Certificate Policy for Certipost E-Trust Normalised Certificates for EUROCONTROL

Version 1.0

Publication Date : 26 March 2009

Effective Date : 1 April 2009

Certificate Policy for Certipost E-Trust Normalised Certificates for EUROCONTROL

This document describes the applications for which certificates, in the form of a Normalised Certipost E-Trust Certificate for EUROCONTROL (hereinafter referred to as the "Certificate") issued by the Certification Service Provider (CSP) under this Certificate Policy (CP), may be used, as well as the procedures to be followed and the responsibilities of the parties involved, in accordance with the CSP's Certification Practice Statements (CPS). This CP applies to Normalised Certificates that meet the following criteria :

Definitions :

Activation Data	Data values, other than keys, that are required to use the private key of a certificate and that need to be protected (e.g. password or PIN Code).
Certipost or Certipost E-Trust	Certipost SA/NV, with registered offices in Muntcentrum ,B-1000 Brussels, Belgium
Certipost E-Trust Services	The Certipost Certification services.
Certipost E-Trust Certificate Public Registry	The electronic registry used by Certipost E-Trust Services to publish the issued Certificates and Certificate Revocation Lists.
Certificate	An electronic statement that maps the signature verification data to a physical, a legal person or an entity and confirms the identity of this person or entity (subject).
Certificate Holder	A physical entity to which a Certification Service Provider has delivered a Certificate. A physical entity may be Certificate Holder for 1 or more Certificates.
Certificate Policy	A named set of rules that indicate the applicability of a Certificate to a particular community and/or class of application with common security requirements.
Certificate Public Registry	The repository that hold the publicly available certificates, CRL's and ARL's, issued by the Certipost E-Trust CA's.
Certification Authority (CA)	The entity that issues Certificates by signing Certificate data with its Private Signing Key according to this CPS.
Certification Practice Statement (CPS)	A statement of the practices, which a Certification Service Provider applies for the issuing of Certificates.
Certificate Revocation List (CRL)	A published list of the suspended and revoked Certificates.
Certification Service Provider	Any physical or legal person which delivers and manages Certificates or provides other services related to electronic signatures.
Customer	Customer of EUROCONTROL
EUROCONTROL Staff	A physical person directly employed by EUROCONTROL, i.e. on the "payroll" of EUROCONTROL (can be e.g. official, contractual staff)
EUROCONTROL Contractor	A physical person (contractually) engaged by EUROCONTROL for performing certain tasks, but person is not on the "payroll" of EUROCONTROL. The engagement can be directly towards the person or indirectly via a company that was awarded a contract by EUROCONTROL for performing tasks.
EUROCONTROL External	A physical person that has a business relationship with EUROCONTROL, but is not contractually engaged by EUROCONTROL to perform certain tasks. The relationship can be direct with the person or as an employee of a partner organisation/company of EUROCONTROL (e.g. employee of airport company, FAA, etc).
Normalised Certificate	A Certificate that is issued according to the requirements of the ETSI technical standard TS 102 042 Normalised Certificate Policy (NCP), and used to support any usage **but** Qualified Electronic

	Signatures of a cryptographic key pair whose corresponding public key pair is certified. The certified key usage's can be any or any mix of the following usage's: encryption, authentication, non-Qualified signatures, etc. The Normalised Certificate Policy offers the same quality as that offer by the Qualified Certificate as defined in ETSI TS 101 456 but without the legal constraints implied by the European Directive, without (NCP) requiring use of Secure User Device (signing or decrypting).
Private Key	The private part of an asymmetric key pair used for Public Key encryption techniques. The Private Key is typically used for creating digital signatures or decrypting messages.
Private Signing Key	A Private Key that is exclusively used for signing data.
Private Decryption Key	A Private Key that is exclusively used for decrypting data.
Public Key	The public part of an asymmetric key pair used for Public Key encryption techniques. The Public Key is typically used for verifying digital signatures or to encrypt messages to the owner of the Private Key.
Local Registration Authority (LRA)	An entity that undertakes to identify and authenticate Certificate Holders on behalf of a CA.
Relying Party	Any entity that relies on the Normalised Certificate. For instance a recipient of an e-mail, signed with the Normalised Certificate by a Certificate Holder or a sender of an e-mail, encrypting this e-mail to a Certificate Holder.
Secure User Device	Device which holds the user's Private Key, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Secure Archiving Device	Device which holds, in encrypted form, a copy of the Private Decryption Keys of the Certificate Holders. This Secure Archiving Device is protected by a PIN Code
Subject	An entity as identified in the subject field of the Certificate as the holder of the Private Key associated with the Public Key given in the Certificate.
Suspension and Revocation Authority (SRA)	An Authority that suspends, unsuspends and/or revokes Certificates on behalf of the CA.

Section		*Ref. RFC 2527*
A	***Detail of the Certificate Policy for Normalised E-Trust Certificates for EUROCONTROL***	**1.1**
	This type of Certificate provides a very high degree of assurance of the electronic personal and professional identity of the Certificate Holder. The Certificate Holder is an employee of a company or belongs to an organization. The link between the Certificate Holder, the company or organization and the public key is certified. For applications to be validated, the person applying for the Certificate must present, for verification, his/her identity card and, only for EUROCONTROL externals, proof of his/her professional status, together with any supporting information to be certified and documents linking his identity to the company or organization. Under this certificate policy, two types of Normalised E-Trust Certificates for EUROCONTROL are described. The private key corresponding to the public key certified in this way can be used for	

<table>
<tr><th>Section</th><th></th><th>Ref. RFC 2527</th></tr>
<tr><td></td><td>digital signing (non Qualified digital signature) of eg e-mails (EUROCONTROL e-mail signing certificate) and for encryption of eg e-mails (EUROCONTROL e-mail encryption certificate). The certificate is specified by the criteria for “Normalised Certificates” as specified by technical standard ETSI TS 102 042.

The Certification Service Providers (CSP’s), authorized to issue Certificates under this CP specify whether they claim to comply to the CP and to the relevant regulatory documents or whether they have been certified to be compliant.

The Certificates issued under this CP include two 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.</td><td></td></tr>
<tr><td>B</td><td>Identification of the Certificate Policy for Normalised E-Trust Certificates for EUROCONTOL</td><td></td></tr>
<tr><td></td><td>A CP is a specific set of rules that indicate a Certificate's applicability to a particular community and/or type of application that shares the same security requirements.

This document sets out and identifies the Normalised E-Trust Certificate Policy for EUROCONTROL. These Certificates are compatible with, and meet the requirements laid down in, ETSI TS 102 042 (NCP).

The CSP, via EUROCONTROL as LRA, is responsible, for the Certificate Holder, for the generation of the Private Key and Public Key.

The Certificates issued under this Normalised Certificate Policy for EUROCONTROL have two CP unique identifiers. This can be used by Relying Parties to determine the applicability and trustworthiness of the Certificate for a particular application. These Identifiers are as specified in the table below :

<table>
<tr><th>Normalised E-Trust Certificate for EUROCONTROL</th></tr>
<tr><td>Normalised Certificate without SSCD
OID ETSI 102 042: 0.4.0.2042.1.1
Signing Certificate: 0.3.2062.7.1.1.251.1</td></tr>
<tr><td>Normalised Certificate without SSCD
OID ETSI 102 042: 0.4.0.2042.1.1
Encryption Certificate: 0.3.2062.7.1.1.252.1</td></tr>
</table>

Table 1. Identification of E-Trust Certificate Policy for Normalised Certificates for EUROCONTROL</td><td></td></tr>
<tr><td>C</td><td>Applicability</td><td>1.3.4</td></tr>
<tr><td></td><td>• This type of Certificate provides a very high degree of assurance with regard to the electronic personal and professional identity of the Certificate Holder. It can therefore be used to protect (signing and encryption) e-mails or other documents in a high sensitive electronic communication context.
• This certificate may only be used in the framework of signing and encrypting e-mails or other electronic documents between EUROCONTROL employees or between an EUROCONTROL employee and a partner of EUROCONTROL.
• Key usage and the applicability of the Certificate are certified (see the description of the Certificate content in Section E of this document). Normalised Certificates for EUROCONTROL issued under this CP comply with ETSI TS 102 042 (NCP).</td><td></td></tr>
</table>

Section		*Ref. RFC 2527*
D	***Rights, responsibilities and obligations***	***2***
D.1	***Rights, responsibilities and obligations of the Certification Service Provider***	**2.1**
	• The CSP issues X509 v3-compatible Certificates (ISO 9594-8). • The CSP issues Normalised Certificates as defined in and accordance with the criteria laid down in ETSI TS 102 042. • The CSP guarantees that all the requirements set out in the applicable CP 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. - **Certipost sa/nv, via its Certipost E-Trust services** provided through the **Certipost E-Trust Secondary Normalised CA for EUROCONTROL**: - *Certification Practice Statements (CPS):* www.e-trust.be/CPS/QNcerts**, CPS OID: 0.3.2062.7.1.0.1.2.0** - *Public Register of Certificates and Certificate Revocation Lists (CRL):* www.e-trust.be/en/x500 • To register persons applying for a Certificate, the CSP uses the following approved Local Registration Authorities (LRA's): - EUROCONTROL, as a contractually bound organization that will act as RA for the provision of authenticated Certificate request files. • As the CSP, via EUROCONTROL as LRA, proceeds to the key pair generation for 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. • The Key Pair is generated by the CSP, via EUROCONTROL as LRA, on a PC under control of the LRA. The Key Pair is not generated directly on a Secure User Device. However, the CSP, via EUROCONTROL as LRA, will proceed after the issuance of the Certificate corresponding to the Key Pair to the installation of the Certificate and the corresponding Key Pair on a Secure User Device. The corresponding Certificate may be used to create signatures or decrypt e-mails or other electronic documents solely by means of this Secure User Device. • 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 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 an 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].	

[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 CSP also guarantees the confidentiality of any data not published in the Certificates.	
D.2	***Rights, responsibilities and obligations of the Certificate Holder***	**2.1.3**

	The Certificate Holder hereby accepts the Certification Practice Statement (CPS) currently in effect, as drafted by the CSP and setting out the procedures used for providing digital Certificates.
	The Certificate Holder agrees to this CP.
	More specifically, the Certificate Holder hereby gives his/her acceptance to the following :
	• The contractual agreement for this type of Certificate is governed by Belgian law.
	• The information submitted to the CSP, via EUROCONTROL as LRA, by the Certificate Holder 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 and/or in this CP and applicable CPS.
	• The Key Pair is generated by the CSP, via EUROCONTROL as LRA, on a PC under control of the LRA. The Key Pair is not generated on a Secure User Device. However, the CSP, via EUROCONTROL as LRA, will proceed to the installation of the Key Pair on a Secure User Device. The corresponding Certificate may be used to create signatures or decrypt messages solely by means of this Secure User Device.
	• In accordance with the applicable CPS and with this CP, the Certificate Holder must keep confidential and protect the Private Key at all times against loss, disclosure, alteration or unauthorized use. Once the Private and Public key pair has been delivered to the Certificate Holder, 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) 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 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:
	  • The Private Key of the Certificate Holder is lost, stolen or potentially compromised; or,
	  • The Certificate Holder no longer has control of the Private Key because the activation data (e.g., PIN code) has been compromised for any reason; and/or,
	  • The certified data has become inaccurate, incorrect 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 inform the CSP, via EUROCONTROL as LRA, of any changes to the data on the Certificate. The Certificate will	

Section		Ref. RFC 2527
	then be revoked immediately. • The Certificate Holder must inform the CSP, via EUROCONTROL as LRA, 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 will promptly cease all use of the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of that Certificate. • 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 Certificate 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 LRA of all information used for the purposes of registration, 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 this CP (Section D1) and in the General Terms and Conditions.	
D.3	***Rights, responsibilities and obligations of EUROCONTROL as the Local Registration Authority (LRA)***	
	The LRA is under a contractual obligation to comply scrupulously with the registration procedures described in the CPS of the CSP. The LRA guarantees that: – Certificate Holders are properly identified and authenticated both as regards to the personal identity of the Certificate Holder as a natural person and as regards to the information about their professional status, during issuance process of the Certificates as well as during the Private Decryption Key recovery request process; – Any requests for Certificates submitted to the CSP are complete, accurate, valid and duly authorized. – Any requests for recovery of the Private Decryption Key to the Key Archiving Authority (KAA) are complete, accurate, valid and duly authorized. – Dual control is implemented in the certificate issuance process, ensuring the timeframe that Activation Data and the Private Key of a Certificate are held by one and the same person is limited to a minimum.	

Section		Ref. RFC 2527

More specifically:

- The LRA Operator (LRAO) informs the Certificate Holder of the terms and conditions for the use of the Certificate. These are referenced to on the website of Certipost (http://www.e-trust.be/QNCerts).
- The LRAO 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 LRAO ensures the storing of one copy of the information provided during registration procedure by the Certificate Holder or during the recovery procedure of the Private Decryption Key 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 (for EUROCONTROL externals only), including any reference numbers on documentation used for this verification as well as any limitations on its validity.
  - A copy of the contractual agreement (delivery receipt) signed by the Certificate Holder and a person higher in the EUROCONTROL hierarchy (for EUROCONTROL staff or contractors) or the legal representative of the organization (for EUROCONTROL externals), including the agreement to all obligations incumbent on these persons.
    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 LRA.
- The issuance procedure used by the LRAO guarantees that the Certificate Holder is in possession of the Private Key linked to the Public Key to be certified :
  - The LRAO guarantees the secure transfer of the Private Decryption Key and Private Signing Key to the Secure User Device.
  - The LRAO Guarantees that the secure deletion of the Private Signing Key after transferring to the Secure User Device.
  - The LRAO guarantees the secure transfer of the Secure User Device, holding the Private Decryption and Private Signing Key, and the corresponding PIN Code to the Certificate Holder.
- The LRAO guarantees the secure transfer of the Private Decryption Key to the KAA.
- Compliance with the requirements relating to the processing of personal data with respect to the registration procedure.

The LRA 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 used in the context of RA activities;
- Employees dealing with registration.

The classification of and responsibility for this data are of crucial importance, i.e.,

- the data itself (registration data, Activation Data, guidelines and procedures, etc.) in paper form and, where applicable, in electronic form;
- The software applications used in the context of LRA activities and their configuration;
- The equipment (hardware, telecommunications tools, etc.) used in the context of LRA activities and their configuration;
- Physical access to the data (buildings, safes, access controls and conditional access to software, etc.).

Section		Ref. RFC 2527
	The LRA 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 EUROCONTROL as the Key Archiving Authority (KAA)***	
	The KAA is under a contractual obligation to comply scrupulously with the procedures described in this CP. The KAA guarantees that a copy of all Certificate Holders' Private Decryption Keys is kept secret. These are only made available, after validation of the request to the LRA. The KAA will keep a copy only of the Certificate Holders' Private Decryption Key. The KAA is not allowed to keep a copy of the Certificate Holders' Private Signing Key. The KAA will keep no copy of the Certificate Holders Activation Data (password or PIN Code). More specifically: – The KAA guarantees that the received copy of the Private Decryption Key from the LRA is transferred securely on the Secure Archiving Device – The KAA guarantees the secure deletion of the received copy of the Private Decryption Key after secure transfer to the Secure Archiving Device – Requests for Recovery of Private Decryption Keys are duly authenticated before handing over the Private Decryption Key to the LRA – The KAA Guarantees the secure transfer of the Private Decryption Key to the LRA – Compliance with the requirements relating to the processing of personal data with respect to the registration procedure. – The KAA guarantees the secure deletion of the Private Decryption Key after transferring to the Secure Archiving Device. The KAA 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 used in the context of KAA activities; • 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 in the context of KAA activities and their configuration; • The equipment (hardware, telecommunications tools, etc.) used in the context of KAA activities and their configuration; • Physical access to the data (buildings, safes, access controls and conditional access to software, etc.). The KAA 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.	

Section		Ref. RFC 2527
D.5	***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 the professional status with respect to the company (or organization). The company (or organization) must agree to: • the CPS currently in effect drafted by the CSP, which sets out the practices used to provide the Certificates; • this CP for E-Trust Normalised Certificates for EUROCONTROL. 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) 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).	
D.6	***Rights, responsibilities and obligations of Relying Parties***	
	Relying 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.	

Section		Ref. RFC 2527
E	***Identification and Authentication – Certified information***	**3.1**

The following information is validated (see Section G of this CP: Certificate application procedure) and certified in the E-Trust Normalised Certificate.

Attribute	**Mandatory/ Optional/Fixed**	**Value**
Distinguished Name :		
countryName (C)	Mandatory	Nationality of the Certificate Holder. In case the Certificate Holder has multiple Nationalities, the value is the Nationality that has been chosen by the Certificate Holder to be registered into EUROCONTROL registers.
Organisation (O)	Mandatory	Issued for EUROCONTROL
serialNumber	Optional	Will only be filled in case the Certificate Holder is an EUROCONTROL employee. In that case, this field is mandatory and will be filled in with the personalID of the EUROCONTROL employee as registered into the EUROCONTOL registers.
organisationalUnit (OU)	Optional	Will only be filled in case the Certificate Holder is external to EUROCONTROL. In that case, this field is mandatory and will be filled in with the organization for which the Certificate Holder is acting.
organizationalUnit (OU)	Optional	Will only be filled in case the Certificate Holder is an EUROCONTORL employee. In that case, this field can be filled in with the function of the Certificate Holder
Pseudonym	Optional	Will only be filled in case the Certificate Holder is an EUROCONTROL employee. In that case, this field will be filled in with the pseudonym of the Certificqte Holder, such as registered in EUROCONTROL databases.
commonName (CN)	Mandatory	Concatenation of the following values : - <First Name of the Certificate Holder> - <Surname of the Certificate Holder> - "-" - "Staff", "External" or "Contractor" (*) - "("<Certificate Usage>")" : E-mail Signing or E-mail Encryption
Rfc822Name	Optional	Certificate Holder's e-mail address.
Extensions (not critical unless specified otherwise)		
SAN		Certificate Holder's e-mail address.
keyUsage	Fixed/Critical	digitalSignature, nonRepudation (for e-mail signing certificate profile) or; keyEncipherment, dataEncipherment (for e-mail encryption certificate profile)
subjectPublicKey	Mandatory	Public Key: Key length: 1024 bits (RSA); public exponent: Fermat-4 (=010001).
certificatePolicies-policyIdentifier	Fixed	0.3.2062.7.1.1.251.1 (for e-mail signing certificate profile) or; 0.3.2062.7.1.1.252.1 (for e-mail encryption certificate profile)

Section				Ref. RFC 2527
	CertificatePolicies-policyQualifier-userNotice	Fixed	"E-Trust Normalised Certificate Policy for EUROCONTROL. Not supported by SSCD, Key Generation by CSP. GTC, CP and CPS: www.e-trust.be/CPS/QNCerts" In case of test certificates, this will become : "E-Trust Normalised Certificate Policy for EUROCONTROL. *** Certificate for test purposes ***. Not supported by SSCD, Key Generation by CSP. GTC, CP and CPS: www.e-trust.be/CPS/QNCerts » *The sections A, B, C, D, F, G, H, I, J,K,L and M of this CP are not applicable on test certificates.*	
	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	http://ca.e-trust.be/NCA_EUROCONTROL.crt	
	CRL Distribution Points	Fixed	http://crl.e-trust.be/NCA_EUROCONTROL.crl	
	Other information:			
	Issuer	Fixed	"CN = Certipost E-Trust Secondary Normalised CA for EUROCONTROL O = Certipost s.a./n.v. C = BE"	
	Validity	Fixed	Maximum of 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, via EUROCONTROL as LRA, for 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 (NCP).			
G	***Certificate-application procedure***			
	The applicant for the Certificate must obtain a Request Form and the General Terms and Conditions for Normalised Certificates (hereafter referred to as "the Request Form" and "the General Terms and Conditions") from the CSP (see Section D.1.5. These together with the CP and CPS constitute the Agreement. The person applying for the Certificate may also ask the CSP to send him/her copies of the documents in question by post or to obtain the documents from a RA approved by the CSP. The correct versions of these documents are available on http://www.e-trust.be/CPS/QNCerts.			

Section		*Ref. RFC 2527*
	The applicant for the Certificate must duly complete the request form. The person applying for the Certificate must go in person to the RA authorized under this CP (see Section D.1(5)). The person applying for the Certificate must arrange a meeting with a RAO and go there in person, taking the following documents. • A (two-sided) copy of the applicant's valid identity card, passport or equivalent official document. The copy must be signed by the person applying for the Certificate; • For EUROCONTROL externals only : A (double-sided) copy of a valid ID card, passport or any equivalent official document of the company's (or organization's) legal representative or duly appointed proxy. The copy must be signed by the legal representative of the company (or organization) or by his/her duly appointed proxy; • For EUROCONTROL externals only : A copy of the current official memorandum and articles of association of the company/organization you officially represent, or, failing this, an excerpt from the register of companies or any other valid official documents, including the relevant excerpts from the Belgian Official Gazette or a similar document. These documents need not to be provided by the applicant for the certificate when this information is already available to the RA (eg via on-line Belgian Official Gazette) • For EUROCONTROL externals only : If the person presenting himself to the LRA and signing the delivery receipt (requestor part) is acting on behalf of the legal representative of the Organisation, the Organisation shall submit proof of the fact that this person is duly authorized to sign for the legal representative. • For EUROCONTROL staff or contractors only : An approval of a person higher in the EUROCONTROL hierarchy then the certificate holder. The Customer must make an appointment with the RAO at the RA of his/her choice authorized under this CP (see Section D.1(5)). The RAO verifies the documents received and checks the following: • the identity of the person applying for the Certificate, based on the latter's identity papers; • on the basis of proof submitted by the person applying for the Certificate, the data to be certified in relation to the company or organization being certified. If the application is validated, the RAO collates all the documents submitted to create a Registration File on the Certificate Holder. The RAO then ensures that one copy is securely archived.	

Section		*Ref. RFC 2527*
H	***Issuing and delivery of the Certificate***	**4.2**
	The certificates will be issued in a suspended mode upon receipt of the Request Form by the LRA. The corresponding activation data (password) will be sent to the Certificate Holder. The Private Decryption Key will be delivered by the LRA towards the KAA for secure archival on a Secure Archiving Device. The LRA will hand over the certificate to the Certificate Holder during an appointment with the Certificate Holder. During this appointment : • the Certificate Holder will validate his identity towards the LRA, as described in section G of this CP. • the Certificate Holder will introduce the activation data (password(s)) of the digital certificate(s) that was/were created • the Certificate Holder will introduce the activation data (PIN Code) of the Secure User Device that holds the Certificate Holders' digital certificate(s). • the Certificate Holder will sign duly the delivery receipt • The LRA will activate the certificate of the Certificate Holder upon receipt of the duly signed delivery receipt, together with the validation documents as described in section G 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 (http://www.certipost.be/en/x500). *Acceptance* • The Certificate Holder must agree to the publication of the digital Certificate in the CSP Public Register of Certificates immediately on creation. • The Certificate is deemed to have been accepted by the Certificate Holder, as the case may be, on the eighth day after its publication in the CSP Public Register of Certificates or its first use by the holder, whichever occurs first. In the intervening period, the Certificate Holder is responsible for checking the accuracy of the content of the Certificate published. The Certificate Holder must immediately notify the CSP of any inconsistency he/she has noted between the information in the contractual agreement and the content of the Certificate. The CSP then revokes the Certificate and takes the appropriate measures to reissue a Certificate. This is the sole recourse available to the Customer if the Certificate in the event of non-acceptance on his/her part.	
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 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 D1.5 of this document.	

Section		Ref. RFC 2527
	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. 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. 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 applicant must make an appointment with an RA approved by the CSP and present himself/herself in person with the duly completed form and a (double-sided) signed copy of his/her identity card. • The RAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the RAO immediately transmits it to the SRA. The SRA 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 applicant must make an appointment with an RA approved by the CSP and present himself/herself in person with the duly completed form and a (double-sided) signed copy of his/her identity card. • The RAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the RAO transmits it to the SRA. The SRA 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, via EUROCONTROL ensures that the certificate requests 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.	

Section		*Ref. RFC 2527*
	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 CertificateHolder. The CSP only issues a Certificate for a previously certified key if the security of the 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 or EUROCONTROL as LRA by the Certificate Holder are entered into a file held by Certipost s.a./n.v. (Exploitation office: Ninovesteenweg, 196, B-9320 Erembodegem (Aalst), Legal office: Muntcentrum 1000 Brussels) and, where necessary, into a file held by EUROCONTROL. 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 EUROCONTROL MIS ServiceDesk : EUROCONTROL MIS ServiceDesk Rue de la Fusée, 96 B-1130 Brussels Belgium Telephone number: +32 (0)2 729 32 32 E-mail address: mis.servicedesk@eurocontrol.int In the event of disputes relating to the validity, interpretation or performance of the agreement concluded between them, the CSP, EUROCONTROL and the Certificate Holder, or his company, 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.	