E-Trust Lightweight Certificate Policy

for the European Commission – IDA Sectoral Networks

(E-Trust IDA LCP)

IMPORTANT FOR RELYING PARTIES: Please read this Certificate Policy carefully prior to certificate usage.
This E-Trust Certificate Policy Document describes the applicability of the certificates issued under this Policy, the procedures that have to be followed and the responsibilities of the parties involved, in accordance with the E-Trust Certificate Practice Statements, hereafter referred to as CPS.

Section		*CPS ref*
A	**Overview of E-Trust Lightweight Certificate Policy for the European Commission – IDA Sectoral Networks (E-Trust IDA LCP).**	1.1
	Medium level Professional digital identity assurance. Remotely requested certificate providing medium level of guarantee for the binding between a Functional Mailbox identity and a public key. This certificate guarantees the identity of the Functional Mailbox and the ownership of the functional mailbox by the Subscriber, who is part of a Company or Organisation. The validation of the request requires evidence of the identity of the Subscriber and evidence that he belongs to the company or organisation. Certificates issued under this policy can only be used in sectoral networks as defined in decisions 1720/1999/EC and 2045/2002/EC of the European Parliament and of the Council. This certificate policy is a "lightweight certificate policy" (LCP) as specified by ETSI standard ETSI TS 102 042.	
B	**Community and Applicability**	**1.3**
	Certification Authority See E-Trust CPS for Qualified and Normalised Certificates. **Registration Authority** The registration process is the responsibility of Local Registration Authority (further called LRA), as assigned by E-Trust. The up to date list of available LRA's, and their contact details, can be found at. http://www.e-trust.be/CPS/IDA **Suspension and Revocation Authority** The LRA will act for this type of certificate as well as Suspension and Revocation Authority (SRA). In case of emergencies, the E-Trust SRA Hotline can also be contacted via 078 / 15 24 70. **Applicability** E-Trust governs this certificate as specified in the CPS. This certificate is only to be used in Sectoral Networks as defined in decisions 1720/1999/EC and 2045/2002/EC of the European Parliament and of the Council. It is the relying party's responsibility to choose the applications for which they trust the certificate, according to the security level of the procedures followed for the certificate issuance (described in section E of the present CP). The key usage and certificate applicability are certified (see certificate content in D).	

Section		*CPS ref*
C	**Rights, liabilities and obligations**	**2**
C.1	**Rights, liabilities and obligations of E-Trust**	**2.1**
	• E-Trust warrants only that its procedures are implemented in accordance with its published current CPS and that any issued certificate that asserts a policy Object Identifier (OID) defined in this CPS was issued in accordance with the stipulations of this CPS and the corresponding Certificate Policy (CP). • See section 2.1, 2.2, and 2.3 of the current E-Trust CPS for additional rights, liabilities and obligations of E-Trust. • In particular cases described in the current CPS (section 4.4), E-Trust has the right to revoke / suspend the Organisation's certificate (encompassing the fact that E-Trust warns and informs the Organisation and the LRA by appropriate means). • Certification Authority (CA) authorised to issue this certificate type: **Certipost E-Trust Primary CA for normalised certificates** as described in the current CPS.	
C.2	**Rights, liabilities and obligations of the LRA**	**2.1.2**
	The Local Registration Authorities are under a contractual obligation to follow scrupulously the registration procedures described in the E-Trust CPS. The LRA guarantees that: • Subscribers receiving a Certificate are correctly identified and authenticated. • Requests for Certificates submitted to the authorised Certification Authority (see section C.1 of the present CP) are complete, accurate, valid and duly authorized. In particular: o The registration officer shall inform the Subscriber of the terms and conditions for the use of the Certificate. These are set out in the Request Form and the General Terms and Conditions to be signed by the requesting Subscriber (paper or notarised electronic format). o The registration officer shall verify the identity of the subscriber on the basis of valid ID papers or passport. o The registration officer shall verify the identity of the representative of the organisation. • The registration officer shall verify the information relating to the Functional Mailbox of the subscriber and the organisation for the purposes of certifying it, as set out in section E of this document. • The registration officer shall safely and securely store one copy of the information provided during the registration procedure, and in particular: o A copy of all information used to verify the identity of the Subscriber; o A copy of the certificate request form signed by the Subscriber and a legal representative of the Organisation; o A copy of the evidence that the person signing on behalf of the Organisation is a legal representative; This data shall be retained for 5 years. • The registration officer shall act as suspension and revocation authority as specified by the CP and the CPS, and act according to the specified procedures and guidelines. • Compliance with the requirements on the protection of personal data in connection with registration procedures is reached. The LRA shall be contractually obliged to take clear and appropriate measures regarding: • The physical security of the information and, where appropriate, of the systems;	

Section		*CPS ref*
	• The logical access to any software; • The employees in charge of registration; The classification of and responsibilities for this data are of crucial importance. This covers the following: • 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; • The items of equipment (hardware, telecommunications tools, etc.) and their configuration; • Physical access to the data (buildings, safes, access controls and conditional access to software, etc.); The LRA shall ensure these items are managed and stored in such a way as to avoid any loss of confidentiality, integrity, availability of this data.	
	Rights, liabilities and obligations of the Subscriber	**2.1.3**
	The Subscriber agrees with the current CPS describing the Practices that are used to deliver E-Trust electronic certificates and edited by E-Trust. The Subscriber agrees with the present Certificate Policy (CP). In particular, the Subscriber accepts that: • The contractual agreement (certificate request form) related to this type of certificate is governed under the Belgian laws • The Subscriber is obliged to protect the private key at all times, against loss, disclosure to any other party, modification and unauthorised use, in accordance with the current CPS and the present CP. From the creation of the private and public key pair on, the Subscriber is solely responsible for the confidentiality and integrity of the private key. Every usage of the private key is assumed to be the act of the Functional Mailbox. The PIN (Personal Identity Number) or pass phrase, used to protect the private key against unauthorised use, shall never be stored in the same location as the private key itself or next to its storage media, and shall never be stored unprotected. The private key must not be left unattended in an unlocked state (i.e., unattended in a workstation when the PIN or pass phrase has been entered). The Subscriber is solely responsible for the usage of the private key; E-Trust is not liable of the usage of the Subscriber's private key. • The Subscriber is responsible for the generation of the key pair for the Certificate. • The Subscriber is responsible for the accuracy of the data he/she transmits to the LRA. • The Subscriber must request the LRA to suspend or revoke the certificate whenever it is required in the current CPS (section 4.4). The suspension and revocation procedures are described in the current E-Trust CPS (section 4.4), and in section H of this CP. • The Subscriber has to inform immediately the LRA on any change in the information included in the certificate. The revocation procedure will be immediately started. • The Subscriber has to inform the LRA of any change in the information that is not included in the certificate, but that has been transmitted to the LRA when registering. The LRA will correct the registered information. • The Subscriber accepts that the electronic certificate will be published in a publicly accessible registry immediately after its creation and that revocation information about the certificate will be published in the E-Trust Certificate Revocation List that is also publicly available. • The Certificate is deemed accepted by the Subscriber within 8 days from	

Section		*CPS ref*
	the issuance or at the moment of its first use, whichever is the earliest. If the Subscriber notices an inconsistency between the contractual agreement information and the content of his/her Certificate, he/she must inform the LRA without any delay. The LRA will then revoke the Certificate and take the appropriate measures to re-issue a certificate. This will be the Subscriber's sole remedy for any acceptance refusal. • The Subscriber agrees with the rights, obligations and liabilities of E-Trust and the LRA. These are described in the current CPS, the Certificate Request Form, and in the present CP (section C). • The Subscriber agrees that E-Trust and the LRA have the right to revoke / suspend the Organisation's certificate in particular cases described in the current CPS (section 4.4). The LRA warns and informs the Subscriber when this happens.	
	Rights, liabilities and obligations of the Subscriber's Company or Organisation	**2.1.3**
	The Subscriber's Company or Organization, represented by its legal representative, permits the Subscriber to obtain an **"E-Trust IDA Lightweight Certificate"** testifying his/her status with the organization. The Subscriber's Company or Organization agrees with: • The E-Trust Certificate Practices Statement for Qualified and Normalised Certificates (CPS) published by E-Trust, which describes the practices used to provide the Certificates; • This CP; In particular, the Subscriber's Company or Organization accepts: • That the Agreement between the company or organization, the Subscriber and E-Trust is governed by Belgian law; • The responsibilities of the Subscriber as described in this CP and the corresponding Certificate Request Form. • That it is responsible for the accuracy of the data it transmits to the LRA. The company or organization shall immediately inform the LRA of any change to this data, and the latter will then take appropriate action. • That in certain cases, described in the CPS, E-Trust or the LRA may revoke or suspend the Certificate (provided that the Subscriber and the company or organization are informed). • That it will ask the LRA to suspend or revoke the Certificate whenever the CPS requires this. The suspension and revocation procedures are described in the CPS. • The rights, liabilities and obligations of E-Trust. These are described in the CPS and this CP (section C).	

<table>
<tr><td>Section</td><td></td><td>CPS ref</td></tr>
<tr><td>D</td><td>Identification and Authentication</td><td>3.1</td></tr>
<tr><td></td><td>The following information is checked (see section E: “Certificate Application Procedure of the present CP) and certified in the issued E-Trust Lightweight Certificate Policy for the European Commission – IDA Sectoral Networks. The Fields in the certificate appear in the following order:
<table>
<tr><th>Field</th><th>Required/ Optional/ Fixed</th><th>Value</th></tr>
<tr><td colspan="3">Distinguished Name</td></tr>
<tr><td>Country (C)</td><td>Required</td><td><Subscribers’s Organisation Country></td></tr>
<tr><td>Location (L)</td><td>Required</td><td><Subscriber’s Organisation City></td></tr>
<tr><td>Organisation (O)</td><td>Required</td><td><Subscribers’s Organisation></td></tr>
<tr><td>Organisational Unit (OU)</td><td>Optional</td><td><Unit within organisation></td></tr>
<tr><td>Organisational Unit (OU)</td><td>Fixed</td><td>Only for IDA Sectoral Networks (1720/1999/EC and 2045/2002/EC)</td></tr>
<tr><td>Common Name (CN)</td><td>Required</td><td><Functional Mailbox Name></td></tr>
<tr><td>EmailAddress</td><td>Required</td><td><Functional Mailbox Email Address></td></tr>
<tr><td colspan="3">Extensions</td></tr>
<tr><td>KeyUsage</td><td>Fixed</td><td>Digital Signature, Non-Repudiation, Key Encryption, Data Encryption, Key Agreement</td></tr>
<tr><td>CPS/CP OID</td><td>Fixed</td><td>OID: 0.3.2062.7.1.1.8.1</td></tr>
<tr><td>CPS/CP Summary</td><td>Fixed</td><td>E-Trust Lightweight Certificate Policy for the European Commission – IDA Sectoral Networks</td></tr>
<tr><td>CPS/CP Location</td><td>Fixed</td><td>http://www.e-trust.be/CPS/IDA</td></tr>
<tr><td colspan="3">Other information</td></tr>
<tr><td>Version</td><td>Fixed</td><td>2 (X.509 Version 3 Certificate)</td></tr>
<tr><td>SerialNumber</td><td>Required</td><td><Set by CA></td></tr>
<tr><td>Algorithm</td><td>Fixed</td><td>Sha1withRSAEncryption</td></tr>
<tr><td>SubjectPublicKey</td><td>Required</td><td><subscriber’s public key (1024 bit)></td></tr>
<tr><td>Validity start date</td><td>Fixed</td><td>Date of issuance</td></tr>
<tr><td>Validity end date</td><td>Fixed</td><td>1 year from date of issuance</td></tr>
<tr><td>Issuer</td><td>Fixed</td><td>CN = Certipost E-Trust Primary CA for Normalised certificates
O = Certipost
C = BE</td></tr>
</table></td><td></td></tr>
<tr><td>E</td><td>Certificate Application Procedure</td><td></td></tr>
<tr><td></td><td>1. The Subscriber downloads and prints the E-Trust Lightweight Certificate Policy for the European Commission – IDA Sectoral Networks Certificate Request Form (hereafter referred as the certificate request form) from the E-Trust Web Site (http://www.e-trust.be/CPS/IDA). This is the Contractual Agreement. The Subscriber can also ask the LRA to receive a copy of this document by post or by e-mail.
2. The Subscriber must send by fax and post to the LRA the following documents:
• The certificate request form, duly filled in and signed by him/her and by a legal representative of his/her Company or Organisation;
• A signed copy of an official form of identity valid in the country of origin of the Subscriber;
• Evidence of the fact that the person signing the Certificate Request Form on behalf of the company or organisation is the legal representative;</td><td></td></tr>
</table>

Section		*CPS ref*
	3. Electronic Certificate Request The Subscriber will send the electronic certificate request (in PKCS#10 Format), via e-mail to the LRA, after having generated the key pair within eight (8) days from the date the request form and the related documents (section E(2)) have been sent, hereafter referred as the Registration File, to the LRA. 4. LRA Validation When collecting the Registration File received from the Subscriber by fax and by post, and the electronic certificate request sent by the Subscriber via e-mail, the LRA Operator (LRAO) performs final validation checks including among others the accuracy of the information provided in the Registration File, a phone and/or e-mail call back. When accepted by the LRAO, the electronic certificate request is sent to the Authorised Certification Authority (see section C1 of the present CP) for certificate issuing. When the certificate request is rejected by the LRAO, the LRAO will inform the Subscriber of this rejection and of the reasons that motivated this rejection.	
F	**Certificate Issuance and delivery**	**4.2**
	On reception of a validated certificate request, the E-Trust Primary CA for Normalised Certificates will deliver the electronic certificate to the LRA. The Subscriber will receive from the LRA an e-mail that contains the certificate. Using the Key Generation Wizard, a Personal Security Environment (PKCS#12) can be generated for importing the certificate into applications.	
G	**Certificate Acceptance and Certificate Publication**	**4.3**
	Publication of the Certificate in E-Trust Certificate Public Registry. Once the certificate has been issued by the E-Trust Primary CA for Normalised Certificates, it is immediately published in E-Trust Certificate Public Registry. *Acceptance* • The Subscriber accepts that the electronic certificate will be published in the E-Trust Certificate Public Registry immediately after its creation. • The Certificate is deemed accepted by the Subscriber within 8 days from the issuance or at the moment of its first use, whichever is the earliest. If the Subscriber notices an inconsistency between the contractual agreement information and the content of his/her Certificate, he/she must inform the LRA without any delay. The LRA will then revoke the Certificate and take the appropriate measures to re-issue a certificate. This will be the Subscriber's sole remedy for any acceptance refusal.	
H	**Procedure for the Revocation , Suspension and Unsuspension.**	**4.4**
	The Subscriber can request to suspend, revoke or unsuspend the certificate. The Subscriber will be informed whenever the certificate is suspended, unsuspended or revoked. **Suspend and unsuspend.** In order to suspend a certificate: First contact the LRA via telephone (contact details of the LRA can be found at http://www.e-trust.be/CPS/IDA). Then send the completed suspend/revoke form (included in the certificate request form) along with a signed copy of an official form of identity, valid in the country of origin, of the person suspending the certificate via fax and then by post to the LRA. Upon notification, the LRA will immediately suspend the certificate and start the validation process to check the accuracy of the received documents. After proper	

Section		*CPS ref*
	validation the LRA can proceed by keeping the certificate suspended or by unsuspending it. In order to confirm the request for suspension, the LRA will do a telephone callback to the Subscriber. **In order to unsuspend a certificate**: Send the completed suspend/revoke form (included in the certificate request form) along with a signed copy of an official form of identity, valid in the country of origin, of the person requesting Subscriber of the certificate via post to the LRA. Upon notification, the LRA will immediately start the validation process to check the accuracy of the received documents. After proper validation the LRA will do a telephone callback to the Subscriber. Only after this validation procedure will the LRA unsuspend the certificate. The certificate will be unsuspended only after proper research and validation of the unsuspend request. Unless the Subscriber requests certificate unsuspension, the LRA will automatically revoke the certificate permanently within a period of 10 (ten) working days. **Revocation.** In order to revoke a certificate: First contact the LRA via telephone. Then send the completed suspend/revoke form (included in the certificate request form) along with a signed copy of an official form of identity, valid in the country of origin, of the person revoking the certificate via fax and then by post to the LRA. Contact details of the LRA can be found at http://www.e-trust.be/CPS/IDA. Upon notification, the LRA will immediately suspend the certificate and start the validation process to check the accuracy of the received documents. After proper validation the LRA will revoke or unsuspend the certificate. In order to confirm the request for revocation, the LRA will do a telephone callback to the Subscriber. Unless the Subscriber requests certificate unsuspension within a period of 10 (ten) working days the certificate will be automatically permanently revoked.	

Section		*CPS ref*
I	**Renewal**	
	In order to receive a new certificate when the validity period expires, the Certificate Application Procedure applies (see section E).	
J	**Privacy**	
	The information collected by the LRA (paper document and electronic information) and provided by the Subscriber in the context of the certificate request and delivery are duly archived by the LRA and E-Trust. The Belgian Law on privacy issues will hereby be respected [1].	
K	**Fees**	**2.5**
	No fees are applicable to the Subscriber or Organisation.	

FOR MORE INFORMATION PLEASE CALL
+32 70 22 55 44
OR SEND AN E-MAIL TO
feedback.fr@contact.certipost.be
feedback.nl@contact.certipost.be

1 In order to carry out its tasks in an efficient manner, Certipost E-Trust and the LRA's use databases with these personal data. In this regard, Certipost E-Trust and the LRA's must respect the privacy of the persons concerned and therefore attaches utmost importance and caution to the processing of personal data.
The personal data that you supply to the LRA and to Certipost E-Trust are incorporated in the files of Certipost S.A., Centre Monnaie, 1, 1000 Brussels. The data will be used only for the provisioning of the certificates and related services. You have the right to access and correct this data.