DISCLOSURE TEXT – PDS APPLICABLE TO CERTIFICATES, FOR THE PURPOSE OF ELECTRONIC SIGNATURE AND AUTHENTICATION

Versión:	1.0
Fecha de la versión:	06.01.2020
Creado por:	SIGNICAT SLU
Aprobado por:	SIGNICAT SLU

Histórico de cambios

Fecha	Versión	Creado por	Descripción del cambio

1. DISCLOSURE TEXT APPLICABLE TO ELECTRONIC SIGNATURE CERTIFICATES AND

AUTHENTICATION.

This document contains the essential information which should be made known to involved parties, relating to the certification service of the Trust Electronic Services Provider SIGNICAT SLU

1.1. Contact information

1.1.1. Responsible company

The Trust Electronic Services Provider SIGNICAT SLU, is an initiative of:

SIGNICAT SLU AVENIDA CIUDAD DE BARCELONA 81. 28004 MADRID EMAIL: info@electronicid.eu

1.1.2. Contact

Whenever you wish to get in touch with us, please contact:

SIGNICAT SLU EMAIL: info@electronicid.eu

1.1.3. Trust Electronic Services Provider issuer

The certificates outlined in this document are issued by SIGNICAT SLU, identified by the aforementioned data.

1.1.4. Contact for the purpose of revocation procedure

Whenever you wish to get in touch with us, please contact:

SIGNICAT SLU
EMAIL: info@electronicid.eu

1.2. Types of Certificates

The following certificates, issued by SIGNICAT SLU, are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014, of the European Parliament and the Council, dated July 23rd, 2014, and comply with the provisions of technical regulations identified by the reference ETSI EN 319 411-2. SIGNICAT SLU has assigned an object identifier (OID) to each type of certificate, for the purposes of its identification by the applications detailed below:

OID Number	Type of certificates
	Natural Person
OID 1.3.6.1.4.1.55193.1.1.1.	*Qualified Certificate of Natural Person on the CLOUD*
OID 1.3.6.1.4.1.55193.1.1.2	Qualified Certificate of Natural Person within a centralized QSCD

1.3. Purpose of certificates

1.3.1. Common stipulations

The qualified certificates described in this document and issued through a Centralized QSCD (Qualified Signature Creation Device), operate by means of qualified signature creation devices, in accordance with Articles 29 and 51 of Regulation (EU) 910/2014, and comply with the provisions of the technical regulations of the European Telecommunications Standards Institute, identified by reference number EN 319 411-2. These qualified certificates guarantee the identity of the signatory by allowing the generation of the "qualified electronic signature", that is to say, an advanced electronic signature based on a qualified certificate and generated by means of a qualified device, thus equal to the handwritten signature for any legal effects or purposes, without having to comply with any other additional prerequisites.

1.3.2. Qualified Certificate of Natural Person on the CLOUD

Qualified Certificate of Natural Person on the CLOUD

This certificate is classified under OID 1.3.6.1.4.1.55193.1.1.1. This is a qualified certificate, issued for the purposes of advanced electronic signature and authentication, in accordance with the QCP-n certification policy, with OID 0.4.0.194112.1.0. The certificates of natural persons on the CLOUD consist of certificates qualified under the provisions of Articles 24 and 28 of Regulation (EU) 910/2014.

They guarantee the identity of the subscriber and of the person appearing in the certificate, and allow the generation of the "advanced electronic signature, based on a qualified electronic certificate".

Certificates can be used for the following applications:

a) Authentication in access control systems.

b) Secure email signature.

c) Other electronic signature applications, in accordance with the agreements between the parties or the legal regulations applicable in each case.

The uses information in the certificate profile indicates the following:

The “key usage” field is enabled and therefore allows us to perform the following functions:

a. Digital Signature in order to perform the authentication function

b. Content Commitment in order to perform the electronic signature function

c. Key Encipherment

1.3.3. Qualified Certificate of Natural Person within a centralized QSCD

This certificate is classified under OID 1.3.6.1.4.1.55193.1.1.2. This is a qualified certificate, issued for the purposes of advanced electronic signature and authentication, in accordance with the QCPn-qscd certification policy, with OID 0.4.0.194112.1.2. This certificate is issued within a centralized QSCD and consists of a certificate qualified under the provisions of Article 28 of Regulation (EU) 910/2014

It operates using qualified signature creation devices (DQCS), in accordance with Articles 29 and 51 of Regulation (EU) 910/2014 and complies with the provisions of the technical regulations of the European Telecommunications Standards Institute, identified by the reference number ETSI EN 319 411-2.

. It guarantees the identity of the signatory and his link with the subscriber of the trust electronic service by allowing the generation of the "qualified electronic signature", that is to say, the advanced signature based on a qualified certificate, which was generated by means of a qualified device, thus equaling the handwritten signature for legal effects and purposes, without the need to meet any other additional prerequisites.

It can also be used for other applications which do not require the electronic signature as an equivalent to the handwritten signature, such as in the applications outlined below:

a) Secure email signature.

b) Other electronic signature applications.

The “key usage” field is enabled and therefore allows us to perform the following functions:

4. Digital Signature in order to perform the authentication function
5. Content Commitment in order to perform the electronic signature function
6. Key Encipherment

1.4 Constraints on certificate usage

1.4.1 Limits of use addressed to signatories

The signatory must use the certificate certification service provided by SIGNICAT SLU, exclusively for the authorized uses of the contract signed between SIGNICAT SLU and the SUBSCRIBER, reproduced later (under the section "Obligations of signatories”).

Likewise, the signatory undertakes to use the digital certification service in accordance with the instructions, manuals or procedures as propounded by SIGNICAT SLU.

The signatory must comply with all laws and regulations likely to affect their right to use the cryptographic tools utilized.

The signatory may not make any inspection, alteration or reverse engineering action with regard to SIGNICAT SLU's digital certification services without its prior and express written authorization.

1.4.2 Constraints on verifiers usage

Certificates are to be used in accordance with their specific functions and for the purposes established, and cannot be used for any other functions and purposes.

Likewise, certificates must be used exclusively in accordance with applicable regulations, taking particular account of import and export restrictions at all times.

Certificates cannot be used to sign any certificate whose key is public, nor to sign certificate revocation lists (CRL).

The certificates were not designed, nor can they be intended for, neither they can be used or resold as equipment for the control of dangerous situations, nor in cases of usages which require faultless interventions, such as in the operation of nuclear installations, navigation or air communications systems, or weapon control system,s where an error can directly result in death, personal injury or serious environmental damage.

The limits indicated in the various fields of the certificate profiles, visible on the SIGNICAT SLU Web (https://www.signicat.com) must be taken into account.

The use of digital certificates during operations which contravene this disclosure text, or contracts with subscribers, must be considered as improper use for all relevant legal effects and purposes, SIGNICAT SLU being therefore hold harmless in accordance with legislation in force from any liability in relation to improper use of certificates, whether made by the signatory, or by any third party.

SIGNICAT SLU does not have access to data to which the use of a certificate may be applied. As a result, and because of the technical impossibility of having access to the content of the message, SIGNICAT SLU cannot therefore evaluate its content, the subscriber, the signatory or any person responsible for the protection, and must therefore assume all responsibility arising from the content, and related to the use of a certificate.

Likewise, the subscriber, the signatory or the person responsible for protection will have to assume any responsibility likely to result from the use of this outside the limits and conditions of use appearing in this disclosure text, or appearing in contracts with subscribers, as well as any other improper use thereof, derived from this paragraph, or likely to be interpreted as such under the applicable regulations.

1.5 Subscribers' obligations

1.5.1 Keys' generation

The subscriber authorizes SIGNICAT SLU to manage the issuance of the private and public keys for the signatories in accordance with the corresponding methods and procedures, and to request the issuance of the certificate in accordance with the SIGNICAT SLU certification policies on their behalf.

1.5.2 Certificates' request

The subscriber undertakes to handle requests for qualified certificates in accordance with the procedure and, if necessary, technical components facilitated by SIGNICAT SLU, under the provisions of the declaration on certification practices (SCP).

1.5.3 Information obligations

The subscriber is responsible for the accuracy and completeness of all information included in his request for a certificate for purposes of the latter, as well as for any updating as may be required at any time.

The subscriber must immediately inform SIGNICAT SLU of:

- any inaccuracy detected in the certificate once it has been issued.
- any change likely to modify the information facilitated and / or recorded for the purpose of the certificate issuance.
- any loss, theft, subtraction, or any other kind of loss of control of the private key by the signatory.

1.6. Signatories' obligations

1.6.1. Protection obligations

The signatory undertakes to protect the personal identification code or any other technical support provided by SIGNICAT SLU, the private keys and, where necessary, the facilitated specifications owned by SIGNICAT SLU.

In case of loss or theft of the private key of the certificate, or if the signer suspects that the private key has lost its reliability for secure use for any reason whatsoever, these circumstances must immediately be notified to the reference Registration Authority or to SIGNICAT SLU.

1.6.2. Obligations of appropriate use

The signatory must use the certification service for natural person certificates issued in QSCD provided by SIGNICAT SLU, exclusively for the uses authorized by the SCP and any other instruction, manual or procedure expedited to the subscriber.

The signatory must comply with all laws and regulations likely to affect his right to use the cryptographic tools used.

The signatory will not be able to request or take measures to inspect, alter, or decompile the digital certification services provided.

The signatory recognizes:

a) that when using any certificate and as long as it has not expired or has not been suspended or revoked, he accepts this certificate which will remain operational.

b) that he is not acting as a certification entity, therefore, he undertakes not to use the private keys corresponding to the public keys contained in the certificates, for the effects of signing any certificate whatsoever.

c) if the private key were to be compromised, he will stop using it immediately and permanently and will proceed in accordance with the terms set out in this document.

1.7. Verifiers' obligations

1.7.1. Informed decision-making

SIGNICAT SLU informs the verifier of his right to access sufficient information in order to make an informed decision when verifying a certificate and entrusting the information contained in the certificate to it.

In addition, the verifier acknowledges that the use of the Register and Certificate Revocation Lists (hereinafter, the "CRL") of SIGNICAT SLU, is governed by the SCP of SIGNICAT SLU and undertakes to comply with the technical, operational and security prerequisites outlined in this SCP.

1.7.2. Prerequisites for verifying an electronic signature

The verification will normally be carried out automatically by the verifier's software and, under all circumstances, in accordance with the SCP and under the following prerequisites:

- It is necessary to use the appropriate software in order to verify an electronic signature with the algorithms and key lengths authorized in the certificate and / or perform any other cryptographic operation, and therefore establish the chain of certificates on which the electronic signature to be verified is based, since the latter is verified by means of these chain of certificates.

- It is necessary to ensure that the identity chain of certificates is the most appropriate one for the electronic signature being verified, since an electronic signature can be based on more than one chain of certificates, with the verifier deciding on the use of the most suitable chain in order to check it.

- It is necessary to check the revocation status of certificates in the chain with the information provided to the SIGNICAT SLU Registry (with CRLs, for example) in order to determine the validity of all certificates in the certificate chain, since a signature can only be considered as correctly verified if each and every one of the certificates in the chain is correct, and currently in force.

- It is necessary to guarantee that all the certificates in the chain authorize the use of the private key by both the subscriber of the certificate and the signatory, since there is the possibility that one of the certificates includes limits of use which prevent trusting in the electronic signature being verified. Each certificate in the chain has an indicator referring to the applicable conditions of use, for the purposes of its review by the verifiers.

- It is necessary to technically verify the signature of all the certificates in the chain before entrusting the certificate used by the signatory.

1.7.3. Trust in an unverified certificate

Whenever the verifier trusts an unverified certificate, he will personally assume all risks derived from this intervention.

1.7.4. Verification effect

By virtue of the correct verification of physical person certificates issued in the QSCD, in accordance with this disclosure text, the verifier can trust the identification and, where applicable, the public key of the signatory, within the framework of the corresponding usage limitations, in order to generate encrypted messages.

1.7.5 Correct usage and prohibited activities

The verifier undertakes not to use any type of certificate status information whatsoever or any other kind facilitated by SIGNICAT SLU, when carrying out any transaction prohibited by the law as applicable to this transaction.

The verifier undertakes not to inspect, interfere with, or otherwise reverse engineer the technical implementation of the SIGNICAT SLU certification public services, without their prior written consent.

In addition, the verifier undertakes not to intentionally compromise the security of the public SIGNICAT SLU certification services.

The digital certification services provided by SIGNICAT SLU were not designed, nor authorized for use or resale as equipment for the control of dangerous situations, nor the uses which require faultless interventions, such as the operation of nuclear installations, navigation, or air communications systems, or weapon control systems where an error can directly result in death, personal injury or serious environmental damage

1.7.5. Disclaimer

The third party who holds the certificate in trust undertakes to hold SIGNICAT SLU harmless from any action or omission resulting in any liability, damage or loss, expense of any kind, including legal costs and lawyer legal fees possibly incurred in respect of the publication and use of the certificate, should any of the following causes occur:

- breach of the obligations of the third party entrusted with the certificate.
- reckless trust in a certificate, given the circumstances.
- failure to check the status of a certificate, in order to determine that it has not been suspended or revoked.
- failure to verify all the guarantee measures as stipulated in the SCP, or any of the rest of the applicable regulations.

1.8. SIGNICAT SLU obligations

1.8.1. Regarding the provision of the digital certification service

SIGNICAT SLU undertakes to:

a) issue, remit, administer, suspend, reactivate, revoke and renew certificates, in accordance with the instructions forwarded by the subscriber and / or signatory, in those cases and for those reasons described in the SIGNICAT SLU SCP.

b) carry out the services using the appropriate technical and material means, with personnel meeting the qualification and experience level conditions as stipulated in the SCP.

c) comply with the service quality levels, in accordance with the provisions of the SCP, with regard to technical, operational and security aspects.

d) notify the subscriber and the signatory, prior to the expiry date of the certificates, of the possibility of renewing them, as well as of the suspension, lifting of this suspension or revocation of the certificates, should these circumstances arise.

e) communicate the status of certificates to third parties who request it, in accordance with the provisions of the SCP relating to the various certificate verification services.

1.8.2. Regarding to the registry verifications

SIGNICAT SLU undertakes to issue certificates based on the data facilitated by the subscriber, so they can perform the checks deemed relevant with regard to the identity and other personal and additional information of the subscribers and, where relevant, of the signatories.

These verifications may include the documentary justification provided, as well as any other relevant document and information facilitated by the subscriber and / or the signatory.

If SIGNICAT SLU detects errors in the data to be included in the certificates, or which justifies this data, they may make any changes deemed necessary before issuing the certificate, or suspend the issuance procedure and manage the corresponding negative impact with the subscriber. If SIGNICAT SLU corrects the data without prior management of the corresponding negative impact with the subscriber, they must notify the certified data to the subscriber at the earliest opportunity.

SIGNICAT SLU reserves the right not to issue the certificate if they consider that the documentary justification is insufficient for the purposes of correct identification and authentication of the subscriber and / or the signatory.

The aforementioned obligations will remain in abeyance in cases where the subscriber acts as a registration authority, and has possession of the technical elements corresponding to the generation of keys, issuance of certificates and registration of corporate signature devices.

1.8.3. Retention periods

SIGNICAT SLU archives the registers corresponding to requests for issuance and revocation of certificates for at least 15 years.

SIGNICAT SLU stores historical information for a period of 1 to 15 years, depending on the type of information recorded, in accordance with the provisions of its policies and procedures.

1.9. Limited warranties and denial of warranties

1.9.1.SIGNICAT SLU Guarantee for digital certification services

SIGNICAT SLU guarantees the subscriber:

- the absence of factual errors in the information included in the certificates, known or made by the Certification Authority.
- the absence of errors of fact in the information included in the certificates, due to a lack of the diligence due during the management of the request for the certificate or the creation of the latter.
- that the certificates meet all the material prerequisites established at the SCP.
- that the revocation services and the use of the deposit comply with all the material prerequisites established at the SCP.

SIGNICAT SLU guarantees third parties entrusted with the certificate:

- that the information included or incorporated by reference to the certificate is correct, provided that the contrary is indicated.
- in the case of certificates published at the deposit, that these have been delivered to the subscriber and signatory identified in it and that the certificate has been accepted.
- that all the material prerequisites established at the SCP have been respected during the approval of the request and the issuance of the certificate.
- the speed and security of the provision of services, especially those of revocation and filing.

In addition, SIGNICAT SLU guarantees the subscriber and third parties entrusted with the certificate:

- that the qualified certificate in terms of signature includes the information that a qualified certificate must contain, in accordance with the provisions of Article 28 of Regulation (EU) 910/2014, thus complying with the provisions of the technical regulations identified by the reference ETSI EN 319 411-2.
- that, in the event of generating the private keys of the subscriber or, where applicable, of the natural person identified in the certificate, their confidentiality is preserved during the procedure.
- the responsibility of the Certification Authority, with established limits. Under no circumstances will SIGNICAT SLU respond in the event of a fortuitous event invoking a case of force majeure.

1.9.2. Exclusion of warranty

SIGNICAT SLU shall refuse any other guarantee which differs from the previous one, and for which there is no legal requirement.

Specifically, SIGNICAT SLU does not grant a warranty for any software used by anyone in order to sign, verify signatures, encrypt, decrypt, or otherwise use any digital certificate issued by SIGNICAT SLU, except in cases where there is a written statement to the contrary.

1.10. Applicable agreements and SCP

1.10.1. Applicable agreements

The agreements applicable to certificates comprise the following:

- certification services contract governing the relationship between SIGNICAT SLU and the certificates subscriber.
- general conditions of service incorporated in this document.
- statement on Certification Practices governing the issuance and use of certificates.

1.10.2. Statement on Certification Practices

SIGNICAT SLU's trust services are technically and operationally governed by the SIGNICAT SLU Statement on Certification Practices Statement (SCP), by its subsequent updates, as well as by any additional documentation.

The SCP and the documentation relating to operations are periodically modified in the Register and can be consulted on the Internet page www.electronicid.eu

1.11. Trust rules for long-lasting signatures

SIGNICAT SLU informs certificate applicants that they do not offer any service which guarantees the reliability of the electronic signature of a document over any given period of time.

1.12. Privacy policy

SIGNICAT SLU cannot disclose, nor shall be obliged to disclose, any confidential information relating to certificates without specific and prior request from:

a) the person from whom SIGNICAT SLU must keep the information confidential, or

b) a judicial, administrative or any other order provided for under the legislation in force.

However, the subscriber accepts that certain predetermined information, of a personal or other nature, made available during the request for certificates, are included in his certificates and the mechanism for verifying the status of certificates, along with any information mentioned is not of a

confidential nature through legal requirements. SIGNICAT SLU does not transfer the data specifically made available for the purpose of providing the certification service to anyone else.

1.13. Confidentiality policy

SIGNICAT SLU has a confidentiality policy outlined under paragraph 9.4 of the SCP, and specific regulations for this confidentiality with regard to the registration procedure, the confidentiality of the latter, and the protection of access to personal information and user consent.

Likewise, it is noted that the documentation justifying the approval of the request must be duly recorded for safekeeping, and be provided with guarantees of security and integrity for a period of 15 years, starting from the date of expiry of the certificate, or even in the event of premature loss of effect upon revocation.

1.14. Reimbursement policy

SIGNICAT SLU will not reimburse the costs of the certification service under any circumstances.

1.15. Applicable regulations and competent jurisdiction

Relations with SIGNICAT SLU will be governed in accordance with the provisions set out under Regulation (EU) 910/2014 SIGNICAT SLUAS, under Spanish laws and, in particular, all those derived from its policy of compliance.

The competent jurisdiction is that indicated in Law 1/2000, dated January 7th, relating to Civil Procedure.

1.16. Link with the List of Qualified Providers of Trust Electronic Services

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

1.17. Severability of clauses, subsistence, full agreement and notification

The clauses of this disclosure text are independent of each other, which is why, if any of the clauses were to be considered null or void, the rest of the clauses of the PDS shall still remain applicable, subject to the counter and express agreement of the parties.

The prerequisites stipulated in sections 9.6.1 (Obligations and responsibility), 8 (Compliance audit) and 9.3 (Confidentiality) of the SIGNICAT SLU SCP shall remain in force following the expiry of the service under the conditions provided therein.

This text reflects the entire will, as well as all agreements concluded between the parties.

The parties shall notify each other of all facts via an email procedure to the following addresses: • info@SIGNICAT SLU.com, for SIGNICAT SLU

•the email address indicated by the subscriber to the contract with SIGNICAT SLU.