Certipost Trust Services

Certificate Policy

for Lightweight Certificates for EUROCONTROL

Version	1.2
Effective date	03 May 2012

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).
Certificate	An electronic statement that maps the signature verification data to a physical or legal person or an entity and confirms the identity of this person or entity (Subject).
Certificate Holder	A legal entity to which a Certification Service Provider has delivered a Certificate. A legal entity may be Certificate Holder for 1 or more Subjects.
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 holds the publicly available certificates, CRL's and ARL's, issued by the Certipost E-Trust CA's.
Certificate Revocation List (CRL)	A published list of the suspended and revoked Certificates.
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.
Certification Service Provider	Any physical or legal person which delivers and manages Certificates or provides other services related to electronic signatures.
Certipost Trust Certificate Public Registry	The electronic registry used by Certipost Trust Services to publish the issued Certificates and Certificate Revocation Lists.
Certipost Trust Services	The Certipost Certification services.
Certipost	Certipost SA/NV, with registered offices in Muntcentrum ,B-1000 Brussels, Belgium
NM	The Network Manager (also called internally the 'Directorate Network Management') is an operational unit of EUROCONTROL, enhancing safety through coordinated management of the air traffic in Europe. It ensures in particular that congestion in the air does not occur and that available capacity is used effectively. NM comprises, among others, the former Central Flow Management Unit (CFMU) of EUROCONTROL
NM Agreement	An agreement that is signed between EUROCONTROL and its' customers, determining the terms and conditions under which EUROCONTROL customers are granted access to the NM Services as described on the EUROCONTROL NM website (www.cfmu.eurocontrol.int).
Customer	Customer of EUROCONTROL Network Manager
Lightweight Certificate	A Certificate that is issued according to the requirements of the ETSI technical standard TS 102 042 Lightweight Certificate Policy (LCP), incorporating less demanding policy requirements than the Normalised Certificate 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.
Local Registration Authority (LRA)	An entity that undertakes to identify and authenticate Subscribers on behalf of a CA.
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.
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.
Registration Authority (RA)	An entity, constituted of as an example, but not limited to a Central Registration Authority (CRA) or Local Registration Authority (LRA), that undertakes to identify and authenticate Subscribers on behalf of a CA.
Relying Party	Any entity that relies on the lightweight certificate. For instance the Network Manager (NM) Web Services provider.
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.
Subscriber	A physical person that requests a Certificate and subscribes with a Certification Service Provider (or CA) on behalf of the Certificate Holder..
Suspension and Revocation Authority (SRA)	An Authority that suspends, unsuspends and/or revokes Certificates on behalf of the CA.

Certificate Policy for Certipost Trust Lightweight Certificates for EUROCONTROL

This document describes the applications for which certificates, in the form of a Lightweight Certipost 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 document acts as a replacement for the previous document with OID number: 0.3.2062.7.1.1.351.1 .This CP applies to Certipost Certificates for EUROCONTROL that meet the following criteria:

Section		*Ref. RFC 2527*
A	***Detail of the Certificate Policy for Lightweight Certipost Certificates for EUROCONTROL***	**1.1**
	This type of digital Certificates provides a reasonable level of assurance with regard to the electronic professional identity of the Certificate Holder in the context of or while acting as a customer of EUROCONTROL which is allowed by EUROCONTROL to access the EUROCONTOL NM Web Services. These Certificates are Lightweight Certificates for which the issuing is **not** conditioned to the physical presentation during the registration. These Certificates provide a reasonable level of assurance to guarantee the link between the professional identity of the Certificate Holder, its' Public Key, its' authorized usage and the information related to the professional qualification as customer of EUROCONTROL, which is allowed by EUROCONTROL to access the EUROCONTROL NM Web Services. The validation of the certificate request will demand the provision of the proof of the identity of the Subscriber as belonging to the organization as a customer of EUROCONTROL and the verification of the pieces guaranteeing his qualification and the quality of the related information that has to be certified. The certified Public Key can only be used in context of authentication of the Subject to the EUROCONTROL NM Web Services. In such a case, the Lightweight Certificate satisfies the "**Lightweight Certificate"** requirements in the sense of the technical standard ETSI TS 102 042. The Certification Service Providers (CSPs), authorised to issue Certificates under this CP, indicate whether they claim to comply to the CP and to the relevant regulatory documents or whether they have been certified to be compliant.	
B	***Identification of the Certificate Policy for Lightweight Certificates for EUROCONTROL***	
	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 Certificate Policy for**	

	EUROCONTROL. These Certificates are compatible with, and meet the requirements laid down in ETSI TS 102 042 (LCP). 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 Lightweight E-Trust Certificate Policy for EUROCONTROL have two CP object identifiers (O.I.D.). These 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 : **Lightweight E-Trust Certificate for EUROCONTROL** Lightweight Certificate without SSCD: OID ETSI 102 042: **0.4.0.2042.1.3** Lightweight Certificate for EUROCONTROL: **1.3.6.1.4.1.3860.1.2.112.1.1** OR Lightweight Certificate for EUROCONTROL testing purposes: **1.3.6.1.4.1.3860.1.2.112.2.1** Table 1: Identification of E-Trust Certificate Policy for Lightweight Certificates for EUROCONTROL	
C	***Applicability***	**1.3.4**
	• This type of digital Certificates provides a reasonable level of assurance with regard to the electronic professional identity of the Certificate Holder in the context or while acting as customer of EUROCONTROL, which is allowed by EUROCONTROL to access the EUROCONTOL NM web services. • This certificate may only be used in the framework or accessing the EUROCONTROL NM Web Services. • 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 EUROCONTROL issued under this CP comply with ETSI TS 102 042 (LCP OID : 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**
	• The CSP issues X.509 v3-compatible Certificates (ISO 9594-8). • The CSP issues Certificates amounting to Lightweight Certificates - as defined in and in 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 Lightweight Certificates under this CP: o **Certipost sa/nv, via its Certipost trust services** provided through the **Certipost E-Trust Secondary Lightweight CA for EUROCONTROL and**	

	Certipost Lightweight CA for EUROCONTROL: o *Certification Practice Statement (CPS):* http://pki.certipost.com o *Public Register of Certificates and Certificate Revocation Lists (CRL):* http://crl.pki.certipost.com • To register subscribers applying for a Certificate, the CSP uses the following approved Local Registration Authorities (LRAs): o EUROCONTROL, as a contractually bound organization, that will act as LRA 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 sole guarantee provided by the CSP is that its procedures are implemented in accordance with its CPS and the verification procedures then in effect, and that all Certificates issued with a CP Object Identifier (OID) have been issued in accordance with the provisions of this CP, the verification procedures, and the CPS then in effect. • See sections 2.1, 2.2 and 2.3 of the CSP related to the additional rights, responsibilities and obligations of the CSP. • In certain cases described in the relevant CPS (Section 4.4), the CSP may revoke or suspend the Certificate (provided it informs the Certificate Holder in advance by appropriate means). • In this regard, the CSP must protect the privacy of the persons concerned. It must therefore attach great importance to this matter and exercise all due care when handling such data. The CSP enters the personal data it receives into files. This data is used solely for the provision of certification services. The Subscriber may consult and change this data[i]. • The CSP also guarantees the confidentiality of any data not published in the Certificates.	
D.2	***Rights, responsibilities and obligations of the Certificate Holder***	**2.1.3**
	• The Certificate Holder hereby accepts the Certification Practice Statement (CPS) currently in effect, as provided by the CSP and setting out the procedures used for providing digital Certificates. • The Certificate Holder agrees to this CP. More specifically, the Certificate Holder hereby gives its' 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 Subscriber,	

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

	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 and will not use the Certificate until it has reviewed and verified the accuracy of the data in each such Certificate. • In using the Key Pair, the Certificate Holder must comply with any limits indicated in the Certificate, this CP and the applicable CPS.. • 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 responsible for ensuring the confidentiality and integrity of the Key Pair. The Certificate Holder is deemed the sole user of the Private Key. It must not be stored without protection and the protection must be adequate. 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 immediately ask the CSP, via EUROCONTROL as LRA, to suspend or revoke the Certificate as required pursuant to the relevant CPS (Section 4.4), and in particular if : o The Private Key of the Certificate holder is lost, stolen or possibly compromised or misused; or, o The Certificate Holder no longer has control of the Private Key because the activation data (e.g., password) has been compromised or for any other reason; and/or, o 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 EURCONTROL 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 as customer of EUROCONTROL 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 is deemed to have been accepted by the Certificate Holder after 8 calendar days of the receipt of the certificate and the corresponding password, via EUROCONTROL as LRA, by the Certificate Holder 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 found between the information in the NM 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 in the event of non-acceptance of the Certificate on its 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 LRA of all information used for the purposes of registration, 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 Relying 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 professional identity of the Certificate Holder and as a customer of EUROCONTROL; • Any requests for Certificates submitted to the CSP are complete, accurate, valid and duly authorized. 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 in the NM Agreement. • The LRAO checks the identity of the Certificate Holder. • The LRAO also verifies any information relating to the Certificate Holder's professional status for the purposes of certification, as indicated in Section E of this document. • As the Certificate Holder is a customer of EUROCONTROL, the LRAO validates there exists a contractual relationship with documentation available as proof of the existence of this relationship. • The LRAO ensures the storing of one copy of the information provided during registration procedure by the Certificate Holder, and in particular : o A copy of all information used to check the identity of the Certificate Holder and any references to its' professional status, including any reference numbers on documentation used for this verification as well as any limitations on its validity. o A copy of the NM Agreement signed by the Certificate Holder, including the latter's agreement to all obligations incumbent on him/her. o 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. o The validation procedure used by the LRAO for electronic Certificate applications guarantees that the Certificate Holder is in possession of the Private Key linked to the Public Key to be certified. o 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 LRA 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 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.). 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 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.	
E	***Identification and Authentication – Certified information***	**3.1**
	The following information is checked (see Section G of this CP: Certificate application procedure) and certified in the Certipost E-Trust Lightweight Certificate.	

Attribute	***Mandatory/ Optional/Fixed***	***Value***
Subject Attributes :		
Common Name (CN)	Mandatory	CCID (=unique EUROCONTROL customer number) to identify the EUROCONTROL customer as Certificate Holder
Pseudonym	Mandatory	Organization Name of the Certificate Holder, as it appears in the EUROCONTROL customer database.
SerialNumber	Mandatory	Unique number per CCID which identifies the computer account of the Certificate Holder using the NM web services If the value of the CCID is between 000 and 499, this concerns a production certificate. If the value of the CCID is between 500 and 999, this concerns a test certificate. *The sections A, B, C, D, F, G, H, I, J,K,L and M of this CP are not applicable in case of test certificates.*
countryName (C)	Mandatory	Country of the operational site of the Certificate Holder.
Extensions (not critical unless specified otherwise)		
KeyUsage	Fixed/Critical	digitalSignature (meaning the certificate may be used for authentication purposes only)
SubjectPublicKey	Mandatory	Public Key: Key length: 2048 bits (RSA); public exponent: Fermat-4 (=010001).

	CertificatePolicies PolicyIdentifier	Fixed	1.3.6.1.4.1.3860.1.2.112.1.1 In case of test certificates, this will become : 1.3.6.1.4.1.3860.1.2.112.2.1	
	CertificatePolicies PolicyIdentifier	Fixed	0.4.0.2042.1.3	
	CertificatePolicies-policyQualifier-userNotice	Fixed	"Lightweight Certificate Policy for EUROCONTROL. Not supported by SSCD, Key Generation by CSP. GTC, CP and CPS: http://pki.certipost.com" **In case of test certificates, this will become :** "Lightweight Certificate Policy for EUROCONTROL. *** Certificate for test purposes ***. Not supported by SSCD, Key Generation by CSP. GTC, CP and CPS: http://pki.certipost.com » *The sections A, B, C, D, F, G, H, I, J,K,L and M of this CP are not applicable in case of test certificates.*	
	CertificatePolicies-policyQualifier-CPS	Fixed	http://pki.certipost.com	
	crlDistributionPoint	Fixed	Certipost E-Trust Secondary Lightweight CA for EUROCONTROL: http://crl.e-trust.be/LWCA_EUROCONTROL.crl **or** Certipost Lightweight CA for EUROCONTROL: http://crl.pki.certipost.com/LWCA_Eurocontrol_v2.crl	
	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	Certipost E-Trust Secondary Lightweight CA for EUROCONTROL: http://ca.e-trust.be/LWCA_EUROCONTROL.crt **or** Certipost Lightweight CA for EUROCONTROL: http://certs.pki.certipost.com/LCA_Eurocontrol_v2.crt	
	Other information:			
	Issuer	Fixed	Certipost E-Trust Secondary Lightweight CA for EUROCONTROL: "CN = Certipost E-Trust Secondary LightWeight CA for EUROCONTROL O = Certipost s.a./n.v. C = BE" **or** Certipost Lightweight CA for EUROCONTROL: "CN = Certipost Lightweight CA for EUROCONTROL O = Certipost n.v./s.a. C = BE"	
	Validity	Mandatory	Maximum of 5 years	
	SerialNumber	Mandatory	Certificate sequence number	

	Algorithm	Fixed	Certipost E-Trust Secondary Lightweight CA for EUROCONTROL: "Sha1withRSAEncryption"	

			or Certipost Lightweight CA for EUROCONTROL: "sha256with RSAEncryption"	
	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 2048 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 (LCP).			
G	***Certificate-application procedure***			
	The EUROCONTROL LRAO's will ensure the collection of the Certificate Holders' and EUROCONTROLs' consent and information required for the completion of the Certificate Registration File. Once this has been done, the LRAO will proceed to the generation of the certificate, including the generation of the key pair, via the Certipost LRAO Administrator Interface.			
H.	***Issuing and delivery of the Certificate***			**4.2**
	The EUROCONTROL LRAO sends the Certificate (containing the private key) and the password to decrypt the private key, to the Certificate Holder via 2 different ways in accordance to EUROCONTROL internal procedures. The Certificate Holders' Private Keys are not archived.			
I	***Acceptance and publication of the Certificate***			**4.3**
	Publication The EUROCONTROL certificate will not be published into the CSPs' public repository. **Acceptance** The Certificate is deemed to have been accepted by the Certificate Holder after 8 calendar days of the receipt of the certificate and the corresponding password, via EUROCONTROL as LRA, by the Certificate Holder 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 it has noted between the information in the NM 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 its' part.			

J	***Procedure for Suspension, Unsuspension or Revocation***	4.4
	The Certificate Holder, the LRA or Certipost (further called the applicant), may apply for suspension, unsuspension or revocation of the Certificate. The Certificate Holder 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 of this document. 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** • The applicant must contact EUROCONTROL (cfr section M for contact details), acting as Suspension and Revocation Authority (SRA) of the CSP that issued the Certificate. • The SRAO (Suspension and Revocation Authority Officer) then calls back to obtain confirmation of the application for suspension. • The SRAO suspends the Certificate at latest the next working day after the application is received. A confirming e-mail or fax must be sent by the applicant to the SRA within 14 working days. The Certificate is otherwise unsuspended. • 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 not automatically revoked. In the case of **unsuspension following suspension** • The applicant must contact EUROCONTROL (cfr section M for contact details), acting as Suspension and Revocation Authority (SRA) of the CSP that issued the Certificate. • The SRAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the SRAO unsuspends the Certificate within 1 working day after the reception of the application. In the case of a **revocation**, the applicant must: • Apply for the suspension of the Certificate (see above). • The SRAO then verifies the documents submitted and the identity of the applicant. If the application is validated, the SRAO revokes the Certificate, at latest 1 working day after the application for revocation is received. • The period of investigation prior to the Certificate being revoked (or unsuspended) 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. The CSP ensures that the infor-	

	mation 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 Section G of this CP). If the CSP changes the General Terms and Conditions, it must communicate those changes to the Certificate Holders. 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 NM Technical Helpdesk: Telephone number: +32 2 745 1997 Fax number: +32 2 729 9023 E-mail address : cfmu.cso.help-desk@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, 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.	