Certipost E-Trust Services

Certificate Policy

for Normalised E-Trust SSL Web Server and Code Signing Certificates

Version	1.1
Effective date	12 January 2011
Object Identification Number (OID)	0.3.2062.7.1.1.240.1

Certificate Policy for Normalised E-Trust (SSL) Web Server and Code Signing Certificates

This document describes the applications for which certificates, in the form of a Normalised E-Trust Secure Socket Layer (SSL) Web Server Certificate or Code Signing 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 and Code Signing 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 or a Software Object. This type of digital Certificates provides a very high level of assurance regarding to the electronic identity of a (web) server. These certificates are Normalised Certificates for which the issuing is conditioned to verifications either directly or indirectly using means which provides assurance of: - The identity of the requestor; - The requestor's authorization (formal mandate) by a legal representative of the organization to obtain such a certificate; - The server identity (e.g. domain name) belonging to the subscribing organization The requestor is either the legal representative of the organization that is responsible for or the owner of the Web Server URL or the Software Object or a duly authorized representative thereof. The link between the Web Server or the Software Object identity and the public key is certified. This type of Certificate also guarantees that the organization is the owner of, or responsible for, the Web Server or the Software Object. For SSL Web Server Certificates, applications are only accepted if the requestor can show that the Web Server URL belongs to the organization. The certified public key must be used solely for establishing secure connections between Web Servers and Web customers and for the authentication of Web Servers (Web Server Certificate), or for electronic signature of Software Code by the organization (Code Signing Certificate). The Certificate also complies with the criteria for a **Normalised Certificate** laid down in ETSI technical standard (TS) 102 042. The Certification Service Providers (CSPs), authorized to issue Certificates under this CP, indicate whether they claim to comply with the CP and to the relevant regulatory documents or whether they have been certified to be compliant (see section D1.4 of this document).	

Section		*Ref. RFC 2527*
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 and Code Signing Certificates**. The key pair is always generated by the Certificate Holder. No copy of the private key is provided nor archived by the CSP. These Certificates are compatible with, and meet the requirements laid down in, ETSI TS 102 042. The Certificates issued under this Normalised E-Trust Certificate Policy for SSL Web Servers and Code Signing Certificates 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: **Normalised E-Trust Certificate for SSL Webserver** SSL Web server identity Key length 1024 bits Key generation by Owner: **0.3.2062.7.1.1.241.1** Status: Issuance stopped in January 2011 Key length 2048 bits Key generation by Owner: **0.3.2062.7.1.1.243.1** Key length 4096 bits Key generation by Owner: **0.3.2062.7.1.1.245.1** **Normalised E-Trust Certificate for Code Signing** Software object authentication Key length 1024 bits Key generation by Owner: **0.3.2062.7.1.1.242.1** Status: Issuance stopped in January 2011 Key length 2048 bits Key generation by Owner: **0.3.2062.7.1.1.244.1** Key length 4096 bits Key generation by Owner: **0.3.2062.7.1.1.246.1** Table 1	
C	***Applicability***	**1.3.4**
	1. **SSL Web Server Certificate:** This type of Certificate provides assurance of the electronic identity of a SSL Web Server or an organization. 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	

Section		*Ref. RFC 2527*
	and interactions with public institutions. 2. **Code Signing Certificate:** This type of Certificate provides assurance of the electronic identity of an organization. It can therefore be used to digitally sign a software code authenticating the software object as issued by the organization. 3. 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). 4. 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, or for the electronic signature of Software Code. 5. Normalised Certificates for SSL Web Servers or Code Signing 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**
	1. The CSP issues X509 v3-compatible Certificates (ISO 9594-8). 2. 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. 3. 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. 4. 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:* +32(0)70/22.55.01 (available 24 hours a day, seven days a week). Suspension/revocation form available from the following address: www.e-trust.be/CPS/QNCerts 5. To register persons applying for a Certificate, the CSP uses the following approved Registration Authorities (RA's): - Certipost personnel authorized by the CSP to act as Central Registration Authority. The authenticated list of approved persons is available on www.e-trust.be/CPS/QNcerts**.** - Contractually bound organizations that will act as LRA for the provision of authenticated Certificate applications files. 6. 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	

Section		*Ref. RFC 2527*
	provisions of this CP, the verification procedures, and the CPS then in effect. 7. See Sections 2.1, 2.2 and 2.3 of the CSP CPS applying to the additional rights, responsibilities and obligations of the CSP. 8. 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). 9. 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 organization responsible for the Certificate may consult and request to change this data. The CSP must clearly specify the customer's right to privacy on its Certificate subscription contracts. 10. 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: 1. The contractual agreement for this type of Certificate is governed by Belgian law. 2. 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. 3. In using the Key Pair, the Certificate Holder must comply with any limits indicated in the Certificate or in contractual agreement. 4. 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 2048 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. 5. 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. 6. 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	

Section		*Ref. RFC 2527*
	Certificate Holder. 7. 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. 8. The Certificate is then revoked immediately. The suspension and revocation procedures are set out in Section J of this document. 9. 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. 10. 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. 11. 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. 12. 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. 13. 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. 14. 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. 15. 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	***Rights, responsibilities and obligations of the Registration Authority (RA)***	
	The RA obligations apply as well to the Central Registration Authority (CRA) located at Certipost E-trust as to the Local Registration Authority (LRA) or any other entity that undertakes to identify and authenticate Subscribers on behalf of a CA. The LRA is under a contractual obligation to scrupulously follow the registration procedures and the RA obligations hereunder: **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	

Section		*Ref. RFC 2527*
	in accordance with section 3 through 6 of this CPS, this CP and the Certipost E-Trust RA Procedures and Guidelines. **b) Maintain Certificate application information** -- The RA is obliged to keep, for **30 years** after the expiry of the last certificate, corresponding to this registration, supporting evidence for any Certificate request made to a CA (e.g., Certificate request forms) in accordance to the CPS. In particular a copy is archived of all information used to verify the identity of the Certificate Holder and any references to his professional status, including any reference numbers on the documentation submitted for verification, and any limitations of its validity together with a copy of the contractual agreement signed by the Certificate Holder, including all obligations incumbent on him. **c) CPS, CP's and Certipost E-Trust RA Procedures and Guidelines provisions compliance** -- The RA is obliged to comply with all provisions in the CPS and this CP and the Certipost E-Trust RA Procedures and Guidelines. **d) Protection of RA's PSE** -- The RA is obliged to protect its Private Key in accordance with the provisions of sections 4 through 6 of the 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 the CPS, this CP and the Certipost E-Trust RA Procedures and Guidelines. **f) Identification and authentication –** The RA shall assure that the 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 and that applications for Certificates submitted to the CSP are complete, accurate, valid and duly authorized. The RAO shall check the identity of the Certificate Holder on the basis of valid identity documents recognized under Belgian law. These documents shall indicate a.o. 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. **g) Informing the Subscribers** -- The RA shall inform the Subscriber 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 approved by the Certificate Holder. **h) Professional status** -- The RA shall also verify any information relating to the Certificate Holder's professional status for the purposes of certification. If the Certificate Holder is an affiliate of a legal person, the RAO shall validate the documents supplied as proof of the existence of this relationship. **i) Protection of personal data** – The RA shall comply with the requirements on the protection of personal data in connection with Certificate registration procedures. **j) Data protection** -- The RA takes appropriate measures to assure the physical security of the registration information and, where appropriate, of the systems; the logical access to any software; and the security awareness of the employees in charge or registration. **k) Data classification** – The RA recognizes the crucial importance of the registration data and ensure that this data is 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. This covers: • 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.	

Section		*Ref. RFC 2527*
	• 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.).	
D.4	***Rights, responsibilities and obligations of the Certificate Holder's or organization***	
	The 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 organization. The 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 SSL Web Server and Code Signing Certificates. • the General Terms and Conditions (GTC) for Certipost E-Trust Qualified, Normalised or Lightweight Certificates In particular, the organization must agree to the following: • The Agreement between the organization, the Certificate Holder and the CSP being governed by Belgian law; • Assumption of all the Certificate Holder's responsibilities specified in the CPS, CP and GTC. • Being responsible for the accuracy of the data it transmits to the CSP for the purposes of registration of the Certificate Holder. The 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 organization by an appropriate means). • The 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 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.)	

<table>
<tr><td>Section</td><td colspan="3"></td><td>Ref. RFC 2527</td></tr>
<tr><td></td><td colspan="3">• 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.</td><td></td></tr>
<tr><td>E</td><td colspan="3">Identification and Authentication – Certified information</td><td>3.1</td></tr>
<tr><td></td><td colspan="3">The following information is checked (see Section E of this CP: Certificate application procedure) and certified in the E-Trust Normalised Certificate.</td><td></td></tr>
<tr><td></td><td>Attribute</td><td>Mandatory/
Optional/Fixed</td><td>Value</td><td></td></tr>
<tr><td></td><td colspan="3">Distinguished Name :</td><td></td></tr>
<tr><td></td><td>Country (C)</td><td>Mandatory</td><td>Country in which the organization’s registered office is established[i]</td><td></td></tr>
<tr><td></td><td>Locality (L)</td><td>Mandatory</td><td>Location in which the organization’s registered office is established[i]</td><td></td></tr>
<tr><td></td><td>Organisation (O)</td><td>Mandatory</td><td>The official name of the organization to which the Certificate Holder belongs[i]</td><td></td></tr>
<tr><td></td><td>Organisational Unit (OU)</td><td>Optional</td><td>Organizational unit or department</td><td></td></tr>
<tr><td></td><td>Common Name (CN)</td><td>Mandatory</td><td>SSL Web Server Certificate:
Exact and full URL for a Web Server.

Code Signing Certificate:
The official name of the organization to which the Certificate Holder belongs[i]</td><td></td></tr>
<tr><td></td><td>Rfc822Name</td><td>Mandatory</td><td>Certificate Holder’s e-mail address.</td><td></td></tr>
<tr><td></td><td colspan="3">Extensions (not critical unless specified otherwise)</td><td></td></tr>
<tr><td></td><td>SubjectAltName-dNSName</td><td>Optional</td><td>Exact and full URL for a Web Server</td><td></td></tr>
<tr><td></td><td>SubjectAltName-dNSName</td><td>Optional</td><td>Exact and full second URL for a Web Server</td><td></td></tr>
<tr><td></td><td>SubjectAltName-dNSName</td><td>Optional</td><td>Exact and full third URL for a Web Server</td><td></td></tr>
<tr><td></td><td>KeyUsage</td><td>Fixed/Critical</td><td>SSL Web Server:
Digital Signature, Key Encipherment, Data Encipherment.</td><td></td></tr>
</table>

[i] as stated in the official bylaws of the Organization

Section				*Ref. RFC 2527*
			Object Signing: Digital Signature.	
	SubjectPublicKey	Mandatory	Public Key: Key length: 1024, 2048 or 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
	CertificatePolicies-policyIdentifier	Fixed	**SSL Web Server – key length 1024 bit** 0.3.2062.7.1.1.241.1 – Issuance stopped in Jan 2011 **Object Signing – key length 1024 bit** 0.3.2062.7.1.1.242.1 – Issuance stopped in Jan 2011 **SSL Web Server – key length 2048 bit** 0.3.2062.7.1.1.243.1 **Object Signing – key length 2048 bit** 0.3.2062.7.1.1.244.1 **SSL Web Server – key length 4096 bit** 0.3.2062.7.1.1.245.1 **Object Signing – key length 4096 bit** 0.3.2062.7.1.1.246.1	
	CertificatePolicies-policyQualifier-userNotice	Fixed	**SSL Web Server:** "E-Trust Certificate Policy for Normalised Certificates for Web Servers. Not supported by SSCD, Key generation by Owner. GTC, CP and CPS: www.e-trust.be/CPS/QNCerts" **Object Signing:** "E-Trust Certificate Policy for Normalised Certificates for Object Signing. 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	http://crl.e-trust.be/NCA_WSOS.crl	
	Other information:			
	Issuer	Fixed	"CN = Certipost E-Trust Primary CA for Normalised Certificates O = Certipost C = BE"	
	Validity	Fixed	Up to 5 years	
	SerialNumber	Mandatory	Certificate sequence number	
	Algorithm	Fixed	"Sha1withRSAEncryption"	
	Version	Fixed	2 (in accordance with v3)	

Section		*Ref. RFC 2527*
	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 2048 bits or 4096 bits. Issuance of certificates based on 1024 bits keys ended in January 2011. ***Key generation by the Certificate Holder.*** The person applying for the Certificate generates the key pair himself/herself. In accordance with the Order Form, he/she must provide a PKCS#10 application for the Certificate when registering with the RAO.	
G	***Certificate-application procedure***	
	The applicant for the Certificate must submit a formal request (which could be based on an online form) and accept the GTC from the CSP (see Section D.1.5.) These together with the CP and CPS constitute the Agreement. The person applying for the Certificate must provide the RA authorized under this CP (see Section D.1.5) with the following: • the formal request which provides the acceptance of the General Terms and Conditions, the CP and CPS from the applicant and the applicant's organization and • in case applying for a SSL Web Server certificate: a proof that the URL to be certified is owned by the organization of the applicant (e.g. an excerpt from the domain name registration agent) and • a two-sided copy of the identity document of the applicant. The copy must be signed by the person applying for the certificate and • a signed copy of the bylaws of the applicant's organization and • the electronic application for the Certificate (PKCS#10 file) delivered to the RA as specified in the CPS section 6.1.3. In case the name of the applicant is not mentioned in the bylaws of the organization, in addition: • a signed (two-sided) copy of the identity document of the person entitled to represent the organization and • a signed mandate from this person indicating that the applicant is authorized to acquire the SSL web server or Code Signing certificate for the organization. ***Registration and validation by a RA:*** The RAO will based on the received documents verify the following:	

Section		*Ref. RFC 2527*
	• the identity of the applicant and • the authorization of the applicant to obtain the certificate (directly or indirectly via the provided mandate) and • in case applying for a SSL Web Server certificate: that the organization is owner of the domain name specified in the URLs to be certified 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. ***Validation*** The CSP performs a second validation of the file which 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 received from the RAs.	
H	***Issuing and delivery of the Certificate***	**4.2**
	The RA sends the Certificate by e-mail to the Certificate Holder. The Certificate is then published in accordance with Section I of this CP.	
I	***Acceptance and publication of the Certificate***	**4.3**
	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.	

Section		*Ref. RFC 2527*
J	***Procedure Certificate Suspension, Unsuspension and Revocation***	**4.4**
	The Certificate Holder, the legal representative (or his duly appointed proxy) of the organization, the RA or Certipost E-Trust may apply for suspension, unsuspension or revocation of the Certificate. The Certificate Holder and, where applicable, the legal representative (or his duly appointed proxy) is notified of the suspension, unsuspension 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 D1.4 of this document. The form of the CSP to be used for applying for the suspension/unsuspension or revocation of the Certificate can be obtained from the RA. Applications and reports relating to a suspension, unsuspension or revocation are processed on receipt, and are authenticated and confirmed in the following manner. In the case of **suspension**: a) The applicant shall notify, either by phone, by e-mail or by fax, the Suspension and Revocation Authority (SRA) of the CSP which issued the concerned Certificate. b) The SRA shall then immediately suspend the Certificate, as from the date on which the application is received and send the Suspension, unsuspension and revocation form to the applicant. c) The applicant shall fill-out the form to formalize the suspension and send it by fax or by post to the CSP which issued the concerned Certificate within 14 working days, failing which the Certificate will be unsuspended. d) When confirmed, the suspension of a Certificate shall be so for an unlimited period of time. In the case of **unsuspension**: a) To obtain the form required for unsuspension, the applicant shall contact the Suspension and Revocation Authority of the CSP which issued the Certificate. b) The applicant shall fill-out the form to formalize the unsuspension and sent it by fax or by post to the CSP which issued the concerned Certificate together with a signed two-sided copy of its identity document. In case the name of the applicant is not mentioned in the bylaws of the organization, in addition: • a signed (two-sided) copy of the identity document of the person entitled to represent the organization and • a signed mandate from this person indicating that the applicant is authorized to unsuspend the SSL web server or Code Signing certificate for the organization. c) The RAO shall then validate the unsuspension request and if valid, the RAO shall immediately transmit it to the SRA. d) The SRA shall then unsuspend the Certificate within 24 hours of receiving the application. In the case of **revocation**, the applicant shall:	

Section		*Ref. RFC 2527*
	a) Request the suspension of the Certificate (see above); b) To obtain the form required for revocation, the applicant shall contact the Suspension and Revocation Authority of the CSP which issued the Certificate. c) The applicant shall fill-out the form to formalize the revocation and sent it by fax or by post to the CSP which issued the concerned Certificate together with a signed two-sided copy of its identity document. In case the name of the applicant is not mentioned in the bylaws of the organization, in addition: a. a signed (two-sided) copy of the identity document of the person entitled to represent the organization and b. a signed mandate from this person indicating that the applicant is authorized to revoke the SSL web server or Code Signing certificate for the organization. d) The RAO shall then verify the documents submitted and the identity of the applicant. e) In case of a valid revocation request, the RAO shall immediately transmit it to the SRA. The Certificate shall be revoked (or unsuspended) after a period of investigation of a maximum of 10 working days. f) **Revocation of a Certificate shall be 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 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). • If the CSP changes the General Terms and Conditions, it must communicate those changes to the Certificate Holder. • 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	***Protection of privacy and personal data***	
	Personal data communicated to Certipost by the applicant are entered into a file held by Certipost s.a./n.v. (Exploitation office: Ninovesteenweg, 196, B-9320 Erembodegem (Aalst), Legal office: Centre Monnaie, 1000 Brussels) and, where necessary, the file held by the RA concerned. The data are used solely for the provision of Certipost services. The Customer has the right to inspect and, where necessary, rectify this data.	

Section		*Ref. RFC 2527*
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 Services** Telephone number: +32(0)70 22 55 33 Fax number: +32(0)70 22 55 01 e-mail address: complaints@certipost.com 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.	