Certificate Policy for

Lightweight E-Trust

Certificates for Business Physical Persons

Version 1.0

Date published: February 2005

Certificate Policy for Lightweight Certipost E-Trust Certificates for Business Physical Persons

This document describes the applications for which certificates, in the form of a Lightweight Certipost E-Trust Certificate for Business Physical Persons (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 Lightweight Certipost E-Trust Certificates

for Business Physical Persons that meet the following criteria:

Section		*Ref. RFC 2527*
A	***Detail of the Certificate Policy for Lightweight Certipost E-Trust Certificates for Business Physical Persons***	**1.1**
	This type of Certificate provides a medium degree of assurance of the electronic personal and the professional identity of the Certificate Holder. A remote request procedure provides a medium level of guarantee on the link between the identity of the Certificate Holder and his/her public key. This certificate policy is a "Lightweight Certificate Policy" (LCP) as specified by ETSI standard ETSI TS 102 042. For Certificate applications to be validated, the person applying for the Certificate must provide, for verification, his/her identity card and a proof of his/her professional status. The Certification Service Provider(s) authorised 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 Lightweight E-Trust Certificates for Business Physical Persons***	
	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 **Lightweight E-Trust Certificate Policy for Business Physical Persons**. These Certificates are compatible with, and meet the requirements laid down in ETSI TS 102 042 (LCP). The Certificate Holder is either responsible for the generation of the Private Key and Public Key or this Key Pair generation is performed by the CSP on behalf of the Certificate Holder. The Certificates issued under this Lightweight E-Trust Certificate Policy for Business Physical Persons 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 0.3.2062.7.1.3.12.1.	
C	***Applicability***	**1.3.4**
	• This type of Certificate provides medium level assurance of the electronic identity of a Business Physical Person. It can therefore also be used to protect medium-level applications in a client/server, browser/server model, such as medium value commercial transactions, web based on-line shopping of medium value, extranets-intranets, signing of e-invoices, … while certifying the identity of the Certificate Holder. • 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). Lightweight Certificates for physical persons issued under this CP comply with ETSI TS 102 042.	

Section		Ref. RFC 2527
D	***Rights, responsibilities and obligations of the Parties***	***2***
D.1	***Rights, responsibilities and obligations of the Certification Service Provider***	**2.1**
	• The CSP issues X.509 v3-compatible Certificates (ISO 9594-8). • The CSP issues Certificates amounting to Lightweight 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 Lightweight Certificates: **Certipost sa/nv, 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 (Central) – (Local) Registration Authorities (CRAs/LRAs): - 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**.** - Contractually binded organizations that will act as LRA for the provision of authenticated Certificate applications files. • In case 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 TS 102 042. • 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 related 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 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.	

[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,

Section		Ref. RFC 2527
	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 provided 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.
	• In case 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.
	• 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:
	  o The Private Key of the Certificate holder is lost, stolen or potentially compromised; or,
	  o 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,
	  o 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.	

where applicable, ask that it be rectified or deleted.

Section		Ref. RFC 2527
	• The Certificate Holder 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 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	***Rights, responsibilities and obligations of the Registration Authority (RA)***	
	The RA is under a contractual obligation to comply scrupulously with the registration procedures described in the CSP CPS (see Section D.1.5). The RA 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 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 Certificate Holder (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. – The RAO 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 RAO validates the documentation supplied as proof of the existence of this relationship.	

Section		Ref. RFC 2527
	– 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: – A copy of all information used to check the identity of the Certificate Holder 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 RA. – 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. The RA 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; • Physical access to the data (buildings, safes, access controls and conditional access to software, etc.). 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.	
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 provided by the CSP, which sets out the practices used to provide the Certificates; • this CP for E-Trust Lightweight 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)	

<table>
<tr><td>Section</td><td></td><td>Ref. RFC 2527</td></tr>
<tr><td></td><td>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).</td><td></td></tr>
<tr><td>D.5</td><td>Rights, responsibilities and obligations of third parties</td><td></td></tr>
<tr><td></td><td>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 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.</td><td></td></tr>
<tr><td>E</td><td>Identification and Authentication – Certified information</td><td>3.1</td></tr>
<tr><td></td><td>The following information is checked (see Section G of this CP: Certificate application procedure) and certified in the E-Trust Lightweight Certificate.
<table>
<tr><td><u>Attribute</u></td><td><u>Mandatory/ Optional/Fixed</u></td><td><u>Value</u></td></tr>
<tr><td colspan="3">Distinguished Name :</td></tr>
<tr><td>Country (C)</td><td>Mandatory</td><td>Nationality of the Certificate Holder (Country)</td></tr>
<tr><td>Locality (L)</td><td>Mandatory</td><td>Place of birth of the Certificate Holder (Locality)</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, department and/or registration number.</td></tr>
<tr><td>Organisational Unit (OU)</td><td>Mandatory</td><td>“Professional status:<…>”
Either :
– Self employed
– Administrator
– C.E.O.
– Manager
– Employee
Or
Another professional status, if the necessary proof is delivered, during registration</td></tr>
</table></td><td></td></tr>
</table>

Section				Ref. RFC 2527
	Organisational Unit (OU)	Mandatory	"Date of birth: <dd/mm/yyyy>" (date of birth of the Certificate Holder (dd/mm/yyyy))	
	Common Name (CN)	Mandatory	Last name and first name (s), exactly as indicated on the identity card	
	Rfc822Name	Mandatory	Certificate Holder's e-mail address.	
	Extensions (not critical unless specified otherwise)			
	KeyUsage	Fixed/Critical	"Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment"	
	SubjectPublicKey	Mandatory	Public Key: Key length: 1024 or 2048 bits (RSA); public exponent: Fermat-4 (=010001).	
	CertificatePolicies-policyIdentifier	Fixed	0.3.2062.7.1.3.12.1	
	CertificatePolicies-policyQualifier-userNotice	Fixed	"E-Trust Certificate Policy for Lightweight Certificates for physical person. General terms and conditions OID: 0.3.2062.7.1.2.6.1"	
	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, 2 or 3 years, as indicated in the purchase order	
	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. ***In the case of CSP generating the key pair*** In case 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 TS 102 042. ***In the case of Certificate Holder generating the key pair*** In this case, the candidate Certificate Holder proceeds to the key pair generation. It is the responsibility of the Certificate Holder to perform this generation in a secured way and such that the privacy of the private key is ensured according to the technical standard TS 102 042.			

Section		Ref. RFC 2527
G	***Certificate-application procedure***	
	Where the MyCertipost certificate issuing procedure is followed: To obtain a certificate, the Certificate Holder shall – in his/her personal MyCertipost secure environment, accessible using his/her relevant codes - send his electronic certificate request. Together with this electronic request, the Certificate Holder shall send via fax or postal mail the duly filled-in and signed purchase order, together with a proof that the URL's to be certified are owned by the requester of the certificate. ***Via the www.e-trust.be website :*** To obtain a Lightweight E-Trust Certificate via the E-Trust website, the Certificate Holder must proceed to the four step procedures available on the web site: • Step 1 : Fill in the electronic request form • Step 2 : Print the electronic request form • Step 3 : Send the electronic request forms and other required documents to Certipost E-Trust in order to prove his/her professional status • Step 4 : Install the issued Certificate To get his/her Lighweight Certipost E-Trust Certificate, the Certificate Holder, as well as his/her organisations' legal representative must sign this printed request form. After the signing of this document, the Certificate Holder must send this signed printed request form via fax or postal mail to Certipost E-Trust, together with the other required documents. The other required documents include : - A recto-verso signed copy of the Certificate Holder's valid identity card - A recto-verso signed copy of the identity card of the legal representative of the Certificate Holder organisation - A copy of the statutes of this organisation These documents has to be sent to Certipost E-Trust : - Either via fax : 053/60 11 02 - Either via Postal Mail : Certipost E-Trust Customers Services Ninovesteenweg 196 9320 Erembodegem (Aalst) ***In the case of an application filed via "Bulk LRA procedure"*** In this case, it is up to the LRA to ensure the collection of the Certificate applicants and potentially their Organisation's consent and information required for the completion of the Certificate Registration File. Once this has been done, the LRA securely sends the Bulk Registration File to the CRA of the CSP, which proceeds to the issuing of the certificates. **A posteriori check** A check of the file is performed, a posteriori, by the CSP Certification Authority Auditor (CAA). The information in the Certificates issued is checked to ensure that it corresponds with that in the files received.	

Section		Ref. RFC 2527
H.	***Issuing and delivery of the Certificate***	**4.2**
	In the case of Certificate Holder generating the key pair The CRA sends the Certificate to the Certificate Holder under appropriate format for installation by the Certificate Holder.. ***In the case of CSP generating the key pair on behalf of the Certificate Holder*** The CRA sends the Certificate (containing the private key) and the password to decrypt the private key, to the Certificate Holder via 2 different secured ways. 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 Certificate Holder if the Certificate in the event of non-acceptance on his/her part.	
J	***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 RA or Certipost E-Trust 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 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 (form appended to the General Terms and Conditions).. 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.	

Section		Ref. RFC 2527
	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 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 SRAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the SRAO 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 SRAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the SRAO 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	

Section		Ref. RFC 2527
	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 (Ninovesteenweg, 196, B-9320 Erembodegem (Aalst)) 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.	
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 feedback.fr@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.	