TERMS OF USE

FOR

SOFTWARE PERSONAL CORPORATE CERTIFICATES

Prior to the verification of the electronic certificate, or to access or use the certificate status information and other information contained in the Repository of ANCERT, you (hereinafter "the verifier") must read and accept these terms of use.

If the verifier checks an electronic certificate, accesses or uses the certificate status information and other information contained in the Repository of ANCERT, it shall be understood that all provisions of these terms of use are accepted.

CLAUSES

FIRST. –Object

1. These conditions of use regulate the provision, by ANCERT, of certificate information services, certificate status and other information published in the Repository, in relation to the certificates described in clause three of these conditions.

2. These terms and conditions include limited warranties for the services provided, excluding all other warranties and liabilities that do not arise from the certification services provided to the verifier.

SECOND. - DCP and documentation of ANCERT operations

1. Certification Services provided by ANCERT and object of the present conditions of use are governed technically and operationally by the Declaration of Certification Practices of the Certification Entity ANCERT General Council of Notaries (hereinafter the DCP) and its subsequent updates, as well as complementary documentation published to comply with Article 19 of Law 59/2003 on electronic signature at the following Internet address: [https://www.ancert.com/condiciones/]

2. The DCP and documentation of ANCERT operations, amended periodically, are incorporated into these terms of use by reference. The verifier declares to know the last version of the DCP , whose legal aspects described therein are fully included in these conditions.

The verifier is committed to complying with the technical, operational and security requirements as described in the DCP and the documentation of ANCERT operations.

4. In case of discrepancy, the meaning of the terms contained in these terms and conditions shall prevail over provisions of the DCP.

THIRD Description of software personal corporate certificate

The Notarial Certification Agency issues software corporate certificates for authentication to private corporations that act as Registration Authorities for their employees.

The Registration Authority identifies and verifies the requestor's personal circumstances, and ensures their sufficient capacity and legitimacy and that the consent was freely given, and according to the law and the will duly informed.

Software personal corporate certificates can be used for three functionalities, each one with a different certificate:

- Generation of advanced electronic signature based on a qualified certificate
- Personal authentication in electronic information systems, in physical presence or distance
- Encryption and decryption of electronic documents, with key recovery.

Software Corporate Personal Certificates guarantee the authenticity of the issuer, the non-repudiation of origin and content integrity:

1) Authenticity of the issuer: the document or electronic communication comes from the signature creation device of the person or entity who claims to be from

   This feature is accomplished by the use of advanced electronic signature. The recipient of an electronically signed message can verify the signature using the subscriber's certificate.

2) Non-repudiation: the issuer of a particular message can not deny the issue of it or its contents, if that benefits him. This feature is accomplished by the use of advanced electronic signature. The recipient of an electronically signed message can verify the signature using the subscriber's certificate. De esta forma puede demostrar la identidad del emisor del mensaje sin que éste pueda repudiarlo.

3) Integrity: an electronic document, signed with advanced electronic signature, has not been modified by any external agent To ensure integrity, cryptographic methods as mathematical summary functions (hash functions) are used in combination with the digital signature This method is based on a single summary of the electronic document, digitally signed with the subscriber's private key so that any alteration of the document causes a modification of its summary

Software personal corporate certificate can include, besides identification data of the subscriber, data of the key holder in accordance with Article 11 of Law 59/2003 on Electronic Signatures

Software personal corporate certificates are certificates in the terms of Article 6 of Law 59/2003 of Electronic Signature, ie documents electronically signed by a Certification Services Provider which bounds signature-verification data to a signatory and confirms their identity.

Conventional software storage (PCKS # 12) is used as support of the Certificates.

These certificates are electronic certificates to generate the advanced electronic signature that guarantees the identity of the subscriber, and they can be used with secure signature creation devices.

Software personal corporate certificates can be used to encrypt or decrypt electronic documents under the sole responsibility of the person identified as the subscriber. All legal liabilities, contractual or extra contractual, direct or indirect damages derived from such uses fall under the responsibility of the subscriber.

Under no circumstances may the private corporation, the subscriber or injured third parties claim the Notarial Certification Agency or the General Council of Notaries any compensation for damages or liabilities derived from the use of keys or certificates for encryption.

Hardware personal corporate certificate for authentication are identified by the object identifier (OID): 1.3.6.1.4.1.18920. 2.1.1.2.4

It is not permitted to use software personal corporate certificates for prohibited uses, such as: A título enunciativo, se prohíbe el uso de los Certificados Corporativos Personales sin dispositivo seguro de creación de firma para:

1) purposes other than pre established.
2) sign end entities certificates or software applications.
3) generate timestamps.
4) provide services of electronic invoicing, OCSP, CRL generation or notification services.
5) purposes contrary to the current Spanish Law regarding electronic signature or certification services.
6) purposes contrary to the provisions of the DPC and these terms of use.

Also, certificates should be used only in accordance with applicable law, taking into account the restrictions on imports and exports in each moment.

Software personal corporate certificates are issued without limits on the amount of financial transactions.

2. Intellectual Property

The verifier recognizes that ANCERT owns all issued certificates, and specifications, cards and brands without prejudice to the rights of third parties.

Duration of the Certificate

Software personal corporate certificates will have maximum validity period of three (3) years from the date of issuance, after which they will not be used

The expiration date of certificates shall be included in the certificates.

FOURTH. -Obligations of the verifier

1. Informed decision

ANCERT informs the verifier that enough information is provided to make an informed decision when verifying a certificate and trust the information contained in the certificate.

Additionally, the verifier recognizes that the use of the Repository and Certificate Revocation Lists (hereinafter "the CRLs" or "CRL") of ANCERT, is governed by the DCP, and undertakes to fulfill the technical, operational and security requirements described in the DCP.

2. Requirements for electronic signature verification

To trust a message or document, the verifier must validate two signatures:

- First, it has to be verified the electronic signature of the message or document. This check is essential to determine that the signature was generated by the subscriber, using the private key corresponding to the public key contained in the software personal corporate certificate, and to ensure that the message or document was not modified after the generation of the electronic signature

Secondly, it has to be verified the electronic signature of the software personal corporate certificate belonging to the subscriber. This check is necessary to determine that the public key contained in the software personal corporate certificate corresponds to the subscriber

This check is normally performed automatically by the verification software and, in any case, taken into account the following requirements according to the DCP:

a) It is necessary to use the appropriate software for verifying the digital signature of the hardware personal corporate certificate with the algorithms and key lengths authorized in the certificate, and/or implementing any cryptographic operation and establish the certification chain on which is based the electronic signature to verify, since the electronic signature is verified using this certification chain.

b) It is necessary to ensure that the identified certification chain is the most appropriate for the electronic signature to be verified, as an electronic signature may be based on more than one certification chain, and is up to the verifier to ensure the use of the most suitable one.

c) It is necessary to check the revocation status of certificates in the chain with the information provided in the Repository of ANCERT Personal Corporate Certificates (with CRLs, for example) to determine the validity of all certificates of the certification chain, as it can only be considered an electronic signature properly verified if each and every one of the certificates in the chain is valid and not expired.

d) It is necessary to ensure that all certificates in the chain authorize the use of the private key by the subscriber and the key holder, because of the possibility of the existence of limits on use that prevent trusting the electronic signature. Each certificate in the chain has an indicator that refers to the applicable conditions of use.

e) It is necessary to verify technically the signature of all certificates in the chain before trusting the certificate used by the signer.

Required diligence

The verifier must act with the utmost care before trusting the certificates. In particular, the verifier is obliged to use software for electronic signature verification with the technical, security and operational capacity enough to perform the signature verification process correctly, and will remain solely responsible for the damage it may suffer from the incorrect choice of the software.

The above limitation shall not apply if the verification software has been provided by ANCERT.

The verifier can trust a certificate under the following conditions:

a) The electronic signature should be verifiable in accordance with the requirements of section 4.2.

b) The verifier must have used updated revocation information at the time of signature verification.

c) The type and class of certificate must be appropriate for the intended use.

d) The verifier must take into account other additional limitations on use of the certificate, including those not processed automatically by the verification software, incorporated by reference to the certificate, and contained in these conditions. In particular, a certificate does not constitute a grant of rights and powers by ANCERT to the subscriber, beyond the description of the certificate under clause 3, or other explicit indication by ANCERT or the subscriber.

e) Finally, trust must be reasonable under the circumstances. If circumstances require additional guarantees, the verifier must obtain such guarantees.

In any case, the final decision to trust or not a verified certificate is the sole responsibility of the verifier.

4. Trusting a non-verified signature

It is strictly forbidden trusting a non verified signature or certificate.

If the verifier trusts a certificate that has not been verified, he will assume all risks associated with this action.

5. Effect of verification

Under the correct verification of the hardware personal corporate certificate, and in accordance with these terms of use, the verifier can rely on the identification and, where appropriate, in the public key of the subscriber, within the limitations for use.

6. Proper use and prohibited activities

The verifier is obliged not to use any type of status information of certificates (or any other type) that has been provided by ANCERT, in performing any act prohibited by applicable law.

The verifier is obliged not to inspect, interfere with or reverse engineer the technical implementation of the public certification services provided by ANCERT, without prior written consent of ANCERT.

Additionally, the verifier agrees not to intentionally compromise the security of the public certification services provided by ANCERT.

Digital certification services provided by ANCERT are not designed, neither can be used or resold for control equipment in dangerous situations or for uses requiring fail-safe performance, such as operation of nuclears, air navigation and communication systems, or weapon control systems, where failure could lead directly to death, personal injury or severe environmental damage.

FIFTH. - Obligations of ANCERT

1. Relating to the certificate verification services

ANCERT agrees to provide the service in certain technical and operational conditions, according to the DCP, including a repository of certificates for publishing information on the status of certificates.

ANCERT is obliged to issue status information, including suspension and revocation, for all issued certificates, in accordance with the DCP, and to assume its responsibilities in front of verifiers, always within the limits of use of the certificates.

2. Limited Warranty of ANCERT

ANCERT warrants to the verifier the following conditions of service

a) The certificate contains information accurate and current at the time of issuance, duly established in accordance with the provisions of Law 59/2003 of December 19th.

b) The certificate meets all requirements for content and format established in the DCP.

c) The subscriber's private key has not been compromised, unless notification to the contrary by the registry.

SIXTH. –Responsibility

1. Responsibility of the verifier

The verifier is liable for breach of its contractual obligations or for negligence.

The verifier is obliged to keep ANCERT harmless from any act or omission resulting in damages of any kind, including:

a) Failure to comply with the obligations of the verifier.

b) Unreasonable confidence in a given certificate.

c) The failure to check the status of a certificate to determine if it has expired or has been suspended or revoked.

2. Responsibility of ANCERT

ANCERT is liable for breach of obligations imposed by law 59/2003 of December 19th on electronic signature, or by negligence, except as follows:

a) ANCERT will not be liable for damages caused by the information contained in the certificates, provided that they are accurate and current at the time of issuance of the certificate.

b) ANCERT will not be liable for any direct or indirect damage, special, incidental, loss of data, punitive damages, foreseeable or unforeseeable, arising from the use, delivery, sublicensing, good or bad functioning of certificates in a system not supplied by ANCERT, as well as digital signatures or any other transaction or service described in the DCP, when used outside the certification and verification services provided by ANCERT.

SEVENTH. - Privacy Policy

The verifier recognizes that certain information on digital certificates contain personal data, held by the subscribers of certificates.

If the verifier receives from ANCERT any personal information then agrees to use it for the sole purpose of verifying the identity of the signer and the electronic signatures of his messages or documents.

The verifier also agrees to protect personal data in accordance with the provisions of Organic Law 15/1999 of December13th on the protection of personal data, in particular for the establishment of appropriate security measures in accordance with Article 9 Organic Law 15/1999.

The verifier shall be solely responsible for any incidents arising from the infringement of these obligations for the protection of personal data, undertaking to indemnify ANCERT for all damage resulting from these incidents.

EIGHTH. - Violations of third party rights

ANCERT is not responsible that the use of a domain and/or other name or designation, or any other information included in the certification request violate the rights of any person in any jurisdiction with respect to its trademarks, service marks, trade names or any other

rights of intellectual property, or that the subscriber intends to use the domain and distinguished names for any unlawful purpose, including, without limitation, breach of contract with fraudulent intent, or obtaining any commercial advantage, unfair competition, infringement of the right to honor, and confusion or deception of a person, both natural and legal.

ANCERT is not responsible for the legality of the information that has been sent by the subscriber for inclusion in the certificates issued by ANCERT, in any jurisdiction in which it may be used or displayed.

NINTH. - Severability of Terms of Use

The provisions of these Terms of Use are independent of each other so that if any provision is invalid or unenforceable, the remaining provisions of these Terms of Use shall remain applicable, except explicit agreement by the parties.

TENTH.-Intellectual and Industrial Property

ANCERT is the exclusive holder of all rights, including rights of exploitation, on the Directory of Certificates and the Certificate Revocation List in accordance with the Law of Intellectual Property approved, including the sui generis right recognized in Article 133 of this law.

Access to the Repository of Certificates and Certificate Revocation Lists is permitted, but is forbidden the reproduction, public communication, distribution, or conversion unless expressly authorized by ANCERT or the Law.

Also, ANCERT owns all the same rights of intellectual property with respect to these Terms and the information related to the provision of certification services (for subscribers, is only granted a right of use).

OIDs own by ANCERT have been registered in the IANA (Internet Assigned Number Authority) under the branch 1.3.6.1.4.1., having been assigned the number 18920 (ANCERT). This information is public: http://www.iana.org/assignments/enterprise-numbers

It is prohibited partial o total use of any of the OID assigned to ANCERT except for allowed uses of Certificates or Certificates Directory.

All unauthorized extraction and/or reuse of the contents of the databases that ANCERT makes available to its subscribers, is also prohibited.

ELEVENTH.- - *Disclaimer*

The Notarial Certification Agency will limit its liability to the issuing and managing of certificates and, where appropriate, managing of subscriber's key pairs and cryptographic

devices (for signing and signature verification, and encryption or decryption) supplied by the Notarial Certification Agency.

Third parties who trust certificates agree to indemnify the Notarial Certification Agency for any damage arising from any act or omission resulting in liability, damage or loss, expense of any kind, including judicial and legal representation that may be incurred by the publication and use of the certificate, under one of the following reasons:

- Breach of the obligations of third parties who trust certificates.
- Unreasonable confidence in a certificate.
- Negligence in the verification of the status of a certificate, to determine if it is suspended or revoked.

TWELFTH. - Severability of Terms of Use

The provisions of these Terms of Use are independent of each other so that if any provision is invalid or unenforceable, the remaining provisions of these Terms of Use shall remain applicable, except explicit agreement by the parties.

THIRTEENTH . -Applicable law and jurisdiction

These conditions shall be interpreted and will be executed in its own terms and, in all matters not provided, the parties shall be subject to Law 59/2003 of December 19th, to administrative law applicable and, secondarily, by civil and commercial law that regulates the system of obligations and contracts.

The competent Jurisdiction is according the provisions of Law 1/2000, of January 7th, on Civil Procedure.