SIGNE Certification Authority

PKI Disclosure Statement (PDS)

Document:	SIGNE-ES-AC-DPC-02
Version:	3.3
Date:	May 30, 2023
Document type:	PUBLIC

Version History

Version	Modifications	Date
1.0	Document created	March 24, 2017
1.1	Homogenization of terminology about the different types of certificate supports	July 31, 2018
1.2	Changes in the format of the document New type of certificates: Corporate signature	March 22, 2019
1.3	Adjustment of document code	March 19, 2020
3.0	Addition of document type Changes in Spanish law and jurisdiction	February 24, 2021
3.1	Changes in contact details for revocation Changes in recipients and purposes of certificates Addition of OCSP services for certificate validation	June 21, 2021
3.2	Change in the validity of the certificates Added new qualified profiles Added online revocation	June 3, 2022
3.3	Minor changes	May 30, 2023

Index

1. Introduction and contact information

1.1. Introduction

This document is an informative text that aims to highlight the basics contained in the Certification Practice Statement (hereinafter CPS) and Certificate Policies (hereinafter CPs) of Signe S.A. (hereinafter SIGNE). By no means this document is intended to replace, develop, expand or amend the aforementioned CPS and CPs of SIGNE.

This informative text is subject to the documentation derived from the seventh clause of this informative text, which must be respected and will be always applicable.

1.2. Certification Authority contact details

For any questions, please contact:

SIGNE
Avda. de la Industria, 18 – 28760 Tres Cantos (Madrid) - España
Tel.: + 34 918 06 00 99
www.signe.es
signe-ac@signe.com

1.3. Contact details for revocation

For revocation, please contact:

SIGNE
Tel.: +34 918 06 10 08
www.signe.es
signe-ac@signe.com

Online revocation service:
https://www.signe.es/en/electronic-certification/obtaining-renewal-revocation/

2. Types and purposes of certificates

2.1. Definitions about recipients

- **Natural person non-associated with an organization - graduate:** natural person with one or more university degrees which link the person to the corresponding universities.
- **Natural person associated with an organization:** natural person with a certain relation with an organization which has signed a contract with SIGNE.
- **Legal person - private:** legal person which is a private entity.
- **Legal person - public:** legal person which is a public entity.

2.2. Definitions about purposes of certificates

- **Authentication:** electronic identification of the natural or legal person.
- **Advanced electronic signature - qualified certificate:** electronic signature which is created with a qualified certificate for electronic signature, in accordance with applicable law.
- **Advanced electronic signature - non-qualified certificate:** electronic signature which is created with a non-qualified certificate for electronic signature, in accordance with applicable law.
- **Qualified electronic signature:** electronic signature which is created with a qualified certificate for electronic signature by a Qualified electronic Signature Creation Device (QSCD), in accordance with applicable law.
- **Advanced electronic seal - qualified certificate:** electronic seal which is created with a qualified certificate for electronic seal, in accordance with applicable law.
- **Qualified electronic seal:** electronic seal which is created with a qualified certificate for electronic seal by a Qualified electronic Seal Creation Device (QSCD), in accordance with applicable law.

2.3. Types of certificates

Type of certificates	Recipients	Purposes	OID	Validity
Graduate	Natural person non-associated with an organization - graduate	Authentication Advanced electronic signature - qualified certificate	1.3.6.1.4.1.36035.1.1.2: Other devices - Medium Level	Up to 3 years
Natural person	Natural person non-associated with an organization	Authentication Advanced electronic signature - qualified certificate Qualified electronic signature	1.3.6.1.4.1.36035.1.3.1: Portable QSCD - High Level 1.3.6.1.4.1.36035.1.3.2: Other devices - Medium Level 1.3.6.1.4.1.36035.1.3.3: Centralized QSCD - High Level	Up to 3 years
Corporate natural person	Natural person associated with an organization	Authentication Advanced electronic signature - qualified certificate Qualified electronic signature	1.3.6.1.4.1.36035.1.2.1: Portable QSCD - High Level 1.3.6.1.4.1.36035.1.2.2: Other devices - Medium Level 1.3.6.1.4.1.36035.1.2.3: Centralized QSCD - High Level	Up to 3 years
Corporate signature	Natural person associated with an organization	Authentication Advanced electronic signature - non-qualified certificate	1.3.6.1.4.1.36035.1.20.2: Other devices - Medium Level	Up to 3 years
Corporate signature of legal representative	Natural person legal representative of an organization	Authentication Advanced electronic signature - qualified certificate Qualified electronic signature	1.3.6.1.4.1.36035.1.21.1: Portable QSCD - High Level 1.3.6.1.4.1.36035.1.21.2: Other devices - Medium Level 1.3.6.1.4.1.36035.1.21.3: Centralized QSCD - High Level	Up to 3 years
Corporate electronic seal	Legal person - private Legal person - public	Authentication Advanced electronic seal - qualified certificate Qualified electronic seal	1.3.6.1.4.1.36035.1.5.1: Portable QSCD - High Level 1.3.6.1.4.1.36035.1.5.2: Other devices - Medium Level 1.3.6.1.4.1.36035.1.5.3: Centralized QSCD - High Level	Up to 3 years

Organ seal	Legal person - public	Authentication Advanced electronic seal - qualified certificate Qualified electronic seal	1.3.6.1.4.1.36035.1.10.1: Portable QCSD - High Level 1.3.6.1.4.1.36035.1.10.2: Other devices - Medium Level 1.3.6.1.4.1.36035.1.10.3: Centralized QSCD - High Level	Up to 3 years

2.4. Certificate validation

CRLs are posted on SIGNE website and the URLs identified in the issued certificates and certificates in the certificate chain.

OCSP services are provided on the URLs identified in the issued certificates and certificates in the certificate chain.

2.5. Issuing Certification Authority

Certificates are issued by SIGNE Certification Authority.

3. Certificate usage limits

Certificates will be used in accordance with their own function and purposes, and they may not be used with other functions and other purposes.

Certificates must be used only in accordance with applicable law, especially given existing import and export restrictions at any given moment.

The X.509 v3 certificate Key Usage and Extended Key Usage extensions will be used to set technical usage limits to a private key corresponding to a public key listed in a certificate. It should be noted that the effectiveness of restrictions based on certificate extensions sometimes depend on the operation of computer applications that have not been developed or cannot be controlled by SIGNE.

Certificates are not designed, and their use or resale is not authorized, as control equipment for hazardous applications or for uses requiring fail-safe measures, such as operation in nuclear facilities, navigation systems, air communications or weapons systems, where a mistake could lead directly to death, personal injury or serious environmental damage.

3.1. Usage limits aimed at subscribers

Subscribers and, where applicable, key holders must use the certification services provided by SIGNE exclusively for authorized purposes, which are concisely listed in the fourth clause of this informative text.

Subscribers and, where applicable, key holders undertake to use the certification services in accordance with the instructions, manuals and procedures provided by SIGNE.

Subscribers and, where applicable, key holders must comply with any laws and regulations that may affect their right to use the cryptographic tools.

Subscribers and, where applicable, key holders cannot take measures of inspection, alteration or reverse engineering of SIGNE certification services without prior and express written permission from SIGNE.

3.2. Usage limits aimed at verifiers

Certificate verifiers must use the information services provided by SIGNE exclusively for authorized purposes, which are concisely listed in the fifth clause of this informative text.

Verifiers undertake to use the information services in accordance with the instructions, manuals and procedures supplied by SIGNE.

Verifiers must comply with any law and regulation that may affect their right to use the cryptographic tools.

Verifiers cannot take measures of inspection, alteration or reverse engineering of SIGNE public certification services without prior and express written permission from SIGNE.

4. Subscriber obligations

4.1. Certificate request and key generation

Prior to the issuance and delivery of a certificate, there must be a certificate request.

The request for issuing a certificate implies the subscriber's authorization of SIGNE to generate its keys, and for it to issue the corresponding certificate. The key format and intended use will vary according to the profile.

The subscriber agrees to request the certificate based on:

- the specifications provided for each certificate,
- the procedure stipulated in the CPS, CPs and SIGNE operation documentation,
- the technical components supplied by SIGNE or the Associated Certification Body, if necessary.

4.2. Information accuracy

The subscriber, and where applicable, the key holder assume responsibility for all the information included, by any means, in the certificate request is accurate and complete for such purpose, and up-to-date.

The subscriber and, where applicable, the key holder must report SIGNE immediately any inaccuracies detected in SIGNE certificate once issued, as well as changes in the information provided and/or recorded for issuing the certificate.

In the event that the key holder ceases its relationship with the subscriber, the latter must immediately request the certificate's revocation.

4.3. Delivery and acceptance of the service

By signing the delivery slip, the subscriber or, where applicable, the key holder acknowledges delivery of the certificate, the private key and any other technical format delivered by SIGNE and, when applicable, the personal identification code. The subscriber, or where applicable, the key holder will likewise confirm that these elements are working properly.

The subscriber or, where applicable, the key holder accepts — by signing the delivery slip — the certificate as specified in SIGNE CPS and CPs.

The subscriber must manage the signature of delivery slip by the key holder. All the information will be given to SIGNE or the Associated Certification Body, except when the certificate activation occurs by electronic means.

4.4. Key holders

The subscriber agrees to inform those responsible for key safeguarding (key holders) of the terms and conditions governing the use of certificates.

Likewise, the subscriber agrees that key holders fulfil their obligations as stipulated in the corresponding delivery slip.

4.5. Safeguarding obligations

The subscriber or, where applicable, the key holder undertakes to, where necessary, safeguard the personal identification code, the card or any other technical format delivered by SIGNE or the Associated Certification Body, the private keys and, if necessary, the specifications owned by SIGNE that may have been supplied.

In the event of loss or theft of the private key for the certificate, or if the subscriber or, where applicable, the key holder suspects that the reliability of the private key has been undermined for any reason, he/she must immediately notify SIGNE.

4.6. Proper use obligations

The subscriber and, where applicable, the key holder must use the certification services, the public and private keys, the card or any other technical format delivered by SIGNE or the Associated Certification Body solely for purposes authorized in the CPS and CPs, in accordance with the specific service terms as well as any other instruction, manual and procedure supplied to subscribers by SIGNE or the Associated Certification Body.

The subscriber and, where applicable, the key holder will recognize that when using the certificate, and while it has not expired or has not been revoked, accepts the certificate, and it will be operational.

4.7. Prohibited transactions

Subscribers and, where applicable, key holders undertake not to use their private keys, certificates, cards or any other technical format delivered by SIGNE or the Associated Certification Body in carrying out transactions prohibited by applicable law.

SIGNE certification services are not designed nor do they permit the use or resale as control equipment in hazardous situations or for uses requiring fail-safe measures, such as operation in nuclear facilities, air navigation or communication systems, air traffic control systems or weapons control, where an error could directly cause death, bodily injury or serious environmental damage.

Certificates are issued to subscribers and, where applicable, key holders for the purposes expressly listed in the third section of the second clause of this informative text. Any other use outside those described in this clause is expressly excluded and formally prohibited.

5. Verifier obligations

5.1. Informed consent

SIGNE informs verifiers that they have access to information enough to make an informed decision when verifying a certificate, and they can rely on the information contained therein.

Verifiers acknowledge that the use of SIGNE Certificates Register (with CRLs and OCSP services) is governed by SIGNE CPS and CPs, and undertakes to comply with the technical, operational and security requirements detailed in the aforementioned CPS and CPs.

5.2. Electronic signature or seal verification requirements

In order to rely on an electronic signature or seal, it is essential for verifiers to check the existence and validity of both the certificate and the digital signature, by implementing the verification procedure.

Verification involves checking the authenticity and integrity of the digitally signed data, in order to determine that it was indeed generated using the private key corresponding to the public key contained in the certificate issued by the legitimate Certification Authority, i.e. SIGNE, and that the data was not modified since the digital signature was generated.

Verification will be normally performed automatically by the verifier's software and, in any case, in accordance with the CPS and CPs and the following requirements:

- Using appropriate software to verify technically the digital signature value, by executing cryptographic operations with algorithm and length key in the certificate, and to establish the certificates chain on which the digital signature being verified is based.
- Ensuring that the certificates chain identified is the most appropriate for the digital signature being verified, since a digital signature can be based on more than one certificates chain, and it is up to the verifier to ensure that the most appropriate chain is used for verification.
- Checking the certificate revocation status in the certificates chain with the information provided by SIGNE Certificates Register (with CRLs or OCSP services) to determine the validity of all certificates in the certificates chain, given that an digital signature can only be deemed to be properly verified if each and every one of the certificates in the chain are correct and in force.
- Ensuring that all certificates in the chain authorize the usage of the private key certificate by the certificate subscriber or, where applicable, the key holder, since some certificates may include usage limits that prevent relying on the digital signature being verified.
- Verifying technically the digital signature of all certificates in the chain before trusting the certificate used by the subscriber or, where applicable, the key holder.
- Determining the date and time when the digital signature was generated, since the digital signature can only be deemed properly verified if it was created within the validity period of the certificates chain on which it is based.

- Defining the data that has been digitally signed, since these will be used in verifying the digital signature value.
- Verifying technically the digital signature value, with the algorithm and the key in the signing certificate endorsed by the certificate chain.

5.3. Due diligence

Verifiers must act with the utmost diligence before relying on any certificates. In particular, verifiers must undertake to use the digital signature verification software with the appropriate technical, operational and security aptitude to properly execute the digital signature verification process, and shall be exclusively responsible for any damage that may result from the incorrect selection of such software.

The previous limitation shall not apply when SIGNE has provided the verification software to the verifier.

The verifier can trust a certificate if the following conditions concur:

- The electronic signature or seal must be able to be verified pursuant to the requirements of section two of the fifth clause of this informative text.
- The verifier must have used updated revocation information.
- The type of the certificate must be appropriate for the intended use.
- The verifier shall take into account other additional limitations for use of the certificate as noted in any way on the certificate, including those not processed automatically by the verification software, included as reference in the certificate and contained in the specific service terms. Specifically, a certificate does not grant rights and powers from SIGNE to the subscriber or, where applicable, the key holder beyond the description of the type of the certificate according to the second clause of this informative text or other express indication of SIGNE or the subscriber itself.
- Finally, trust must be reasonable under the circumstances. If circumstances require additional guarantees, the verifier must obtain these guarantees to substantiate reasonable trust.

In any case, the final decision in terms of trusting a verified certificate or not is exclusively up to the verifier, who must take an active attitude and who is required to access all the information provided by SIGNE to take his or her decisions in a fully informed manner. In case of doubt, the verifier should not trust the certificate.

5.4. Trust an unverified certificate

It is forbidden to trust or otherwise use a unverified certificate.

If the verifier trusts an unverified certificate, he or she will assume all the risks of this action.

5.5. Verification effect

Based on the proper verification of a digital signature and/or certificate, in accordance with the usage terms, the verifier can trust the certificate and/or digital signature based on the former, within the corresponding usage constraints.

5.6. Prohibited activities

The verifier undertakes not to use any certificate status information or any other information supplied by SIGNE in performing any act prohibited by the law applicable.

The verifier undertakes not to inspect, alter or perform reverse engineer of SIGNE public certification services without prior written consent of SIGNE. Moreover, the verifier undertakes not to intentionally compromise the security of SIGNE public certification services.

SIGNE certification services are not designed nor do they permit use or resale as control equipment in hazardous situations or for uses requiring fail-safe measures, such as operation in nuclear facilities, air navigation or communication systems, air traffic control systems or weapons control, where an error could cause death, bodily injury or serious environmental damage.

6. Limited warranty and disclaimers

6.1. SIGNE warranty for certification services

SIGNE undertakes to provide certification services in certain technical, legal and operational conditions as set out in its CPS and CPs, including a Certificates Register (with CRLs and OCSP services) where the information regarding certificate status is published.

SIGNE guarantees the following certification services conditions:

- The certificate contains accurate and current information at the time of issuance, duly verified in accordance with the provisions of current legislation.
- The certificate meets all the requirements regarding content and format stipulated by the CPS and CPs.
- SIGNE Certification Authority private key has not been compromised, unless otherwise notified by the Certificates Register (with CRLs or OCSP services).

6.2. Disclaimer

SIGNE does not guarantee any software whatsoever used by anyone to create, verify or use in any way, any digital signature or digital certificate issued by SIGNE, except when there is a written declaration to the contrary or the software has been provided by SIGNE.

6.3. Insurance

SIGNE, as a trust service provider, has guarantee enough to cover its liability under the law.

In case of misuse or unauthorized use of certificates, SIGNE (or the relevant Associated Certification Body) does not act as a fiduciary agent before subscribers, where applicable, key holders, and third parties, who must directly address the person in breach of the usage terms set out by SIGNE (or Associated Certification Body involved).

7. Applicable agreements, CPS and CPs

7.1. Applicable agreements

The agreements which apply to the certificates for the specific service terms.

7.2. Certification Practice Statement (CPS)

SIGNE certification services are technically, legally and operationally regulated by the Certification Practice Statement.

The CPS can be found at:

https://www.signe.es/signe-ac/dpc

Anything not covered in this informative text will be governed by the provisions of the Certification Practice Statement. Likewise, in case of contradiction between the terms of this informative text and the Certification Practice Statement of SIGNE, the latter shall prevail in any case.

7.3. Certificate Policies (CPs)

SIGNE has a Certificate Policy for each type of certificates expressly listed in the third section of the second clause of this informative text, detailing technical, legal and operational requirements of certificates.

The CPs can be found at:

https://www.signe.es/signe-ac/dpc

Anything not covered in this informative text will be governed by the provisions of the Certification Policies. Likewise, in case of contradiction between the terms of this informative text and Certification Policies of SIGNE, the latter shall prevail in any case.

8. Privacy policy

SIGNE (or Associated Certification Body involved) cannot disclose or be compelled to disclose any confidential information concerning certificates without an prior specific request from:

a) the person with whom SIGNE is obliged to keep confidential information, or

b) a court, administrative order or any other kind of order provided regarding current legislation.

However, the subscriber and, where applicable, the key holder agree that certain information, personal and otherwise, provided in the certificate request will be included in the certificate, and that the certificate status information is not confidential, as stipulated by law.

SIGNE (or Associated Certification Body involved) is not liable for any use made by a third party of this information.

8.1. Retention periods

Records related to the lifecycle of certificates will be stored, either on paper or electronically, ensuring the appropriate security, authenticity, integrity and preservation methods related to the information contained in the certificate, for a period of 15 years after certificate expiration. These records must be stored by SIGNE or the Associated Certification Body.

Likewise, the certificate delivery slips will be saved for a period of 15 years after certificate expiration. These records must be stored by SIGNE or the Associated Certification Body.

9. Refund policy

Not applicable.

10. Law and jurisdiction

Parties shall be governed by Spanish law, particularly Law 6/2020, dated 11 November, on electronic trust services, and Regulation (EU) No 910/2014 of the European Parliament and of the Council, dated 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter eIDAS).

Parties, waiving any other jurisdiction that may correspond to them, submit to the Spanish Courts and Tribunals.

11. Accreditations and quality seals

SIGNE has passed the following audits:

- eIDAS Compliance.

www.signe.es

Avda. de la Industria, 18
28760 Tres Cantos (Madrid)
España

Tel.: + 34 918 06 00 99
signe-ac@signe.com