Certificate Policy for

Normalised E-Trust

SSL WebServer Certificates

Version 1.2

Date published: March 2004

Certificate Policy for Normalised E-Trust Secure Socket Layer Web Server Certificates

This document describes the applications for which certificates, in the form of a Normalised E-Trust Secure Socket Layer (SSL) Web Server 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 E-Trust SSL Web Server Certificates that meet the following criteria.

Section		*Ref. RFC 2527*
A	***Detail of the Certificate Policy for Normalised E-Trust SSL Web Server Certificates***	**1.1**
	This type of Certificate provides a high degree of assurance of the electronic identity of a Web Server. It guarantees proper authentication given that the Customer must be present in person when his/her application is registered by a Local Registration Authority (LRA). The Customer is either the legal representative of the company (organization) that is responsible for or the owner of the Web Server URL or a duly authorized representative thereof. The link between the Web Server identity and the public key is certified. This type of Certificate also guarantees that the company (organization) is the owner of, or responsible for, the Web Server. Applications are only accepted if the Customer can show that the Web Server URL belongs to the company (organization). The Certificate provides the highest degree of assurance of proper authentication since the person applying for the Certificate must go to a LRA in person for official registration before a Web Server Certificate can be issued by the Certification Service Provider. 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 the Web Server to the company (organization). A public key certified in this way must be used solely for establishing secure connections between Web Servers and Web customers and for the authentication of Web Servers. The Certificate also complies with the criteria for a **Normalised Certificate** laid down in ETSI technical standard (TS) 102 042. The Certification Service Provider(s) authorized to issue Certificates under this CP specifies (specify) whether it (they) comply 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).	
B	***Identification of the Certificate Policy for Normalised E-Trust Certificates***	
	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. This document sets out and identifies the **Normalised E-Trust Certificate Policy for SSL Web Servers**. The key pair is always generated by the Certificate holder. These Certificates are compatible with, and meet the requirements laid down in,	

Section		*Ref. RFC 2527*
	ETSI TS 102 042. The Certificates issued under this Normalised E-Trust Certificate Policy for SSL Web Servers 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 0.3.2062.7.1.1.1.1.	
C	***Applicability***	**1.3.4**
	• This type of Certificate provides assurance of the electronic identity of a SSL Web Server. 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 the Certificate (described in Sections B and F of 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). The public key certified in this way may only be used for establishing secure connections between Web customers and Web Servers and for the authentication of Web Servers. • Normalised Certificates for SSL Web Servers issued under this CP comply with ETSI TS 102 042.	
D	***Rights, responsibilities and obligations***	***2***
D.1	***Rights, responsibilities and obligations of the Certification Service Provider***	**2.1**
	• The CSP issues X509 v3-compatible Certificates (ISO 9594-8). • The CSP issues certificates amounting to 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. - For the issue of Normalised Certificates: **Certipost SA, via its Certipost E-Trust services** provided through the **Certipost E-Trust Primary Certification Authority (CA) for Normalised Certificates**: - *Certification Practice Statements (CPS):* www.e-trust.be/CPS/QNcerts - *Public Register of Certificates and Certificate Revocation Lists (CRL):* www.e-trust.be/en/x500 - *Statement of compliance:* www.e-trust.be/CPS/QNcerts - *Suspension/Revocation Authority:* 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 LRAs:	

[1] The personal data and completed Certificates delivered to the CSP and LRA are entered into files held by the LRA. 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
	- Belgacom and 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. - The list of Post Offices and other LRAs authorized to register for an electronic MyCertipost account. This list is available on www.e-trust.be/CPS/QNcerts. • 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 data[1] 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	***Rights, responsibilities and obligations of the Certificate Holder***	**2.1.3**
	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. The Certificate holder agrees to this CP. More specifically, the Certificate holder hereby gives his/her acceptance to the following. • The contractual agreement for this type of Certificate is governed by Belgian law. • 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. • 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,	

Section		Ref. RFC 2527

	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:
	  • 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.
	• 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 LRA registration - by the CSP and the LRA 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	

Section		Ref. RFC 2527
	relating thereto, and in this CP (Section D1).	
D.3	***Rights, responsibilities and obligations of the Local Registration Authority (LRA)***	
	The LRA is under a contractual obligation to comply scrupulously with the registration procedures described in the CSP CPS (see Section D.1.5). The LRA guarantees that: – 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. More specifically: – The LRA Operator (LRAO) 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 LRAO 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. – The LRAO also verifies any information relating to the Certificate holder's professional status for the purposes of certification, as indicated in Section E of this document. – If the Certificate holder is an affiliate of a legal person, the LRAO validates the documentation supplied as proof of the existence of this relationship. – The LRAO 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: – 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 of the last Certificate linked to the holder's registration by the LRA. – The validation procedure used by the LRAO 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. The LRA has a contractual obligation to put in place clear and appropriate measures with respect to: • The physical security of the information and, where appropriate, of the systems concerned; • Logical access to any software; • Employees dealing with registration. The classification of and responsibility for this data are of crucial importance, i.e., • 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;	

Section		*Ref. RFC 2527*
	• Physical access to the data (buildings, safes, access controls and conditional access to software, etc.). The LRA 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.	
D.4	***Rights, responsibilities and obligations of the Certificate holder's company (or organization)***	
	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). The company (or organization) must agree to: • the CPS currently in effect drafted by the CSP, which sets out the practices used to provide the Certificates; • this CP for E-Trust Normalised WebServer SSL Certificates. In particular, the company (or organization) must agree to the following: • 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 responsibilities of the CSP. These are set out in the CPS currently in effect, in the contract and this CP (section D).	
D.6	***Rights, responsibilities and obligations of third parties***	
	Third parties who base themselves on Certificates issued in accordance with this CP must: • 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	***Identification and Authentication – Certified information***	**3.1**

Section				Ref. RFC 2527
	The following information is checked (see Section E of this CP: Certificate application procedure) and certified in the E-Trust Normalised Certificate.			
	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	
	Common Name (CN)	Mandatory	Exact and full URL for a Web Server. N.B.: wildcards (* and |) are permitted.	
	Rfc822Name	Mandatory	Certificate holder's e-mail address.	
	Extensions (not critical unless specified otherwise)			
	SubjectAltName-dNSName	Optional	Exact and full second URL for a Web Server. N.B.: wildcards (* and |) are permitted.	
	SubjectAltName-dNSName	Optional	Exact and full third URL for a Web Server. N.B.: wildcards (* and |) are permitted.	
	SubjectAltName-dNSName	Optional	Exact and full third URL for a Web Server. N.B.: wildcards (* and |) are permitted.	
	KeyUsage	Fixed/Critical	Digital Signature, Key Encipherment, Data Encipherment.	
	SubjectPublicKey	Mandatory	Public Key: Key length: minimum 1024 or 2048 bits (RSA); public exponent: Fermat-4 (=010001).	
	CertificatePolicies-policyIdentifier	Fixed	0.3.2062.7.1.1.1.1	
	CertificatePolicies-policyQualifier-userNotice	Fixed	"E-Trust Certificate for Normalised SSL Web Server Certificate. General terms and conditions OID: 0.3.2062.7.1.2.1.1"	
	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).	
	Authority Info Access	Fixed	Access Method=On line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.e-trust.be	
	Other information:			
	Issuer	Fixed	"CN = Certipost E-Trust Primary CA for Normalised Certificates O = Certipost C = BE"	
	Validity	Fixed	1 year, 2 years or 3 years (as indicated in the purchase order)	

Section				Ref. RFC 2527
	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***			
	The key size must be 1024 bits or 2048 bits. ***Key generation by the Certificate holder*** The person applying for the Certificate generates the key pair himself/herself In which case: • 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 LRAO; • or, in the case of registration during the MyCertipost subscription procedure, the person applying for the Certificate may generate the Key Pair and secure electronic application within his/her MyCertipost environment and secure account.			
G	***Certificate-application procedure***			
	In the case of an application filed via a secure MyCertipost account 1. The person applying for the Certificate must first obtain a MyCertipost account, in accordance with the procedures and terms and conditions for such an account. To do this, the person applying for a Certificate must register a priori online via the website http://www.mycertipost.be. He/she must register as self-employed or as a legal person, print and sign the MyCertipost contract and go in person to the accredited MyCertipost registration office. By signing the MyCertipost contract, the person applying for the Certificate and the company (or organization) accept the General Terms and Conditions, the CP and CPS applicable to online applications for a Qualified or Normalised Certificate. 2. The applicant for the Certificate must duly complete and sign the Order Form. (The correct, up-to-date version of the Order Form can be found on http://www.e-trust.be/CPS/QNCerts.) The Order Form will make it possible to certify the data validated during the registration process for the MyCertipost account - with the exception of the e-mail address, which can be added as required - and after receipt of the electronic certificate application (see Step 3) (verification in particular by the Central Registration Authority of whether the URL(s) belongs (belong) to the company/organization that has submitted the application). Throughout this process, the person applying for the Certificate must accept the General Terms and Conditions, the CP and CPS in effect. These documents and the online Certificate application constitute the Agreement. 3. The person applying for the Certificate must fax the duly completed and signed Order Form to the Certipost E-Trust Central Registration Authority or send it by post. Details of the Central Registration Authority are given on http://www.e-trust.be/CPS/QNCerts. 4. The person applying for the Certificate submits his/her electronic Certificate application within the secure MyCertipost environment in PKCS#10 format to the Certipost E-Trust Central Registration Authority. 5. The Certipost E-Trust Central Registration Authority checks the electronic Certificate application and Order Form. The Certipost E-Trust Central			

Section		Ref. RFC 2527

Registration Authority checks whether the URLs for which a Certificate is applied for genuinely belong to the company/organization that has submitted the application.

Validation

Validation is undertaken by the Certification Authority Auditor (CAA), who checks that the Certificates issued and files received by the LRAs are consistent.

In all other cases

The applicant for the Certificate must obtain an Order Form and the General Terms and Conditions for E-Trust Qualified or Normalised Certificates (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 LRA approved by the CSP. The correct versions of these documents are available on http://www.e-trust.be/CPS/QNCerts.

The applicant for the Certificate must duly complete and sign the Order Form. The Order Form falls into two parts:

a. The Requestor Part must be duly completed and signed by the person applying for the Web Server Certificate.
b. The Organization Part must be duly filled in and signed by a legal representative (or his/her duly appointed proxy) of the company (or organization) to which the person applying for the Certificate belongs.

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.

The person applying for the Certificate must go in person to the LRA authorized under this CP (see Section D.1(5)). The person applying for the Certificate must arrange a meeting with an LRAO and go there in person, taking the following documents.

- 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;
- 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 memorandum and articles of association of the company (or organization);
- If the person signing the Order Form is a duly appointed proxy of a legal representative, the applicant for the Certificate must provide proof that this person has the authority to sign on behalf of the legal representative.

The Customer must make an appointment with the LRAO at the LRA of his/her choice authorized under this CP (see Section D.1(5)).

Section		*Ref. RFC 2527*
	Registration and validation by a LRA. The Customer must go, in person, to the LRA where a meeting has been arranged, with the following documents. The LRAO verifies the documents received and checks the following: 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 ownership of the URLs for certification. If the application is validated, the LRAO collates all the documents submitted to create a Registration File on the Certificate holder. The LRAO then ensures that one copy is securely archived and prepares the original for secure transmission to the CSP, where it will be held. **Validation** If the LRA is not connected directly to the CSP Certification Services, the Central Registration Authority (CRA) performs a final validity check, on receipt of the applicant's registration file from the LRAO and of the electronic application for a certificate sent by the customer: To confirm the accuracy of the information provided in the customer's Registration File received from the LRAO, it calls the applicant back by telephone. If it is accepted by the CRA Officer (CRAO), the electronic application for a certificate is sent to the CSP Certification Authority for the Certificate to be issued. If the application for the Certificate is rejected by the CRAO, the latter must inform the applicant and set out the grounds for this rejection. If the LRA is directly connected to the CSP Certification Service, the second check of the file is carried out *a posteriori* by the CSP Certification Authority Auditor (CAA). The CAA verifies that the information on the Certificates issued corresponds to the information in the files transmitted by the LRA. **A posteriori check** A second check of the file is performed, a posteriori, by the CSP CAA. The information in the Certificates issued is checked to ensure that it corresponds with that in the files received from the LRAs.	
H.	***Issuing and delivery of the Certificate***	**4.2**
	In the case of an application filed via a secure MyCertipost account On receipt of the application for a certificate validated by the MyCertipost platform, the CSP Certification Authority issues the certificate and provides it to the certificate holder by placing it in the MyCertipost account. The Certificate is then published in accordance with Section I of this CP. ***In all other cases*** The CRA sends the Certificate by e-mail to the Certificate holder. If the LRA is connected directly to the Certification services, it provides the Certificate to the Certificate holder on a diskette. The Certificate is then published in accordance with Section I of this CP.	
I	***Acceptance and publication of the Certificate***	**4.3**

Section		*Ref. RFC 2527*
	Publication of the Certificate in the CSP Public Register of Certificates 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. *Acceptance* 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.	
Y	***Procedure for Suspension/Reinstatement after Suspension /Revocation***	**4.4**
	The Certificate holder, the legal representative (or his duly appointed proxy) of the company/organization, the LRA 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. 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. 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. Applications and reports relating to a suspension, reinstatement following suspension or revocation are processed on receipt, and are authenticated and confirmed in the following manner. In the case of **suspension** • 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. In the case of **reinstatement following suspension** • To obtain the application form required for reinstatement	

Section		Ref. RFC 2527
	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 LRA 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 LRAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the LRAO immediately transmits it to the SRA. The SRA reinstates the Certificate within 24 hours of receiving the application. In the case of a **revocation**, the applicant must: • 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 LRA 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 LRAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the LRAO 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	***Procedure for renewal of keys and Certificates and for updates***	
	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/or 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: • 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); OR, in the case of a renewal - provided the Certificate holder's keys and Certificate are still valid (i.e., not revoked, suspended or expired) and electronic signature is permitted by the key usage - the CSP accepts applications that are electronically signed using the private key for which the public key is certified, and accompanied by a text, also duly signed electronically, that states that no information in the file has changed since the last application was made. • If the CSP changes the General Terms and Conditions, it must communicate those changes to the Certificate holder. • The CSP only issues a Certificate for a previously certified key if the security of the cryptographic parameters for this key is still adequate and the key concerned has not been compromised.	
L	***Protection of privacy and personal data***	
	Personal data communicated to Certipost by the applicant are entered into a file held by Certipost SA (Willebroekkaai, 22, B-1000 Brussels) and, where necessary, the file held by the LRA concerned. ***The data are used solely for the provision of Certipost services. The Customer has the right to inspect and, where***	

Section		*Ref. RFC 2527*
	necessary, rectify this data.	
M	***Complaints and dispute settlement***	
	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: Certipost (E-Trust) Telephone number: 070 22 55 33 Fax number: 070 22 55 01 E-mail address: feedback.nl@contact.certipost.be 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.	