Certipost E-Trust Services

Certificate Policy for Lightweight E-Trust Certificates for Communities

Version 1.1

Effective Date:
December 2009

Certificate Policy for Lightweight Certipost E-Trust Certificates for Communities

This document describes the applications for which certificates, in the form of a Lightweight Certipost E-Trust Certificate for Communities (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 Communities that meet the following criteria:

Section		*Ref. RFC 2527*
A	***Detail of the Certificate Policy for Lightweight Certipost E-Trust Certificates for Communities***	**1.1**
	This type of digital Certificates provides a reasonable level of assurance with regard to the electronic personal and professional identity of the Certificate Holder in the context or while acting as a member of a specific Community. Evidence of the identity shall be checked against a physical person either directly or indirectly using means which do not necessarily provide equivalent assurance to physical presence. These Certificates provide a reasonable level of assurance to guarantee the link between the personal identity, his/her Public Key, its authorized usage and the information related to the professional qualification of the member of a specific Community, who is subject of the Certificate. The validation of the request will demand the provision of the proof of the identity of the applicant as a member of a specific Community and the verification of the pieces guaranteeing his quality(ies) and the related information that have to be certified. The so certified Public Key can only be used in context of any usage except Qualified Digital Signature (e.g., normalised digital signature, encryption and/or authentication, or any combination of these, etc.). In such a case, the Lightweight Certificate satisfies the requirements in the sense of the technical standard ETSI 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). This Certificate type constitutes a reasonable level of professional electronic identity that can be used to secure applications requiring electronic signature operations or encryption/authentication performed in the context of a specific Community. The Certificates issued under this CP include one or several CP identifiers that can be used by relying parties in order to determine the applicability and the trustworthiness of the Certificate in relation with a specific application. This CP satisfies specific requirements for Physical Persons in relation to the Community: – Obligation for the member of a specific Community applying to be a Certificate Holder to register through a Registration Authority (RA) certified and trained by Certipost E-Trust and the Community, if applicable.	

Section		*Ref. RFC 2527*
	– Obligation for the member of a specific Community applying to be a Certificate Holder to provide the RA with identification proofs as required in the CP and related to its quality(ies) in respect to the Community. – Allowed ability for the Community, via the certified RAs, to be involved in the revocation/suspension process, in case applicable.	
B	***Identification of the Certificate Policy for Lightweight E-Trust Certificates for Communities***	
	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 Communities**. These Certificates are compatible with, and meet the requirements laid down in ETSI TS 102 042 (LCP). The CSP, on behalf of the Certificate Holder is responsible for the generation of the Private Key and Public Key. The Certificates issued under this Lightweight E-Trust Certificate Policy for Communities have a CP unique identifier (O.I.D.). 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: **Lightweight E-Trust Certificate for Communities** All usage except Qualified Digital Signature Lightweight Certificate without SSCD ETSI TS 102 042: **0.4.02042.1.3** Key generation by CSP: **0.3.2062.7.1.1.311.1** Table 1	
C	***Applicability***	**1.3.4**
	• This type of digital Certificates provides a reasonable level of assurance with regard to the electronic personal and professional identity of the Certificate Holder in the context or while acting as a member of a specific Community. It can therefore be used to protect medium security level applications in a client/server, browser/server model for medium value commercial transactions, extranets-intranets access, e-mail security, document signing etc.. • The applications for which the Certificate is deemed to be trustworthy must be decided by the parties themselves on the basis of the nature of the Certificate and the level of security of the procedures followed for issuing and managing the Certificate as described in this CP. • Key usage and the applicability of the Certificate are certified (see the description of the Certificate content in Section E of this document). Lightweight Certificates for Communities issued under this CP comply with ETSI TS 102 042 (LCP: 0.4.02042.1.3).	
D	***Rights, responsibilities and obligations of the Parties***	***2***
D.1	***Rights, responsibilities and obligations of the Certification Service Provider***	**2.1**
	1. The CSP issues X.509 v3-compatible Certificates (ISO 9594-8).	

Section		*Ref. RFC 2527*
	2. 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 (see applicable CPS). 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 Lightweight Certificates under this CP: - **Certipost s.a./n.v., via its Certipost E-Trust services** provided through the **Certipost E-Trust Secondary LightWeight Certification Authority (CA) for Communities**: - *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 (Central) – (Local) Registration Authorities (CRAs/LRAs) - Certipost personnel authorized by the CSP to act as Registration Authorities. The authenticated list of approved persons is available on www.e-trust.be/CPS/QNcerts**.** - Contractually bound organizations that will act as LRA for the provision of authenticated Certificate applications files. 6. As the CSP proceeds to the key pair generation on behalf of the Certificate Holder, it guarantees that such key pair generation is performed in a secured way and that the privacy of the private key is ensured according to the technical standard ETSI TS 102 042. 7. 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. 8. See RFC 2527 Sections 2.1, 2.2 and 2.3 of the CPS related to the additional rights, responsibilities and obligations of the CSP. 9. 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). 10. 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 change this data[1] The CSP must clearly specify the customer's right to privacy on its Certificate subscription contracts. 11. 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**

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

Section		*Ref. RFC 2527*
	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 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 (RFC 2527 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. password or 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. • 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, or membership to a Community 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	

Section		Ref. RFC 2527
	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 his 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 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 in accordance with section 3 through 6 of the 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 with 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, 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) Quality of the Key Pair Generation** – If the RA generates the Subscribers' keys: to generate their cryptographic key pairs, and to use them properly, the RA is obliged to use reliable technical means that present an adequate security level in order to, among others, prevent or detect any integrity flaw to a piece of data that has been encrypted or decrypted with the keys and to	

Section		Ref. RFC 2527
	prevent or detect any unauthorized usage of a Private Key. In particular, the RA is obliged to generate the Subscribers' keys using a key generation algorithm, a key length, and a signature algorithm recognized as being fit for the purposes of certificate usage. **g) 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. **h) 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. **i) 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. **j) Link between Private and Public key** -- If the key pair is not generated by the CSP or the RA, the validation procedure used by the RA for electronic Certificate applications shall guarantee that the Certificate Holder is in possession of the Private Key linked to the Public Key to be certified. **k) Protection of personal data** – The RA shall comply with the requirements on the protection of personal data in connection with Certificate registration procedures. **l) 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. **m) 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. • 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.). **n) Key archiving and Recovery** -- In case the Certificate Holders' private key is archived, the RA shall assure that: • The Subscriber is duly informed about the fact that his / her private key is archived; • The Certificate Holder's private keys are kept secret and that no other copy of the Certificate Holder's private key is kept beside the one which is stored in the secure archive; • The archived keys of the Certificate Holder are not accessed without the physical presence of the KRO and the required key recovery authorization. • The key recovery request is authorized in a way which guarantees	

Section		*Ref. RFC 2527*
	equivalent assurance of identity and authentication of the Certificate Holder as guaranteed during registration; • The request for key recovery submitted to the CSP are complete, accurate, valid and duly authorized; • The Certificate Holder's certificate should be revoked or should have expired to recover the encryption key; • That an authorized key recovery request is performed under dual control with the physical presence of the KRO. • A Certificate Holder's private key shall only be recovered without the holder's authority for their legitimate and lawful purposes, such as to comply with judicial or administrative process or search warrant, and not for any illegal, fraudulent or other wrongful purpose.	
D.4	***Rights, responsibilities and obligations of the Certificate Holder's Community***	
	The Community represented by its legal representative, must give its consent to the registration of the Certificate Holder for the purposes of obtaining a Certificate attesting his quality(ies) with respect to the Community. The Community 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 Lightweight Certipost E-Trust Certificates for Communities • the General Terms and Conditions (GTC) for Certipost E-Trust Qualified, Normalised or Lightweight Certificates In particular, the Community must agree to the following: • The Agreement between the Community, 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 Community 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 (RFC 2527 Section 4.4), the CSP may revoke or suspend the Certificate (provided that it duly notifies the Certificate Holder and the Community by an appropriate means). • The Community must ask the CSP to suspend or revoke the Certificate as required under the CP and the CPS currently in effect (RFC 2527 Section 4.4). The suspension and revocation procedures are described in the CPS currently in effect (RFC 2527 Section 4.4). • The Community 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.5	***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 of this document.)	

<table>
<tr><td>Section</td><td></td><td>Ref. RFC 2527</td></tr>
<tr><td></td><td>

- 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 Lightweight Certipost E-Trust Certificates for Communities

<table>
<tr><th>Attribute</th><th>Mandatory/ Optional/Fixed</th><th>Value</th></tr>
<tr><td colspan="3">Subject Attributes :</td></tr>
<tr><td>countryName (C)</td><td>Mandatory</td><td>Nationality of the Certificate Holder (Country)</td></tr>
<tr><td>localityName (L)</td><td>Mandatory</td><td>Place of birth of the Certificate Holder (Locality)</td></tr>
<tr><td>organizationName (O)</td><td>Mandatory</td><td>The official name of the organization (or Community) to which the Certificate Holder belongs [2].</td></tr>
<tr><td>organizationalUnitName (OU)</td><td>Optional</td><td>Organizational unit, department and/or registration number.</td></tr>
<tr><td>organizationalUnitName (OU)</td><td>Optional</td><td>Organizational unit, department and/or registration number.</td></tr>
<tr><td>organizationalUnitName (OU)</td><td>Optional</td><td>“Role in the organization : <…>”
Either :
- Self employed
- Administrator
- C.E.O.
- Manager
- Employee
Or
Another professional status statement, if the necessary proof is delivered, during registration</td></tr>
<tr><td>organizationalUnitName (OU)</td><td>Mandatory</td><td>“Date of birth: <dd/mm/yyyy>” (date of birth of the Certificate Holder (dd/mm/yyyy))</td></tr>
<tr><td>commonName (CN)</td><td>Mandatory</td><td>Last name and first name (s), as indicated on the identity card
Optionally the intended use of the certificate could be indicated in the common name between brackets: “ - (Sign)”, “ - (Access)” or “ - (Encrypt)”.</td></tr>
<tr><td>surName</td><td>Optional</td><td>Certificate Holder’s surname</td></tr>
<tr><td>givenName</td><td>Optional</td><td>Certificate Holder’s given name</td></tr>
<tr><td>serialNumber</td><td>Optional</td><td>Certificate Holder’s serial Number or distinctive number (free format)</td></tr>
<tr><td>homePostalAddress</td><td>Optional</td><td>Postal Address of Certificate Holder</td></tr>
<tr><td>emailAddress</td><td>Mandatory</td><td>Certificate Holder’s e-mail address</td></tr>
<tr><td>title</td><td>Optional</td><td>Certificate Holder’s title or professional status statement</td></tr>
<tr><td>initials</td><td>Optional</td><td>Certificate Holder’s initials</td></tr>
<tr><td colspan="3">Subject Alternative Name (subjectAltName)</td></tr>
<tr><td>Rfc822Name</td><td>Mandatory</td><td>Certificate Holder’s e-mail address.</td></tr>
<tr><td colspan="3">Extensions (not critical unless specified otherwise)</td></tr>
<tr><td>KeyUsage</td><td>Fixed/Critical</td><td>“digitalSignature, keyEncipherment, dataEncipherment”</td></tr>
<tr><td>SubjectPublicKey</td><td>Mandatory</td><td>Public Key: Key length: 1024 bits (RSA); public exponent: Fermat-4 (=010001).</td></tr>
<tr><td>CertificatePolicies PolicyIdentifier</td><td>Fixed</td><td>0.3.2062.7.1.1.311.1</td></tr>
<tr><td>CertificatePolicies PolicyIdentifier</td><td>Fixed</td><td>0.4.0.2042.1.3</td></tr>
<tr><td>CertificatePolicies-policyQualifier-userNotice</td><td>Fixed</td><td>“E-Trust Certificate Policy for Lightweight Certificates for Communities. Not supported by SSCD, Key Generation by CSP. GTC, CP and CPS: www.e-trust.be/CPS/QNCerts”</td></tr>
<tr><td>CertificatePolicies-policyQualifier-CPS</td><td>Fixed</td><td>http://www.e-trust.be/CPS/QNcerts</td></tr>
<tr><td>crlDistributionPoint</td><td>Fixed</td><td>http://crl.e-trust.be/LWCA_Com.crl</td></tr>
</table>

</td><td></td></tr>
</table>

[2] As stated in the official bylaws of the Organization

Section				*Ref. RFC 2527*
	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	http://ca.e-trust.be/LWCA_Com.crt	
	Other information:			
	Issuer	Fixed	"CN = Certipost E-Trust Secondary LightWeight CA for Communities O = Certipost s.a./n.v. C = BE"	
	Validity	Fixed	Up to 5 years	
	SerialNumber	Mandatory	Certificate sequence number	
	Algorithm	Fixed	"Sha1withRSAEncryption"	
	Version	Fixed	2 (in accordance with v3)	
	The Certification Authority's signature is appended to this certified information and relates to all of the information certified.			
F	***Key-generation procedure***			
	The key size must be 1024 bits. As the CSP proceeds to the key pair generation on behalf of the Certificate Holder, it guarantees that such key pair generation is performed in a secured way and that the privacy of the private key is ensured according to the technical standard ETSI TS 102 042 (LCP).			
G	***Certificate-application procedure***			
	The applicant for the Certificate must submit a formal request 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 to obtain the Certificate including the identity information of the applicant; and • the acceptance of the GTC, CP and CPS. This acceptance could be provided by the applicant when joining the Community; and • the proof of membership to the Community (e.g. membership number, employee number, …); and • the authorization from a legal representative (or a mandated person) of the Community to obtain the Certificate; and • additional applicant authentication information as required by a specific Community. ***Registration and validation by a RA:*** The RAO will based on the received documents verify the following: • the correspondence between the identity information provided by the applicant and the registered Community membership identity information; and • the authorization of the applicant to obtain the certificate (directly or			

Section		*Ref. RFC 2527*
	indirectly via the provided mandate); and • additional authentication of the applicant as required by a specific Community. 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. ***In the case of an application filed via "Bulk LRA procedure"*** The LRA ensures the collection of the Certificate applicants' consent and potentially their Community'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 issued Certificates is checked to ensure that it corresponds with that in the files received.	
H	***Issuing and delivery of the Certificate***	**4.2**
	After validation of the request the RA requests the CA to issue the Certificate of the applicant. The issued Certificate (containing the private key) is sent by the RA to the Certificate Holder in suspended mode. The password to access the private key is also sent to the Certificate Holder via an alternative way. The Certificate Holder contacts the RA to confirm the receipt and asks for the activation (unsuspension) of the Certificate. The RA unsuspends the certificate after successful authentication of the Certificate Holder. The Certificate is then published in accordance with Section I of this CP. The CSP allows archiving of the Certificate Holders' Private Keys linked to the Certipost E-Trust Certificate for Communities, under the condition that the Subscriber formally agrees with it. This formal agreement for Key Archiving by the CSP should be stated in the Order Form submitted by the Subscribers or specified in the agreement between the LRA and Certipost. In case of the latter all certificates issued by the LRA under this CP will be archived.	
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	

Section		*Ref. RFC 2527*
	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 Certificate Suspension, Unsuspension and Revocation***	**4.4**
	The Certificate Holder, the legal representative (or his duly appointed proxy) of the Community, 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 send it by fax or by post to the CSP which issued the concerned Certificate. c) The RA which issued the Certificate shall authenticate the applicant in the following possible ways: a. By asking the applicant to provide the challenge password. This challenge password is the one provided by the Certificate Holder or the RA during registration. Additionally it should be verified that the applicant is still member of the Community. or b. By identifying the applicant following the same procedure as used during the application procedure (See section G). d) The RAO shall then validate the unsuspension request and if valid, the RAO	

Section		*Ref. RFC 2527*
	shall immediately transmit it to the SRA. e) The SRA shall then unsuspend the Certificate within 24 hours of receiving the application. In the case of **revocation**, the applicant shall: 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. d) The RA which issued the Certificate shall authenticate the applicant in the following possible ways: a. By asking the applicant to provide the challenge password. This challenge password is the one provided by the Certificate Holder or the RA during registration; or b. By identifying the applicant following the same procedure as used during the application procedure (See section G). e) The RAO shall then verify the documents submitted and the identity of the applicant. f) The Certificate shall be revoked (or unsuspended) after a period of investigation of a maximum of 10 working days. g) **Revocation of a Certificate shall be definitive.** Also a legal representative of the Community (or a person mandated by a legal representative) can request revocation of a Certificate. In this case the legal representative of the Community (or a person mandated by a legal representative) shall be authenticated.	
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	***Procedure for Certificate Holders' Private Key Recovery***	
	In case the CSP has archived the Certificate Holders' Private Keys, the recovery of the Private Key can be requested following the same procedure as described for issuance of the Certificate (See section H of this CP). The Order Form should clearly indicate the serial number of the Certificate for which the corresponding Private Key needs to be recovered. The RA shall at any time respect the requirements for Key Recovery as specified	

Section		*Ref. RFC 2527*
	in section D3 of this CP.	
M	***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.	
N	***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@staff.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.	