TERMS OF USE

APPLYING TO THE

CORPORATE CERTIFICATES OF REGISTERED BODY

Before verifying the electronic certificate or accessing or using the information on state of certificates and other information contained in the EC-OMC Register, you (hereinafter, "the verifier") should read and accept these terms of use.

If the verifier checks an electronic certificate, accesses or uses the information about the state of certificates and other information contained in the EC-OMC Register, it will be understood that he accepts all the clauses of these terms of use.

The terms of issue of the corporate certificate of registered body, applying to the subscriber or owner of the certificate keys, are regulated in the applicable "General Terms of Issue".

In the event that the Verifier does not agree to all the conditions of these Terms of Use he shall abstain from carrying out any action that is related to the clauses contained herein. In this case, the EC-OMC assumes no responsibility

CLAUSES

ONE. - *Purpose*

1. These terms of use regulate the provision by the OMC of the information services on certificates, the status of the certificates and other information published at the Register, with regard to the certificates described in clause three of these terms of use.

2. These terms of use provide limited guarantees for the service offered, excluding any other guarantee, and also any responsibility that is not derived from the certification service offered to the verifier.

TWO. - *DPC and documentation of operations of the OMC*

1. The OMC Certification Services, object of these terms of use, are technically and operationally regulated by the Declaration of Certification Practices of the EC-OMC (hereinafter, the DPC) and its subsequent updates, and also by the complementary documentation published, in compliance with articles 18, and 19 of Law 59/2003, on electronic signature, at the following Internet address: http://www.cgcom.es/registro

2. The DPC and the operations documentation of the OMC, periodically modified, is included as reference in these terms of use. The verifier states he knows the latest version of the DPC; the legal aspects described in it that are contained in full in these terms of use.

3. The verifier undertakes to comply with the technical, operational and security requirements described in the DPC and in the operations documentation of the OMC.

4. In the event of disagreement, the significance of the terms contained in these terms of use shall prevail over those set out in the DPC.

THREE. - *The corporate certificate of registered body*

This document covers the following certificates:

NAME OF CERTIFICATE	OBJECT IDENTIFIER (OID) NUMBER	FUNCTIONS
Certificates of registered body on card	1.3.6.1.4.1.26852.1.1.4	Identification, signature and encipherment
Certificates of registered body on card (I)	1.3.6.1.4.1.26852.1.1.4.1	Identification
Certificates of registered body on card (F)	1.3.6.1.4.1.26852.1.1.4.2	Signature
Certificates of registered body on card (C)	1.3.6.1.4.1.26852.1.1.4.3	Encipherment

The corporate certificates of registered body are certificates qualified in accordance with the provisions set out in article 11.1, with the contents prescribed in article 11.2 and issued in compliance with the obligations of articles 12, 13, and 17 to 20 of Law 59/2003, of 19 December, on electronic signature.

Corporate certificates of registered body work with secure device for creating electronic signature, in accordance with article 24.3 of Law 59/2003, of 19 December, and they comply with the provisions laid down in the technical standards of the European Telecommunications Standards Institute, identified with reference TS 101 456.
The certificates are issued to registered bodies in the corporate scope of the subscriber medical association, and in no event are they issued to the public. This body is considered the owner of the respective keys and of the card and complementary software.

1. Certificate of registered body on card for identification, signature and encipherment.

This certificate has OID 1.3.6.1.4.1.26852.1.1.4.

The corporate certificates of registered body (identification, signature and encipherment) guarantee the identity of the subscriber and owner of the private identification key and signature, and permit the "qualified electronic signature" to be generated; in other words, the advanced electronic signature which is based on a qualified certificate and which has been generated using a secure device, for which, as set out in article 3 of Law 59/2003, of 19 December, it has a status equal to the written signature, for legal effects, without having to fulfil any other additional requirement.

They likewise include a declaration concerning the category and organic office of the owner of keys, that have been verified before issuing the certificate, and are correct. It should be pointed out that this indication is not, in itself, sufficient to determine the powers which the owner of keys holds in order to sign on behalf of the subscriber; consequently the user of the certificate will have to verify the signature authorities and powers of the owner by means other than the certificate, for example the OMC validation service.

On the other hand, the corporate certificates of registered body (identification, signature and encipherment) may be used in applications that do not require electronic signature equivalent to written signature, but only the identification of the owner of the keys, in the name of the subscriber, such as the applications which are indicated below:

a) Authentication in access control systems.
b) Secure electronic mail signature.
c) Other digital signature applications.

The electronic signature generated in the use of these applications will have the effects determined in the regulatory standards of the application, which may declare the equivalence with the written signature or only the identification effect, because this signature, at least, will have been produced with the secure device.
Lastly, the corporate certificates of registered body (identification, signature and encipherment) may be used to encipher own documents or to receive confidential documents, in any format, protected by the encipherment of the document using:

a) The public key of the owner of keys indicated in the certificate.
b) An encipherment key to session, symmetric, ciphered with the public key of the key owner indicated in the certificate.

In all events, the owner of the key shall use his private key to decipher the message, warning the subscriber of the certificate and the owner of the key that in no event can a lost key be recovered, so that the CGCOM will not respond for any loss of enciphered information that cannot be recovered in cases of loss of certificates or keys.

2. Certificates of registered body on card for identification

This certificate has OID 1.3.6.1.4.1.26852.1.1.1.4.
The corporate certificates of registered body (identification) guarantee the identity of the subscriber and owner of the private identification key.

3. Certificates of registered body on card for signature

This certificate has OID 1.3.6.1.4.1.26852.1.1.4.2.
The corporate certificates of registered body (signature) guarantee the "qualified electronic signature" to be generated; in other words, the advanced electronic signature which is based on a qualified certificate and which has been generated using a secure device, which, as set out in article 3 of Law 59/2003, of 19 December, has a status equal to the electronic signature, for legal effects, without having to fulfil any other additional requirement.

They likewise include a declaration concerning the category and organic office of the owner of keys, that they have been verified before issuing the certificate, and are correct. It should be pointed out that this indication is not, in itself, sufficient to determine the powers which the owner of keys has in order to sign on behalf of the subscriber; consequently the user of the certificate will have to verify the signature authorities and powers of the owner by other different means to the certificate, for example the OMC validation service.

On the other hand, the corporate certificates of registered body (signature) may be used in applications that do not require electronic signature equivalent to written signature, such as the applications which are indicated below:

a) Secure electronic mail signature.
b) Other digital signature applications.

The electronic signature generated in the use of these applications will have the effects determined in the regulatory standards of the application, which may declare the equivalence with the written signature or only the identification effect, because this signature will at least have been produced with the secure device.

4. Certificates of registered body on card for encipherment

This certificate has OID 1.3.6.1.4.1.26852.1.1.4.3.

The encipherment certificates may be used to cipher own documents or to receive confidential documents, in any format, protected by the encipherment of the document using:
The public key of the owner of keys indicated in the certificate.
An encipherment key to session, symmetric, ciphered with the public key of the key owner indicated in the certificate.

In all events, the owner of the key shall use his private key to decipher the message, warning the subscriber of the certificate and the owner of the key that in no event can a lost key be recovered, so that the CGCOM will not respond for any loss of enciphered information that cannot be recovered in cases of loss of certificates or keys.

FOUR.- Licence of use of the Certificate

1. Reservation of rights

All accessible contents with regard to the provision of the certification services, the specific one of the corporate certificate of registered body, and the specifications, cards, marks and other applications entailed with their use are subject to intellectual and industrial property rights of the EC-OMC or other third parties which own them.

In no event does the provision of those services imply any kind of waiver, transfer or total or partial assignment of other rights which are expressly recognised to them and granted in these Terms of Use.

2. Licence of use of the corporate certificate of registered body

The EC-OMC grants the Verifier the non-exclusive and non-transferable licence of use of the corporate certificate of registered body and of the information about its status, for the sole, exclusive purpose of providing him the services and permitting the use of the certificate in accordance with these Terms of Use.

3. Non-existence of suitability guarantee

The EC-OMC cannot guarantee that the use of the corporate certificate of registered body and related IT applications allows the Verifier to obtain or cover needs, data or purposes of any nature, other than those

which may be reached through their use, according to their own nature and as deduced from their licence of use.

4. Limitations in use and prohibited uses

The corporate certificate of registered body shall only be used within the limits of use set out expressly in their licence of use and in these Terms of Use. Any other uses other than those described in this clause are expressly excluded from the present scope of contract and are formally forbidden.

The certificate has not been designed, cannot be used and its use or resale is not authorised as control devices of dangerous situations or for uses that require fail-safe actions, such as the functioning of nuclear plants, navigation systems or air communications, or weapons control systems, where a failure could directly lead to death, personal injuries or severe environmental damage.

5. Term of licence

The corporate certificates of registered body shall have a maximum term of validity of three (3) years counted from their date of issue, after which they shall not be used.

The expiry date of the certificates will be displayed on the actual certificates.

FIVE. - *Obligations of the verifier*

1. Informed decision

OMC informs the verifier, who is deemed notified, that he has access to sufficient information to adopt an informed decision at the time of verifying a certificate and trusting the information contained in the certificate.

In addition, the verifier recognises that the use of the Register and the Lists of Revoked Certificates (hereinafter, "the LRCs" or "the CRLs) of the OMC, is ruled by the DPC of the EC-OMC and he undertakes to comply with the technical, operational and security requirements described in that DPC of the EC-OMC.

2. Verification requirements of the electronic signature

Before ciphering a message or document by an individual, the addressee's public key must be used. This public key can be obtained from his corporate certificate of registered body.

This certificate must therefore be verified before being ciphered.

The verification of the electronic signature of the certificate is essential to determine that the public key contained in the certificate corresponds to the owner and that the respective private key permits the deciphering of the message.

This verification will normally be executed automatically by the verifier's software and, in all events, in accordance with the DPC, with the following requirements:

a) The suitable software must be used to verify the digital signature of the corporate certificate of registered body with the algorithms and lengths of keys authorised in the certificate and/or to

execute any other cryptographic operation, and establish the chain of certificates on which the electronic signature to be verified is based, because the electronic signature is verified using this chain of certificates.

b) It must be ensured that the chain of certificates identified is the most suitable for the electronic signature that is verified, because an electronic signature may be based on more than one chain of certificates, and it is up to the verifier to ensure that the most suitable chain is used in order to verify it.

c) The revoke state of the certificates of the chain must be verified with the information supplied in the EC-OMC Register (with LRCs, for example) to determine the validity of all the certificates of the chain of certificates, because an electronic signature can only be considered correctly verified if each and every one of the certificates in the chain are correct and valid.

d) It must be ensured that all certificates in the chain authorise the use of the private key for the certificate subscriber and the key owner, because of the possibility that any of the certificates may include limits in use that impede trusting the electronic signature that is verified. Each certificate in the chain has an indicator which refers to the applicable terms of use, for their review by the verifiers.

e) The signature of all the certificates in the chain must be technically verified before trusting the certificate used by the signatory.

f) Determine the date and hour of generating the electronic signature, because the electronic signature can only be considered correctly verified if it was created within the term of effectiveness of the chain of certificates on which it is based.

g) Define the data which have been digitally signed, because these will be used when verifying the signature.

h) Technically verify the actual signature with the certificate of the signatory guaranteed by the chain of certificates.

3. Due diligence

The verifier shall act with maximum diligence before trusting the certificates. The verifier specifically undertakes to use electronic signature verification software with sufficient technical, operational and security capacity to correctly execute the signature verification process, and he shall continue to be the exclusive party responsible for any damage which he might undergo from an incorrect choice of that software.

The above provision shall not apply when the EC-OMC has supplied the verifier the verification software.

The verifier may trust a certificate when the following conditions concur:

a) It must be possible to verify the electronic signature in accordance with the requirements set out in item 4.2.

b) The verifier shall have used updated revoke information at the time of verifying the signature.

c) The type and class of certificate must be suitable for the use which it is intended making.

d) The verifier must consider other additional limitations in use of the certificate which are indicated in any form in the certificate, even those not automatically processed by the verification software, included by making reference to the certificate, and contained in these terms of use. In particular, a certificate does not constitute a concession of rights and authorities by the OMC to the subscriber or to the key owner, other than the description of the certificate according to clause 3.1 or some other specific indication by the EC-OMC or by the actual subscriber.

e) Lastly, the certificate shall be reasonably trustworthy according to the circumstances. If the circumstances require additional guarantees, the verifier must obtain these guarantees for this to be reasonably trustworthy.

In any case, the final decision with regard to trusting or not trusting a verified certificate lies exclusively with the verifier, who shall adopt an active attitude and who is required to provide access to all the information provided by the EC-OMC in order to adopt his decisions in a fully informed manner. When in doubt, the Verifier shall not trust the corporate certificate of registered body.

4. Trust in a non-verified signature

It is forbidden to cipher messages or documents by an addressee without having successfully verified his certificate.

If the verifier trusts a non-verified certificate, he will assume all the risks arising from this action.

5. Effect of the verification

By reason of the correct verification of the corporate certificate of registered body, in accordance with these terms of use, the verifier may trust the identification and, if applicable, the public key of the key owner, within the respective limitations in use.

6. Correct use and forbidden activities

The verifier undertakes not to use any kind of information on state of the certificates or of any other class that has been supplied by the EC-OMC, in performing any act prohibited by the applicable law.

The verifier undertakes not to inspect, interfere, or carry out inverse engineering in the technical implementation of the public certification services of the EC-OMC, without the previous written consent of the EC-OMC.

In addition, the verifier undertakes not to intentionally compromise the security of the public certification services of the EC-OMC.

The digital certification services provided by the EC-OMC have not been designed nor do they permit the use or resale, as control equipment of dangerous situations or for uses that require error-free actions, such as the operation of nuclear facilities, navigation systems or air communication, air traffic control systems,

or weapons control systems, where an error could cause death, physical damage or serious environmental damage.

SIX. - *Obligations of the EC-OMC*

1. Relating to the provision of the certificates verification service

The EC-OMC undertakes to provide the service in certain technical and operational conditions, as set out in the DPC of the EC-OMC, including a Register of certificates, where information about the state of the certificates is published.

The EC-OMC undertakes to issue information about the state, including suspension and revoke, of the certificates issued, in accordance with the DPC, and also assume its responsibilities with the verifiers, always within the limits of use established for the certificates.

2. Limited guarantee of the EC-OMC

The EC-OMC guarantees the verifier the following service conditions:

a) The certificate contains correct and updated information at the time of issue, duly verified, in accordance with the provisions set out in Law 59/2003, of 19 December.

b) The certificate fulfils all the requirements concerning the contents and format which are established in the DPC.

c) The private key of the EC-OMC has not been committed, except when otherwise notified by the Register.

SEVEN. - Responsibility

1. Responsibility of the verifier

The verifier will respond for non-fulfilment in his contractual obligations or for negligence.

The verifier undertakes to hold the EC-OMC harmless of any act or omission from which all classes of damage may result, including:

a) Non-fulfilment of the verifier's own obligations.

b) The trust in a certificate is not reasonable.

c) The non-fulfilment of the obligation to verify the state of a certificate to determine whether it has expired or has been suspended or revoked.

2. Responsibility of the EC-OMC

The EC-OMC will respond for non-fulfilment of the obligations which, in each case, is imposed by Law 59/2003, of 19 December, on electronic signature or for negligence, except in the following cases:

a) The EC-OMC will not be responsible for damage caused for the information contained in the certificates, provided these are correct and updated at the time of issue of the certificate.

b) The EC-OMC will not be responsible for any direct or indirect, special, incidental, emergent damage, for any loss of profit, loss of data, punitive, foreseeable or non-foreseeable damage, deriving from the use, remittance, licence to third parties, functioning or non-functioning of the certificates in a system not provided by the EC-OMC, and also for the digital signatures or any other transaction or service described in the DPC, when used outside the certification service of the EC-OMC and the EC-OMC verification services.

EIGHT. - *Protection of personal data*

The verifier acknowledges that certain information concerning digital certificates contain personal data, holdership of the key owners and, if applicable, of the certificate subscribers.

In the event that the verifier should receive any kind of personal information from the EC-OMC in execution of the present terms of use, he undertakes to use it for the exclusive purpose of verifying the personal identity of the signatory and the electronic signatures of his messages or documents.

He furthermore undertakes to protect the personal data in accordance with the provisions set out in Organic Law 15/1999, of 13 December, on personal data protection, and in particular he undertakes to establish the suitable security measures, in accordance with article 9 of Organic Law 15/1999, and rules of implementation.

The verifier shall have sole responsibility for the incidents derived from the infringement of these personal data protection obligations and undertakes to hold the EC-OMC harmless from any damage arising from these incidents.

NINE. - *Infractions in third party rights*

The EC-OMC accepts no responsibility if the remittance to the EC-OMC, by the subscriber or by the key owner, for including in the certificate, and the use of a domain and/or any other type of name or denomination, and any other application information of the certificates, should infringe the rights of any person in any jurisdiction with regard to its registered trademarks, service trade marks, trade names or any other intellectual or industrial property right, or if the subscriber or owner of keys intends using the domain and distinguished names for any illegal purpose, including, by way of illustration only and without limitation, the fraudulent infraction of a contract, or obtaining possible commercial advantages, unfair competition, attack on its right to honour, and the confusion or deceit of an individual or legal entity.

The EC-OMC shall not be held responsible for the legality of the information which it has been notified by the subscriber or by the key owner, for including in the certificates issued by the EC-OMC, in any jurisdiction in which this may be used or viewed.

TEN. - *Divisibility of the terms of use*

The clauses of these terms of use are independent *per se*, for which reason if any clause is considered invalid or inapplicable, the other clauses of these terms of use shall continue to apply, unless otherwise expressly agreed by the parties.

ELEVEN. - *Applicable law and competent jurisdiction*

These terms of use shall be interpreted, and shall be executed in their own terms, and in any matters not foreseen herein, the parties shall be ruled by Law 59/2003, of 19 December, by the civil and mercantile legislation that rules the system of obligations and the contracts.

The competent jurisdiction is the jurisdiction indicated in Law 1/2000, of 7 January, on code of civil procedure.