PUBLIC EMPLOYEE HIGH LEVEL CERTIFICATE

INFORMATIVE TEXT APPLICABLE

This document contains the essential information to know in relation to the entity's certification ESFIRMA certification service.

1. Contact information

1.1. Organization responsible for

The ESFIRMA certification entity, hereinafter "ESFIRMA", is an initiative of:

AULOCE S.A.U. (esFIRMA)

CALLE BARI 39 (Bldg. Binary Building)

50197 ZARAGOZA

(+ 34) 976300110

1.2. Contact

For any inquiry, please contact:

AULOCE S.A.U. (esFIRMA)

CALLE BARI 39 (Bldg. Binary Building)

50197 ZARAGOZA

(+ 34) 976300110

1.3. Contact for reversal processes

For any inquiry, please contact:

AULOCE S.A.U. (esFIRMA)

CALLE BARI 39 (Bldg. Binary Building)

50197 ZARAGOZA

(+ 34) 976579516

2.Type and purpose of the certificate

This certificate provides the OID 1.3.6.1.4.1.47281.1.1.1 for identification and signature.

Public employee high level certificates are certificates recognized in accordance with in article 11(1), the content prescribed by article 11.2 and issued to fulfilling the obligations of articles 12, 13, and 17 to 20 of law 59/2003, of 19 December, eSignature.

These certificates are issued to public servants to identify them as persons in the service of the Administration, agency, or entity of public law, linking them with this, fulfilling the requirements laid down in law 11/2007, of 22 June, of electronic access of citizens to public services and its implementing regulations.

Public employee high level certificates work with device secure signature creation, in accordance with article 24.3 of the law 59/2003, of 19 December, signature, and give compliance provisions of the regulations by the European Telecommunications Standards Institute, technical identified with TS 101 456 reference. In addition, certificates of individual high level public employees are issued in accordance with the scheme of identification and electronic signature of public administrations in their up-to-date version to date of this document.

These certificates guarantee the identity of the Subscriber and the signer, and allow the generation of the "recognized electronic signature"; i.e., the advanced electronic signature based on a qualified certificate and which has been generated using a secure device, which in accordance with the provisions of article 3 of law 59/2003, of December 19, equates the firm written by legal effect, without any other additional requirement.

They can also be used in applications that do not require the electronic signature equivalent to the written signature, like the applications listed below:

a) Safe email.

b) Other digital signature applications.

EsFIRMA does not offer backup and key recovery services. Therefore esFIRMA is not liable under any circumstances for loss of encrypted information that cannot be recovered.

Applications in the profile of certificate information indicates the following:

a) The "key usage" field is activated, and therefore allows to perform the following functions:

to. Digital signature (Digital Signature for authentication)

b. Commitment to content (Content commintment to perform the function of electronic signature)

b) "Qualified Certificate Statements" field contains the following statement:

to. QcCompliance (0.4.0.1862.1.1), which advises that the certificate is issued as recognized.

b. QcSSCD (0.4.0.1862.1.4), which advises that the certificate is used exclusively in conjunction with a secure signature-creation device.

2.1. CA certification

Certificates of individual high level public employees are issued by ESFIRMA, identified using the contact details listed above.

3. Limits of use of the certificate

3.1. Limits of use for signers

The signer must use the service of certification provided by ESFIRMA exclusively for the purposes authorized in the contract signed between ESFIRMA and the Subscriber, and playing later (section "obligations of the signatories").

Also the signatory undertakes to use the service of digital certification in accordance with the instructions, manuals or procedures provided by ESFIRMA.

The signer should meet any law and regulation that may affect your right to use the cryptographic tools that use.

The signer cannot take measures of inspection, alteration, or reverse engineering of the services of ESFIRMA digital certification, without express permission.

3.2. Limits of use for verifiers

Certificates are used to its own function and purpose established, unless they can be used in other functions and for other purposes.

Similarly, certificates must be used only in accordance with applicable law, especially taking into account restrictions on import and export existing at all times.

Certificates cannot be used to sign petitions for issuance, renewal, suspension or revocation of certificates, or to sign any public key certificates, or to sign lists of revoked certificates (CRL).

Certificates are not designed, do not they can allocate and does not authorize its use or resale as control equipment in hazardous situations or for applications that require actions to be judgment proof, as the operation of nuclear facilities, navigation systems or air communications systems of arms control, where a failure could directly lead to the death, personal injury, or severe environmental damage.

Should take into account the limits indicated in the various fields of the certificate profiles, visible on the web (https://www.esfirma.com).

The use of digital certificates in operations that contravene this text of disclosure, or contracts with subscribers, it is abuse to the legal effects appropriate, exempting both to ESFIRMA, according to the legislation in force, of any responsibility for this misuse of certificates that make the signer or any third party.

ESFIRMA does not have access to the data on which the use of a certificate can be applied. Therefore, and as result of this technical impossibility of access to the contents of the message, is not possible by ESFIRMA rating any content the above, assuming therefore the Subscriber, the signatory or the person responsible for the custody, any resulting liability of content coupled with the use of a certificate.

In addition, it will be attributable to the Subscriber, the signatory or the person responsible for the custody, any liability that might arise from the use of the same outside the limits and conditions of use that are collected in this text of disclosure, or in contracts with subscribers, as well as of any other improper use of the same derivative of this section or which can be interpreted as such according to the legislation in force.

4. Obligations of subscribers

4.1. Key generation

Subscriber authorizes ESFIRMA to generate private and public keys for identification and electronic signatures of the signatories, and requested the issuance of the certificate of high level civil servant in his name.

4.2. Certificate request

The subscriber undertakes to perform requests for certificates in accordance with the procedure and, if necessary, the technical components supplied by ESFIRMA, in accordance with what is established in (DPC) certification practice statement and the documentation of ESFIRMA operations.

4.3. Information obligations

The Subscriber responsible for the information included in your certificate application is accurate, comprehensive for the purpose of the certificate and is up to date at all times.

Subscriber must promptly inform ESFIRMA:

- Of any inaccuracies detected once the certificate has been issued.
- The changes that occur in the information provided or for the issuance of the certificate.
- Of the loss, theft, abduction, or any other kind of loss of control of the private key by the signatory.

4.4. Obligations of custody

The subscriber undertakes to safeguard the information that generates in his activity as a Registrar's.

5.obligations of the signatories

5.1. Obligations of custody

The signatory undertakes to safeguard the personal identification code or any technical support delivered by ESFIRMA, private keys and, if necessary, specifications owned by ESFIRMA that are supplied. The signatory undertakes to keep personal identification (PIN) code.

In case of loss or theft of the private key of the certificate, or in case that the signatory suspected that the private key has lost reliability for any reason, such circumstances must be notified immediately to ESFIRMA by means of the Subscriber.

5.2. Obligations of proper use

The signer must use the service of certification of certificates of individual public employees high level provided by ESFIRMA, exclusively for authorized in the DPC and applications in any other instructions, manual or procedure provided to the Subscriber.

The signer must meet any law and regulation that may affect your right to use the employed cryptographic tools.

The signer may not adopt measures of inspection, alteration or decompilation of digital certification services.

The signer will recognize:

a) That when you use any certificate, and the certificate has not expired or has been suspended or it has been revoked, this certificate will be accepted and will be operational.

b) Which does not act as a certification authority, and therefore undertakes not to use the private key corresponding to the public key contained in the certificates for the purpose of signing any certificate.

c) That in case of compromised private key, its use is immediately and permanently suspended.

5.3. Prohibited transactions

The undersigned undertakes not to use their private keys, certificates or any other technical support delivered by ESFIRMA in the accomplishment of some transaction prohibited by applicable law.

Digital certification services provided by ESFIRMA are not designed nor allow their use or resale as dangerous situations control equipment, or for applications that require actions to goof-proof, as the operation of nuclear facilities, navigation systems or air communication, systems of air traffic control systems of arms control, in which an error could directly cause death injury or severe environmental damage.

6. Obligations of the verifiers

6.1. Informed decision

ESFIRMA informs the verifier that it has access to sufficient information to make an informed decision at the time a certificate verify and rely on the information contained in the certificate.

In addition, the Verifier will recognize that the use of the register and the certificates revocation lists (in the future, "the LRCs" or "the CRLs) of ESFIRMA, are governed by the DPC's ESFIRMA and he will commit to meet the technical, operational and safety requirements described in the aforementioned DPC.

6.2. Verification of the electronic signature requirements

The check will be executed normally automatically by the software of the Verifier and, in any case, according to the DPC, with the following requirements:

- It is necessary to use the appropriate software for the verification of a digital signature algorithms and key lengths of authorized on the certificate and/or execute any other cryptographic operations, and establish the chain of certificates is based on the electronic signature to verify, since the electronic signature is verified using this certificate chain.

- It is necessary to ensure that the chain of certificates identified is most suitable for the electronic signature verified, since an electronic signature may be based on more than one chain of certificates, and is decision of the controller make sure the use of the most appropriate string to verify it.

- It is necessary to check the revocation status of the certificates in the chain with the information provided to the register of ESFIRMA (with LRCs, for example) to determine the validity of all certificates in the certificate chain, since you can only be properly checked an electronic signature if each and every one of the certificates in the chain are correct and are effective.

- It is necessary to ensure that all certificates in the chain to authorize the use of the private key by the Subscriber of the certificate and the signatory, since there is the possibility that any of the certificates includes usage limits that prevent rely on the electronic signature verified. Each certificate in the chain has an indicator that refers to the applicable conditions of use, for review by the verifiers.

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

6.3. Trust in a certificate not verified

If the Verifier trusts a certificate not verified, you will assume all risks arising from this action.

6.4. Effect of the verification

Under correct verification of individual certificates used public high level, in accordance with this informative text, the Verifier can rely in identifying and, where appropriate, public key of the signer, within the limitations of use corresponding to generate encrypted messages.

6.5. Correct use and prohibited activities

The Verifier is obliged not to use any information from State of certificates or any type that has been provided by ESFIRMA, in the realization of a prohibited transaction for the law applicable to this transaction.

The Verifier must not inspect, interfere with, or reverse engineer the technical implementation of the public services of certification of ESFIRMA, without prior written consent.

In addition, the Verifier is obliged to not intentionally compromise the security of public services of certification of ESFIRMA.

Digital certification services provided by ESFIRMA are not designed nor allow the use or resale, such as equipment control of dangerous situations or for applications that require actions to goof-proof, as the operation of nuclear facilities, air communication / navigation systems, systems of air traffic control, systems of arms control, where an error could cause death injury or severe environmental damage.

6.6. Indemnity clause

The third party who relies on the certificate is committed to hold harmless ESFIRMA of harm from any action or omission resulting in liability, damage or loss, expenses of any kind, including the judicial and legal representation that may be incurred, by the publication and use of the certificate, when any of the following causes:

- Failure to comply with the obligations of the third party who relies on the certificate.
- Reckless reliance on a certificate, under the circumstances.
- Lack of verification of the status of a certificate, to determine that it is not suspended or revoked.
- Lack of verification of all measures prescribed in the DCP or rest of implementing rules.

The indicated certificate allows the encoding of documents, content, and data messages, under the exclusive responsibility of the signer. ESFIRMA is not liable under any circumstances for loss of encrypted information that cannot be recovered.

7. ESFIRMA obligations

7.1. In relation to the provision of digital certification service

ESFIRMA undertakes to a:

a) Issue, deliver, manage, suspend, revoke, and renew certificates, in accordance with the instructions provided by the Subscriber, in cases and for the reasons described in the DPC's ESFIRMA.

b) Run the services with adequate material and technical means and staff that meets the conditions of qualification and experience in the DPC.

c) Meet the levels of quality of service, in accordance with what is established in the DPC, in technical, operational aspects and safety.

d) Notify the Subscriber, prior to the expiry date of the licences, the possibility of renewing them, as well as the suspension, hoist this suspension or revocation of certificates, when these circumstances occur.

e) Inform the third parties that the status of the certificates, so request, in accordance with what is established in the DPC for the different services of verification of certificates.

7.2. In relation to the registry checks

ESFIRMA undertakes to issuance of certificates on the basis of the data supplied by the Subscriber, which can perform checks it deems appropriate with respect to identity and other personal and complementary information of subscribers and, where from the signatories.

These checks may include the documentary justification provided by the signer by the Subscriber, if considered necessary, ESFIRMA and any other document information relevant and provided by the Subscriber or the signer.

In the event that ESFIRMA detects errors in the data which should be included in certificates or justifying these data, you can make any changes it deems necessary before issuing the certificate

or suspend the issuance process and manage the corresponding incidence with the Subscriber. Where ESFIRMA correct data without prior management of the corresponding incidence with the Subscriber, you must notify finally certified to the Subscriber data.

ESFIRMA reserves the right to not issue the certificate, when you consider that the documentary justification is insufficient for correct identification and authentication of the Subscriber and/or the signer.

The above obligations shall be suspended in cases in which the Subscriber acting as registration authority and dispose of the technical elements corresponding to the generation of keys, certificate issuance and recording of corporate signature devices.

7.3. Storage times

ESFIRMA archives records corresponding to requests for issuance and revocation of certificates for at least 15 years.

ESFIRMA stores the information of logs for a period of 1 to 15 years, depending on the type of recorded information.

8. Limited warranties and rejection of guarantees

8.1. Guarantee of ESFIRMA by digital certification services

ESFIRMA guarantees to the Subscriber:

- There is no error in fact in the information contained in the certificates, known or made by the certification body.
- No errors in fact in the information contained in the certificates, due to lack of the due diligence in the management of the certificate request or in the same building.
- That the certificates meet all material requirements established in the DPC.
- That revocation services and use of the tank meet all material requirements established in the DPC.

ESFIRMA guarantees to the third party who relies on the certificate:

- That the information contained or incorporated by reference in the certificate is accurate, except when stated otherwise.
- In the case of published certificates in the tank, that the certificate has been issued to the Subscriber and signer identified therein and that the certificate has been accepted.
- That in approval of the certificate application and the issuance of the certificate have been met all material requirements established in the DPC.
- The speed and safety in the provision of services, especially the reversal and deposit services.

In addition, ESFIRMA warrants to Subscriber and the third party who relies on the certificate:

- That the certificate contains information which must contain a qualified certificate in accordance with article 11 of law 59/2003, of 19 December.
- Where it generates the private keys of the Subscriber or, where appropriate, individual identified in the certificate, is maintained confidentiality during the process.
- The responsibility of the certification entity, with the limits established. In any case ESFIRMA will respond to unforeseen circumstances and force majeure.

8.2. Exclusion of warranty

ESFIRMA disclaims all other warranties other than the previous one which is not legally enforceable.

Specifically, ESFIRMA does not guarantee software any used by anyone to sign, verify signatures, encrypt, decrypt, or use another way digital certificate one issued by ESFIRMA, except in cases where there is a statement written in the opposite direction.

9.Applicable agreements and DPC

9.1. Applicable agreements

The agreements applicable to high level public servant certificate are as follows:

- Contract of certification services, which regulates the relationship between ESFIRMA and the company subscriber certificates.

- General conditions of service embodied in the text of the disclosure of certificate or PDS.

- DPC, governing the issuance and use of certificates.

9.2. DPC

ESFIRMA certification services are regulated technically and operationally by the DPC's ESFIRMA, its subsequent updates, as well as supporting documentation.

The DPC and operations documentation is periodically modified in the registry and can be consulted on the website: https://www.esfirma.com.

10. Rules of confidence for long-term signatures

Point b.2 of the article 18 of law 59/2003, of 19 December, electronic signature refers to the obligation of the certification bodies to inform applicants of the mechanisms to ensure the reliability of the electronic signature of a document over time.

ESFIRMA informs applicants for certificates of civil servant level that does not offer a service that guarantees the reliability of the electronic signature of a document over time.

ESFIRMA recommends, for the reliability of the electronic signature of a document over time, the use of the standards described in section 7.3 (rules of confidence for long-term signatures) Guide of application of the standard technique of interoperability "Policy of electronic signature and certificates of administration".

General considerations for rules of confidence for long-term signatures are collected in the subsection IV.3 of the NTI's electronic signature.

11. Privacy policy

ESFIRMA can not disclose or may be obliged to disclose any confidential information in relation to certificates without a prior specific request coming from:

(a) a person with regard to which ESFIRMA has a duty to keep confidential information, or

(b) a judicial, administrative order or otherwise provided for in the legislation in force.

However, the Subscriber agrees that certain information, personal and otherwise, provided in the certificate request, it is included in your certificates and the mechanism of checking the status of the certificates, and that the above information does not have confidential, by imperative legal.

ESFIRMA does not yield any person the data specifically for the provision of certification services.

12. Privacy policy

ESFIRMA has a privacy policy in section 9.4 of the DPC, and specific regulation of privacy in relation to the registration process, the confidentiality of the registration, access to personal information protection, and the consent of the user.

Also includes supporting documentation of approval of the application must be preserved and properly registered and with guarantees of safety and integrity within the period of 15 years from the expiration of the certificate, including all anticipated loss of force by reversal.

13. Reinstatement policy

ESFIRMA not refunded the cost of the service of certification in any case.

14. Applicable law and competent jurisdiction

ESFIRMA relations are governed by Spanish law, and in particular to law 59/2003, of 19 December, electronic signature, as well as by the civil and commercial legislation.

The competent court is that indicated in the law 1/2000, of 7 January, code of Civil procedure.

15. Accreditations and quality seals

Without stipulation.

16. Link to the list of providers

http://www.minetur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

17. Severability of clauses, survival, entire agreement and notification

The clauses of the present text of disclosure are independent of each other, reason why if any provision is held invalid or unenforceable, the remainder of the PDS clauses continue to apply, except expressly otherwise agreed by the parties.

The requirements contained in the section 9.6.1 (obligations and liability), 8 (compliance audit) and 9.3 (confidentiality) ESFIRMA DPC will continue in force after the termination of the service.

This text contains the full will and all agreements between the parties.

The Parties reported facts mutually procedure a shipping email to the following addresses: info@esfirma.com