.1.1.201.x					
Normalised Certificate without SSCD OID ETSI 102 042: 0.4.0.2042.1.1 Key generation by CSP: 0.3.2062.7.1.1.202.x					
Normalised Certificate without SSCD OID ETSI 102 042: 0.4.0.2042.1.1 Key generation by owner: 0.3.2062.7.1.1.211.x					
C	Applicability	1.3.4			
	<ul style="list-style-type: none">• This type of Certificate provides a very high assurance of the electronic identity of a Physical Person or a Legal Entity. It can therefore also be used to protect top-level applications in a client/server, browser/server model, such as major commercial transactions, conclusion of contracts and signing of files, bank transactions and interactions with public institutions.• The applications for which the Certificate is deemed to be trustworthy must be decided by the parties themselves on the basis of the nature of the Certificate and the level of security of the procedures followed for issuing and managing the Certificate as described in this CP.• Key usage and the applicability of the Certificate are certified (see the description of the Certificate content in Section E of this document). Normalised Certificates for physical persons and legal entities issued under this CP comply with ETSI TS 102 042 (NCP).				
D	Rights, responsibilities and obligations	2			
D.1	Rights, responsibilities and obligations of the Certification Service Provider	2.1			
	<ul style="list-style-type: none">• The CSP issues X509 v3-compatible Certificates (ISO 9594-8).• The CSP issues Normalised Certificates as defined in and accordance with the criteria laid down in ETSI TS 102 042.To this end, the CSP publishes the elements supporting this statement of compliance.• The CSP guarantees that all the requirements set out in the applicable CP (and indicated in the Certificate in accordance with Section B of this document) are complied with. It also assumes responsibility for ensuring such compliance and providing these services in accordance with its CPS.• Information about the CSP(s) authorized to issue Certificates under this CP.				

¹ The personal data and completed Certificates delivered to the CSP and RA are entered into files held by the RA. These data are used solely for the purposes of providing certification services. The data owner is entitled to consult this information, and, where applicable, ask that it be rectified or deleted.

Section		Ref. RFC 2527
	<ul style="list-style-type: none"> - Certipost SA, via its Certipost E-Trust services provided through the Certipost E-Trust Primary Certification Authority (CA) for Normalised Certificates: <ul style="list-style-type: none"> - <i>Certification Practice Statements (CPS)</i>: www.e-trust.be/CPS/QNcerts, CPS OID: 0.3.2062.7.1.0.1.2.0 - <i>Public Register of Certificates and Certificate Revocation Lists (CRL)</i>: www.e-trust.be/en/x500 - <i>Statement of compliance</i>: www.e-trust.be/CPS/QNcerts - <i>Suspension/Revocation Authority</i>: 078 15 24 70 (available 24 hours a day, seven days a week). Suspension/revocation form available from the following address: www.e-trust.be/CPS/QNcerts • To register persons applying for a Certificate, the CSP uses the following approved Registration Authorities (RA's): <ul style="list-style-type: none"> - Certipost personnel authorized by the CSP to act as Registration Authorities. The authenticated list of approved persons is available on www.e-trust.be/CPS/QNcerts. - Contractually bound organizations that will act as RA for the provision of authenticated Certificate applications files. • When the CSP proceeds to the key pair generation on behalf of the Certificate Holder, it guarantees that such key pair generation is performed in a secured way and that the privacy of the private key is ensured according to the technical standard ETSI TS 102 042. • If the use of a Secure Signature Creation Device (SSCD) is imposed under the applicable CP, the Key Pair must be generated using this device and the Certificate must be used to create signatures solely by means of this device. • The sole guarantee provided by the CSP is that its procedures are implemented in accordance with its CPS and the verification procedures then in effect, and that all Certificates issued with a CP Object Identifier (OID) have been issued in accordance with the provisions of this CP, the verification procedures, and the CPS then in effect. • See Sections 2.1, 2.2 and 2.3 of the CSP CPS applying to the additional rights, responsibilities and obligations of the CSP. • In certain cases described in the relevant CPS (RFC 2527, Section 4.4), the CSP may revoke or suspend the Certificate (provided it informs the person applying for the Certificate in advance by an appropriate means). • In this regard, the CSP must protect the privacy of the persons concerned. It must therefore attach great importance to this matter and exercise all due care when handling such data. The CSP enters the personal data it receives into files. This data is used solely for the provision of certification services. The company/organization responsible for the Certificate may consult and change this data¹. The CSP must clearly specify the customer's right to privacy on its Certificate subscription contracts. • The CSP also guarantees the confidentiality of any data not published in the Certificates. 	
D.2	<i>Rights, responsibilities and obligations of the Certificate Holder</i>	2.1.3
	<p>The Certificate holder hereby accepts the Certification Practice Statement (CPS) currently in effect, as drafted by the CSP and setting out the procedures used for providing digital Certificates.</p> <p>The Certificate holder agrees to this CP.</p> <p>More specifically, the Certificate holder hereby gives his/her acceptance to the following.</p> <ul style="list-style-type: none"> • The contractual agreement for this type of Certificate is governed by Belgian law. 	

Section		Ref. RFC 2527
	<ul style="list-style-type: none"> • The information submitted to the CSP by the person applying for the Certificate must be precise, accurate, complete and meet the requirements for the type of Certificate and the CP(s) referred to in Section B of this document, and in particular with the corresponding registration procedures. The Certificate holder is responsible for the accuracy of the data provided to the CSP. • In using the Key Pair, the Certificate holder must comply with any limits indicated in the Certificate or in contractual agreement. • When the Certificate Holder is responsible for key-pair generation, this must be undertaken in accordance with the CP - using an algorithm and given key length (minimum of 1,024 bits) meeting the criteria set out in the CP - and with the contractual provisions concluded with the CSP. In addition, the Certificate holder must give an undertaking that he/she is the sole holder of the Private Key linked to the Public Key to be certified. • If the use of a Secure Signature Creation Device (SSCD) is imposed under the applicable CP, the Key Pair must be generated using this device and the Certificate must be used to create signatures solely by means of this device. • In accordance with the applicable CPS and with this CP, the Certificate holder must 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 is personally responsible for ensuring the confidentiality and integrity of the Key Pair. The Certificate holder is deemed the sole user of the Private Key. The PIN (Personal Identity Number) or password used to prevent unauthorized use of the Private Key must never be held in the same place as the Private Key itself, nor alongside its storage medium. Nor must it be stored without protection and that protection must be adequate. The Certificate holder must never leave the 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 has sole liability for the use of the Private Key. The CSP is not liable for the use made of the Key Pair belonging to the Certificate holder. • The Certificate holder must ask the CSP to suspend or revoke the Certificate as required pursuant to the relevant CPS (Section 4.4), and in particular if: <ul style="list-style-type: none"> • The Private Key of the Certificate holder is lost, stolen or potentially compromised; or, • The Certificate holder no longer has control of the Private Key because the activation data (e.g., PIN code) has been compromised or for any other reason; and/or, • The certified data has become inaccurate or has changed. • The Certificate is then revoked immediately. The suspension and revocation procedures are set out in Section J of this document. • The Certificate holder must immediately inform the CSP Certification Service of any changes to the data on the Certificate. The Certificate is then revoked immediately. • The Customer holding the Certificate must inform the CSP of any changes to data not included in the Certificate but submitted to the CSP during registration. The CSP then rectifies the data registered. • The Certificate holder must ask for the revocation of the Certificate if the information submitted to the CSP as proof of professional status becomes obsolete, in full or in part. • The Certificate holder must agree to his/her digital Certificate being published in the CSP Public Register of Certificates immediately after it has been issued. 	

Section		Ref. RFC 2527
	<ul style="list-style-type: none"> • The Certificate is deemed to have been accepted by the Certificate holder on the eighth day after its publication in the CSP Public Register of Certificates or its first use by the holder, whichever occurs first. In the intervening period, the Certificate holder is responsible for checking the accuracy of the content of the Certificate published. The Certificate holder must immediately notify the CSP of any inconsistency he/she has noted between the information in the contractual agreement and the content of the Certificate. The CSP then revokes the Certificate and takes the appropriate measures to reissue a Certificate. This is the sole recourse available to the Customer in the event of non-acceptance of the Certificate on his/her part. • The Certificate holder must agree to the retention - for a period of 30 years from the date of expiry of the last Certificate linked to the RA registration - by the CSP and the RA of all information used for the purposes of registration, for the provision of a SSCD or for the suspension or revocation of the Certificate, and, in the event that the CSP ceases its activities, the Certificate holder must permit this information to be transmitted to third parties under the same terms and conditions as those laid down in this CP. • The Certificate holder hereby acknowledges the rights, obligations and responsibilities of the CSP. These are set out in the CPS currently in effect, in the Order Form and in the General Terms and Conditions relating thereto, and in this CP (Section D1). 	
D.3	<i>Rights, responsibilities and obligations of the Registration Authority (RA)</i>	
	<p>The RA is under a contractual obligation to comply scrupulously with the registration procedures described in the CSP CPS (see Section D.1.5).</p> <p>The RA guarantees that:</p> <ul style="list-style-type: none"> – Certificate holders are properly identified and authenticated both as regards the personal identity of the Certificate holder as a natural person and as regards any information about professional status; – Any applications for Certificates submitted to the CSP are complete, accurate, valid and duly authorized. <p>More specifically:</p> <ul style="list-style-type: none"> – The RA Operator (RAO) informs 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 Customer (paper or notarized electronic form). – The RAO checks the identity of the Certificate holder on the basis of valid ID papers recognized under Belgian law. These papers must indicate the full name (last name and first names), date and place of birth, and the physical address at which the Certificate holder can be contacted. – If the Certificate holder is an affiliate of a legal person, the RAO validates the documentation supplied as proof of the existence of this relationship. – The RAO ensures the storing of one copy of the information provided during registration procedure by the Certificate holder and that was sent, in its entirety, to the CSP, and in particular: <ul style="list-style-type: none"> – A copy of all information used to check the identity of the Customer and any references to his/her professional status, including any reference numbers on documentation used for this verification as well as any limitations on its validity. – A copy of the contractual agreement signed by the Certificate holder, including the latter's agreement to all obligations incumbent on him/her. This information is retained for a period of 30 years from the date of expiry 	

Section		Ref. RFC 2527
	<p>of the last Certificate linked to the holder's registration by the RA.</p> <ul style="list-style-type: none"> – The validation procedure used by the RAO for electronic Certificate applications guarantees that the Certificate holder is in possession of the Private Key linked to the Public Key to be certified. – Compliance with the requirements relating to the processing of personal data with respect to the registration procedure. <p>The RA has a contractual obligation to put in place clear and appropriate measures with respect to:</p> <ul style="list-style-type: none"> • The physical security of the information and, where appropriate, of the systems concerned; • Logical access to any software used in the context of RA activities; • Employees dealing with registration. <p>The classification of and responsibility for this data are of crucial importance, i.e.,</p> <ul style="list-style-type: none"> • the data itself (registration data, guidelines and procedures, etc.) in paper form and, where applicable, in electronic form; • The software applications used and their configuration; • The equipment (hardware, telecommunications tools, etc.) and their configuration; • Physical access to the data (buildings, safes, access controls and conditional access to software, etc.). <p>The RA guarantees that these items are managed and stored in such a way as to avoid any repercussions as a result of a loss of confidentiality, integrity or even availability of this data.</p>	
D.4	<i>Rights, responsibilities and obligations of the Certificate holder's company (or organization)</i>	
	<p>The company (or organization), represented by its legal representative, must give its consent to the registration of the Certificate holder for the purposes of obtaining a Certificate attesting to professional status with respect to the company (or organization).</p> <p>The company (or organization) must agree to:</p> <ul style="list-style-type: none"> • the <u>CPS</u> currently in effect drafted by the CSP, which sets out the practices used to provide the Certificates; • this <u>CP</u> for E-Trust Normalised Certificates. <p>In particular, the company (or organization) must agree to the following:</p> <ul style="list-style-type: none"> • The Agreement between the company (or organization), the Certificate holder and the CSP being governed by Belgian law; • Assumption of all the Customer's responsibilities specified in the Customer contract. • Being responsible for the accuracy of the data it transmits to the CSP for the purposes of registration of the Certificate holder. The company (or organization) must immediately inform the CSP of any change to this data, and the latter will then take appropriate action. • In certain cases described in the relevant CPS (Section 4.4), the CSP may revoke or suspend the Certificate (provided that it duly notifies the Certificate holder and the company (or organization) by an appropriate means). • The company (or organization) must ask the CSP to suspend or revoke the Certificate as required under the CP and the CPS currently in effect (Section 4.4). The suspension and revocation procedures are described in the CPS currently in effect (Section 4.4). • The company (or organization) must accept the rights, obligations and 	

Section		Ref. RFC 2527																																				
	responsibilities of the CSP. These are set out in the CPS currently in effect, in the contract and this CP (section D).																																					
D.6	<i>Rights, responsibilities and obligations of third parties</i>																																					
	<p>Third parties who base themselves on Certificates issued in accordance with this CP must:</p> <ul style="list-style-type: none"> • Verify the validity of the Certificate by checking - against the CSP Certificate Revocation Lists (CRLs) - the contents and signature of the CSP which provided the Certificate and, where appropriate, the affiliate certification chain, the suspension or revocation of the Certificate, the Certificate of the CSP that issued the Certificate or the Certificate of any affiliate certification chain. (See Section D1.5 of this document.) • Take into account all the limitations on the use of the Certificate specified in the Certificate, the contractual documents and this CP. • Take all the other precautions with regard to use of the Certificate set out in the CP or elsewhere. 																																					
E	<i>Identification and Authentication – Certified information</i>	3.1																																				
	<p>The following information is validated (see Section E of this CP: Certificate application procedure) and certified in the E-Trust Normalised Certificate.</p> <table border="1"> <thead> <tr> <th>Attribute</th><th>Mandatory/ Optional/Fixed</th><th>Value</th></tr> </thead> <tbody> <tr> <td colspan="3">Distinguished Name :</td></tr> <tr> <td>Country (C)</td><td>Mandatory</td><td>Country in which the company's registered office is established (as specified in the memorandum and articles of association).</td></tr> <tr> <td>Locality (L)</td><td>Mandatory</td><td>Location in which the company's registered office is established (as specified in the memorandum and articles of association).</td></tr> <tr> <td>Organisation (O)</td><td>Mandatory</td><td>The official name of the company (or organization) to which the Certificate holder belongs, as published in the memorandum and articles of association of the company (or organization), including the legal form.</td></tr> <tr> <td>Organisational Unit (OU)</td><td>Optional</td><td>Organizational unit or department</td></tr> <tr> <td>Organizational Unit (OU)</td><td>Optional</td><td> <p>"Role in the organization : <...>"</p> <p>Either :</p> <ul style="list-style-type: none"> - Self employed - Administrator - C.E.O. - Manager - Employee <p>Or</p> <p>Another professional status statement, if the necessary proof is delivered, during registration</p> </td></tr> <tr> <td>commonName (CN)</td><td>Mandatory</td><td> <p>For certificates for a legal entity : The organisation name, followed by "KBO" followed by the KBO Number.</p> <p>For certificates for physical persons: Last name and first name (s), as indicated on the identity card</p> </td></tr> <tr> <td>surName</td><td>Optional</td><td>Certificate Holder's surname</td></tr> <tr> <td>givenName</td><td>Optional</td><td>Certificate Holder's given name</td></tr> <tr> <td>Rfc822Name</td><td>Optional</td><td>Certificate holder's e-mail address.</td></tr> <tr> <td colspan="3">Extensions (not critical unless specified otherwise)</td></tr> </tbody> </table>	Attribute	Mandatory/ Optional/Fixed	Value	Distinguished Name :			Country (C)	Mandatory	Country in which the company's registered office is established (as specified in the memorandum and articles of association).	Locality (L)	Mandatory	Location in which the company's registered office is established (as specified in the memorandum and articles of association).	Organisation (O)	Mandatory	The official name of the company (or organization) to which the Certificate holder belongs, as published in the memorandum and articles of association of the company (or organization), including the legal form.	Organisational Unit (OU)	Optional	Organizational unit or department	Organizational Unit (OU)	Optional	<p>"Role in the organization : <...>"</p> <p>Either :</p> <ul style="list-style-type: none"> - Self employed - Administrator - C.E.O. - Manager - Employee <p>Or</p> <p>Another professional status statement, if the necessary proof is delivered, during registration</p>	commonName (CN)	Mandatory	<p>For certificates for a legal entity : The organisation name, followed by "KBO" followed by the KBO Number.</p> <p>For certificates for physical persons: Last name and first name (s), as indicated on the identity card</p>	surName	Optional	Certificate Holder's surname	givenName	Optional	Certificate Holder's given name	Rfc822Name	Optional	Certificate holder's e-mail address.	Extensions (not critical unless specified otherwise)			
Attribute	Mandatory/ Optional/Fixed	Value																																				
Distinguished Name :																																						
Country (C)	Mandatory	Country in which the company's registered office is established (as specified in the memorandum and articles of association).																																				
Locality (L)	Mandatory	Location in which the company's registered office is established (as specified in the memorandum and articles of association).																																				
Organisation (O)	Mandatory	The official name of the company (or organization) to which the Certificate holder belongs, as published in the memorandum and articles of association of the company (or organization), including the legal form.																																				
Organisational Unit (OU)	Optional	Organizational unit or department																																				
Organizational Unit (OU)	Optional	<p>"Role in the organization : <...>"</p> <p>Either :</p> <ul style="list-style-type: none"> - Self employed - Administrator - C.E.O. - Manager - Employee <p>Or</p> <p>Another professional status statement, if the necessary proof is delivered, during registration</p>																																				
commonName (CN)	Mandatory	<p>For certificates for a legal entity : The organisation name, followed by "KBO" followed by the KBO Number.</p> <p>For certificates for physical persons: Last name and first name (s), as indicated on the identity card</p>																																				
surName	Optional	Certificate Holder's surname																																				
givenName	Optional	Certificate Holder's given name																																				
Rfc822Name	Optional	Certificate holder's e-mail address.																																				
Extensions (not critical unless specified otherwise)																																						

Section				Ref. RFC 2527
	KeyUsage	Fixed/Critical	digitalSignature, keyEncipherment, dataEncipherment	
	SubjectPublicKey	Mandatory	Public Key: Key length: 2048 bits (RSA); public exponent: Fermat-4 (=010001).	
	CertificatePolicies-policyIdentifier	Fixed	Physical persons with SSCD: 0.3.2062.7.1.1.201.1 Physical persons without SSCD: 0.3.2062.7.1.1.202.1 Legal persons without SSCD: 0.3.2062.7.1.1.211.1	
	CertificatePolicies-policyQualifier-userNotice	Fixed	Physical persons with SSCD: "E-Trust Certificate Policy for Normalised Certificates for Physical Persons. Supported by SSCD, Key Generation by CSP. GTC, CP , and CPS: www.e-trust.be/CPS/QNCerts " Physical persons without SSCD: "E-Trust Certificate Policy for Normalised Certificates for Physical Persons. Not supported by SSCD, Key Generation by CSP. GTC, CP , and CPS: www.e-trust.be/CPS/QNCerts " Legal persons without SSCD: "E-Trust Certificate Policy for Normalised Certificates for Legal Persons. Not supported by SSCD, Key Generation by Owner. GTC, CP and CPS: www.e-trust.be/CPS/QNCerts "	
	CertificatePolicies-policyQualifier-CPS	Fixed	http://www.e-trust.be/CPS/QNCerts	
	subjectKeyIdentifier	Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).	
	CRL Distribution Points	Fixed	Physical persons: http://crl.e-trust.be/NCA_PhP.crl Legal persons: http://crl.e-trust.be/NCA_LeP.crl	
	Other information:			
	Issuer	Fixed	"CN = Certipost E-Trust Secondary CA for Normalised Certificates O = Certipost C = BE"	
	Validity	Fixed	5 years	
	SerialNumber	Mandatory	Certificate sequence number	
	Algorithm	Fixed	"Sha1withRSAEncryption"	
	Version	Fixed	2 (in accordance with v3)	
	The Certification Authority's signature is appended to this certified information and relates to all of the information certified.			
F	Key-generation procedure			
	<p>The key size must be 1024 bits, except in the case of a certificate for a legal entity with a validity of 5 year, in this case the key size must be 2048 bits.</p> <p>Key generation by the Certificate holder When the person applying for the Certificate generates the key pair himself/herself as appropriate and in accordance with the Order Form, he/she must provide a diskette containing the PKCS#10 application for the Certificate when registering with the RAO:</p>			

Section		Ref. RFC 2527
	<p>Key generation by the CSP</p> <p>When the CSP proceeds to the key pair generation on behalf of the Certificate Holder, it guarantees that such key pair generation is performed in a secured way and that the privacy of the private key is ensured according to the technical standard ETSI TS 102 042 (NCP).</p>	
G	Certificate-application procedure	
	<p>The applicant for the Certificate must obtain an Order Form and the General Terms and Conditions for <u>Normalised Certificates</u> (hereafter referred to as “the Order Form” and “the General Terms and Conditions”) from the CSP (see Section D.1.5. These together with the CP and CPS constitute the Agreement. The person applying for the Certificate may also ask the CSP to send him/her copies of the documents in question by post or to obtain the documents from an RA approved by the CSP. The correct versions of these documents are available on http://www.e-trust.be/CPS/QNCerts.</p> <p>The applicant for the Certificate must duly complete and sign the order form. By signing the Order Form, the person applying for the Certificate and the company (or organization) accept the General Terms and Conditions, the CP and CPS.</p> <p>The person applying for the Certificate must go in person to the RA authorized under this CP (see Section D.1(5)). The person applying for the Certificate must arrange a meeting with an RAO and go there in person, taking the following documents.</p> <ul style="list-style-type: none"> • The order form, duly filled in and signed; • A (two-sided) copy of the applicant's valid identity card, passport or equivalent official document. The copy must be signed by the person applying for the Certificate; • the electronic application for the Certificate on diskette, CD-ROM or USB-Stick, containing the key pair to be certified; • A (double-sided) copy of a valid ID card, passport or any equivalent official document of the company's (or organization's) legal representative or duly appointed proxy. The copy must be signed by the legal representative of the company (or organization) or by his/her duly appointed proxy; • A copy of the current official memorandum and articles of association of the company/organization you officially represent, or, failing this, an excerpt from the register of companies or any other valid official documents, including the relevant excerpts from the Belgian Official Gazette or a similar document. • If the person presenting himself to the LRA and signing the order form (requestor part) is acting on behalf of the legal representative of the Organisation, the Organisation shall submit proof of the fact that this person is duly authorized to sign for the legal representative. <p>The Customer must make an appointment with the RAO at the RA of his/her choice authorized under this CP (see Section D.1(5)).</p> <p>The RAO verifies the documents received and checks the following:</p> <ul style="list-style-type: none"> • the identity of the person applying for the Certificate, based on the latter's identity papers; • on the basis of proof submitted by the person applying for the Certificate, the data to be certified in relation to the company or organization being certified. 	

Section		Ref. RFC 2527
	<p>If the application is validated, the RAO collates all the documents submitted to create a Registration File on the Certificate holder. The RAO then ensures that one copy is securely archived and prepares the original for secure transmission to the CSP, where it will be held.</p> <p>A posteriori validation</p> <p>A check of the file is performed, a posteriori, by the CSP Certification Authority Auditor (CAA). The information in the issued Certificates is checked to ensure that it corresponds with that in the files received.</p>	
H.	<i>Issuing and delivery of the Certificate</i>	4.2
	The RA will hand over the certificate to the certificate holder on appropriate media.	
I	<i>Acceptance and publication of the Certificate</i>	4.3
	<p><i>Publication of the Certificate in the CSP Public Register of Certificates</i></p> <p>Once the Certificate has been issued by the CSP, it is immediately published in the CSP Public Register of Certificates. This is in the public domain and is accessible at all times (http://www.certipost.be/en/x500).</p> <p><i>Acceptance</i></p> <ul style="list-style-type: none"> • The Certificate holder must agree to the publication of the digital Certificate in the CSP Public Register of Certificates immediately on creation. • The Certificate is deemed to have been accepted by the Certificate holder, as the case may be, on the eighth day after its publication in the CSP Public Register of Certificates or its first use by the holder, whichever occurs first. In the intervening period, the Certificate holder is responsible for checking the accuracy of the content of the Certificate published. The Certificate holder must immediately notify the CSP of any inconsistency he/she has noted between the information in the contractual agreement and the content of the Certificate. The CSP then revokes the Certificate and takes the appropriate measures to reissue a Certificate. This is the sole recourse available to the Customer if the Certificate in the event of non-acceptance on his/her part. 	
J	<i>Procedure for Suspension/Reinstatement after Suspension /Revocation</i>	4.4
	<p>The Certificate holder, the legal representative (or his duly appointed proxy) of the company/organization, the RA or Certipost may apply for suspension, reinstatement following suspension or revocation of the Certificate. The Certificate holder and, where applicable, the legal representative (or his duly appointed proxy) is notified of the suspension, reinstatement following suspension or revocation of the Certificate.</p> <p>The CSP makes information relating to the status of the suspension or revocation of a Certificate available to all parties at all times, as indicated in Section D1.5 of this document.</p> <p>The form to be used for applying for the suspension/reinstatement following suspension/revocation of the Certificate can be obtained from the Certificate Service Provider.</p> <p>Applications and reports relating to a suspension, reinstatement following</p>	

Section		Ref. RFC 2527
	<p>suspension or revocation are processed on receipt, and are authenticated and confirmed in the following manner.</p> <p>In the case of suspension</p> <ul style="list-style-type: none"> • The applicant must contact the Suspension and Revocation Authority (SRA) of the CSP that issued the Certificate. • The SRA then calls back to obtain confirmation of the application for suspension. • The SRA suspends the Certificate from the date on which the application is received. The form must be sent by fax or by post to the CSP within 14 working days. The Certificate is otherwise reinstated. • The Certificate is suspended for one month. Thereafter, a new application for suspension must be submitted, extending the suspension for one further month. The Certificate is otherwise automatically revoked. <p>In the case of reinstatement following suspension</p> <ul style="list-style-type: none"> • To obtain the application form required for reinstatement following suspension, the applicant must contact the SRA of the CSP that issued the Certificate or use the form appended to the General Terms and Conditions. • The applicant must make an appointment with an RA approved by the CSP and present himself/herself in person with the duly completed form and a (double-sided) signed copy of his/her identity card. • The RAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the RAO immediately transmits it to the SRA. <p>The SRA reinstates the Certificate within 24 hours of receiving the application.</p> <p>In the case of a revocation, the applicant must:</p> <ul style="list-style-type: none"> • Apply for the suspension of the Certificate (see above). • The applicant must contract the SRA to obtain a form applying for the revocation of a Certificate or use the form appended to the General Terms and Conditions. • The applicant must make an appointment with an RA approved by the CSP and present himself/herself in person with the duly completed form and a (double-sided) signed copy of his/her identity card. • The RAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the RAO transmits it to the SRA. The SRA revokes the Certificate, from the date on which the application for revocation is received. • The period of investigation prior to the Certificate being revoked (or reinstated) is no more than 10 working days. • The revocation of a Certificate is definitive. 	
K	<i>Procedure for renewal of keys and Certificates and for updates</i>	
	<p>The CSP ensures that the certificate applications submitted by a Certificate holder who has been duly registered in the past, are complete, valid and authorized. This also applies if a certificate and keys are renewed following a revocation or close to the expiry date, or if there is a change to the data certified. The CSP ensures that:</p> <ul style="list-style-type: none"> • the information used to check the certificate holder's identity is still valid, and, to that end, that the same procedure is followed as that used for the initial registration (see Point G of this CP). • If the CSP changes the General Terms and Conditions, it must communicate those changes to the Certificate holder. 	

Section		Ref. RFC 2527
	<ul style="list-style-type: none"> The CSP never issues a certificate for a previously certified key. For every renewal of a certificate a new key pair will be generated in accordance with point F. 	
L	<i>Protection of privacy and personal data</i>	
	<p>Personal data communicated to Certipost by the applicant are entered into a file held by Certipost nv/SA (Ninovesteenweg 196, B-9320 Erembodegem) and, where necessary, the file held by the RA concerned. <i>The data are used solely for the provision of Certipost services. The Customer has the right to inspect and, where necessary, rectify this data.</i></p>	
M	<i>Complaints and dispute settlement</i>	
	<p>In the event of technical problems relating to the Certificate or complaints about the services provided under this CP, the Certificate holder may contact the CSP helpdesk:</p> <ul style="list-style-type: none"> - Certipost (E-Trust) <ul style="list-style-type: none"> - Telephone number: 070 22 55 33 - Fax number: 070 22 55 01 - E-mail address: feedback.nl@contact.certipost.be feedback.fr@contact.certipost.be <p>In the event of disputes relating to the validity, interpretation or performance of the Agreement concluded between them, the CSP and the Certificate holder must make every endeavor to find an amicable solution. If no amicable solution can be found, any dispute concerning the validity, interpretation or performance of the Agreement binding the parties must be brought before the courts of Brussels.</p>	