Certipost E-Trust[1] Lightweight Certificate Policy

for Justice and Home Affairs DG CUG functional mailboxes – EC Regulation 2725/2000

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 Justice and Home Affairs DG CUG functional mailboxes – EC Regulation 2725/2000.**	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 this Functional Mailbox by the Organisation and for which the Organisation is responsible. The validation of the request will require evidence of the identity of the Subscriber and evidence that he/she represents an Organisation identified on the list of authorities identified under Article 15 of EC Regulation 2725/2000. 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 whole registration process will be the responsibility of Justice and Home Affairs DG of the European Commission, which will act as the Local Registration Authority, further called LRA. The LRA can be contacted at: JAI DAC LRAO Office LX 46 5/82 DG Justice and Home Office Affairs European Commission, B1049 Brussels Tel : +32 2 296 22 72 (or +32 2 29 84458) Fax: +32 2 29 67688 E-Mail: jai-dac-lsa@cec.eu.int or admin@cap01.dac.cec.eu-admin.net The LRA will act for this type of certificate as well as Suspension and Revocation Authority (SRA). **Subscriber** • The Organisation o The Organisation Listed Responsible: the person representing the Organisation, mentioned on the list of authorities identified under Article 15 of EC Regulation 2725/2000.	

[1] At the creation of Certipost, the entire Belgacom E-Trust activity has been transferred to Certipost. Certipost acts as Certificate Service Provider having entirely taken the Belgacom E-Trust activities over; Certipost has thus endorsed all Belgacom E-Trust duties and responsibilities in that matter.

Section		*CPS ref*
	○ The Private Key Responsible: a person that is indicated in the request form as responsible for the use of the private key and the follow up of the procedures (typically the head of the department that is responsible for the functional mailbox). The Private Key Responsible will be the person who performs the Certificate Request (possibly aided by a Private Key Operator). ○ The Private Key Operator(s): one or more persons that need and do have access to the private key for operational reasons. It is possible that the Private Key Responsible is a Private Key Operator at the same time. Whenever this document refers to the "Organisation", this is applicable to all roles, with the final responsibility lying with the Private Key Responsible. **Applicability** E-Trust governs this certificate as specified in the CPS. This type of certificate is a functional digital identity guarantee that can be used to secure S/MIME communication in the framework of the EC Regulation 2725/2000. It is however 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 the certificate content in D).**	
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 sa acting as Certification Service Provider via its E-Trust services and having took over the Belgacom **E-Trust Primary CA for normalised certificates** as described in the current CPS.	
C.2	**Rights, liabilities and obligations of the LRA (DG JAI)**	**2.1.2**
	The Justice and Home Affairs DG, in its capacity as Local Registration Authority, is under a contractual obligation to follow scrupulously the registration procedures described in the E-Trust CPS. As a LRA, the Justice and Home Affairs DG guarantees that: • Organisations 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: ○ The registration officer shall inform the requestor of the terms and conditions for the use of the Certificate. These are set out in the	

Formatted: English (U.K.)

Formatted: English (U.K.)

Section		*CPS ref*
	Request Form and the General Terms and Conditions to be signed by the requesting Organisation (paper or notarized electronic format). o The registration officer shall check the identity of the requestor on the basis of valid ID papers or passport. • The registration officer shall verify the information (whether compulsory or optional) relating to the Functional Mailbox of the Organisation for the purposes of certifying it, as set out in section E of this document and in accordance with the files and information of the Justice and Home Affairs DG. • 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 requestor of the Certificate. o A copy of the contractual agreement signed by the Private Key Responsible, including the latter's agreement to all obligations incumbent on him and his Organisation. This data, including the original MG Reg. 2725 request form, 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.	
	In its capacity as a LRA, the Justice and Home Affairs DG shall be contractually obliged to take clear and appropriate measures regarding: • The physical security of the information and, where appropriate, of the systems; • 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 Justice and Home Affairs DG shall ensure these items are 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.	
	Rights, liabilities and obligations of the Organisation	**2.1.3**
	The Organisation agrees with the current CPS describing the Practices that are used to deliver E-Trust electronic certificates and edited by E-Trust. The Organisation agrees with the present Certificate Policy (CP). In particular, the Organisation accepts that: • The contractual agreement related to this type of certificate is governed under the Belgian laws • The Organisation (in particular the Private Key Operators) is obliged to	

Formatted: English (U.K.)

Formatted: English (U.K.)

Formatted: English (U.K.)

Section		CPS ref
	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, the Organisation 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 passphrase, used to protect unauthorised use of the private key shall never be stored in the same location as the private key itself or next to its storage media, shall never be stored unprotected, and shall be given sufficient protection. The private key must not be left unattended in an unlocked state (i.e., unattended in a workstation when the PIN or passphrase has been entered). The Organisation is solely responsible for the usage of the private key, E-Trust is not liable of the usage of the Organisation's key pair. • The Organisation is responsible for the generation of the key pair for the Functional Mailbox. • The Organisation is responsible for the accuracy of the data it transmits to the LRA. • The Organisation 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 Organisation must request the LRA to revoke the certificate whenever a person that had been appointed Private Key Operator for that certificate has been removed from that responsibility (i.e. whenever a person who has had access to the private key, is not allowed to operate it any further). • The Organisation has to inform immediately the LRA Services on any change in the information included in the certificate. The revocation procedure will be immediately started. • The Organisation 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 on registration. The LRA will correct the registered information. This includes warning the LRA if an additional person is appointed Private Key Operator. • The Organisation accepts that the electronic certificate will be published in a publicly accessible registry immediately after its creation and that revocation information on 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 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 Organisation agrees with the rights, obligations and liabilities of E-Trust and the LRA. These are described in the current CPS, the Functional Mailbox Certificate request form, and in the present CP (section C). • The Organisation agrees that E-Trust and the LRA have the right to	

Formatted: English (U.K.)

Formatted: English (U.K.)

Formatted: English (U.K.)

Section		*CPS ref*
	revoke / suspend the Organisation's certificate in particular cases described in the current CPS (section 4.4). The LRA warns and informs the Organisation.	

Formatted: English (U.K.)

Formatted: English (U.K.)

Section		CPS ref
D	**Identification and Authentication**	**3.1**

The following information is checked (see section E: "Certificate Application Procedure of the present CP) and certified in the issued E-Trust Lightweight Professional Certificate Policy for Justice and Home Affairs DG CUG functional mailboxes – EC Regulation 2725/2000. The Fields in the certificate appear in the following order:

Field	Required/ Optional/ Fixed	Value
Distinguished Name		
Country (C)	Required	**<Organisation's Country>**
Organisation (O)	Required	**<Organisation's Name>**
Organisational Unit (OU)	Optional	**<Organisational Unit Name>**
Organisational Unit (OU)	Fixed	Only for EC Regulation 2725/2000
Location (L)	Required	**<Organisations's City (legal siege)>**
Common Name (CN)	Required	**<Functional mailbox name>**
EmailAddress	Required	**<Functional mailbox email address>**
Extensions		
KeyUsage	Fixed	Signature and encryption
Extended Key Usage	Fixed	S/MIME
CPS/CP OID	Fixed	OID: 0.3.2062.9.6.1.20.3 (version) OID: 0.4.0.2042.1.3
CPS/CP Summary	Fixed	E-Trust Lightweight Certificate Policy for Justice and Home Affairs DG CUG functional mailboxes – EC Regulation 2725/2000
CPS/CP Location	Fixed	https://forum.europa.eu.int/Members/irc/jai/jai_eurodac/library?l=/pki_documents
Other information		
Version	Fixed	2 (X.509 Version 3 Certificate)
SerialNumber		Certificate serial number as generated by the CA
Algorithm	Fixed	Sha1withRSAEncryption
SubjectPublicKey	Required	**<subscriber's public key (1024 bit)>** **Public Key: Key Length 1024 bit** **Public Exponent: Fermat-4(=010001)**
Validity start date	Fixed	Date of issuance
Validity end date	Fixed	1 year from date of issuance
Issuer	Fixed	CN = Belgacom E-Trust Primary CA OU = E-Trust O = Belgacom C = BE

E	**Certificate Application Procedure**

1. The Private Key Responsible downloads and prints the E-Trust Lightweight Professional Certificate Policy for the Justice and Home Affairs DG CUG functional mailboxes – EC Regulation 2725/2000 Request Form (hereafter referred as the MG Reg. 2725 request form) from the Justice and Home Affairs Interest Group on CIRCA (https://forum.europa.eu.int/Members/irc/jai/jai_eurodac/library?l=/pki_documents). This is the Contractual Agreement. The Private Key Responsible can also ask the LRA to receive a copy of this document by post or by e-mail.

2. The Organisation must send by fax and post to the LRA the following documents:

Formatted: English (U.K.)

Section		*CPS ref*
	• The MG Reg. 2725 request form, duly filled in and signed by the Private Key Responsible (including the list of private key operators) ; • A signed copy of an official form of identity valid in the country of origin of the Private Key Responsible; • A signed copy of an official form of identity valid in the country of origin of the Organisation Listed Responsible; • A mandate letter nominating the Private Key Responsible as responsible for the Private Key and the Certificate, signed by the Organisation Listed Responsible; 3. Electronic Certificate Request The Subscriber will send the electronic certificate request (in PKCS#10 Format), via e-mail to admin@cap01.dac.cec.eu-admin.net, 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 Organisation either by fax and/or by post, and the electronic certificate request sent by the Organisation, 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, E-Trust Primary CA will deliver the electronic certificate to the LRA. The Organisation will receive from the LRA an e-mail that contains the certificate. The certificate can then be installed in the application.	
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 Qualified and Normalised Certificates, it is immediately published in E-Trust Certificate Public Registry. *Acceptance* • The Organisation 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.	

Formatted: English (U.K.)

Formatted: English (U.K.)

Section		*CPS ref*
H	**Procedure for the Revocation , Suspension and Unsuspension.**	**4.4**
	The Organisation can request to suspend, revoke or unsuspend the certificate. The Organisation 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 (+32 2 296 22 72). Then send the completed suspend/revoke form (included in the MG Reg. 2725 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 (fax: +32 2 29 67688). 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 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 related Private Key Responsible. In order to unsuspend a certificate: Send the completed suspend/revoke form (included in the MG Reg. 2725 request form) along with a signed copy of an official form of identity, valid in the country of origin, of the person who has suspended 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 related Private Key Responsible. Only after this validation procedure will the LRA unsuspended the certificate. The certificate will be unsuspended only after proper research and validation of the unsuspended request. Unless the Organisation requests certificate unsuspension, within a period of 10 (ten) working days the certificate will be permanently revoked automatically. **Revocation.** In order to revoke a certificate: First contact the LRA via telephone (+32 2 296 22 72). Then send the completed suspend/revoke form (included in the MG Reg. 2725 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 (fax: +32 2 29 67688). 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 related Private Key Responsible. Unless the Organisation requests certificate unsuspension, within a period of 10 (ten) working days the certificate will be automatically permanently revoked.	

Formatted: English (U.K.)

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. The Belgian Law on privacy issues will hereby be respected [2].	
K	**Fees**	**2.5**
	No fees are applicable to the Subscriber or Organisation.	

Formatted: English (U.K.)

Formatted: English (U.K.)

Formatted: English (U.K.)

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

[2] In order to carry out its tasks in an efficient manner, the LRA uses databases with these personal data. In this regard, the LRA must respect the privacy of the persons concerned and therefore attaches utmost importance and caution to the processing of personal data.
The personal data which you supply to the LRA are incorporated in the files of the Justice and Home Affairs DG of the European Commission. 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.