Tinexta Infocert

PDS - CAMERFIRMA'S NON-PERSONAL CERTIFICATES DISCLOSURE STATEMENT

Version 1. 1

Drafting and Review: Camerfirma's Compliance and Legal Departments

Approval (AP): Camerfirma's Legal Department

This document can be obtained at the address:
https://pds.camerfirma.com/

Language: English

Code: PUB-2025-18-09

INDEX

1 TRUST SERVICE PROVIDER INFORMATION

1.1 ORGANIZATION

The corporate data of the Trust Service Provider are:

Corporate name:	AC CAMERFIRMA, S.A.
TAX ID:	A82743287
Registered office:	Calle de Rodríguez Marín 88 - 28016 Madrid
Phone:	+34 91 136 91 05
Email:	ca@camerfirma.com/ info@camerfirma.com
Website:	https://www.camerfirma.com

2 TYPE AND PURPOSE OF CERTIFICATES ISSUED UNDER THE NON-PERSONAL CERTIFICATE POLICY

Camerfirma issues the following types of certificates under the Certificate Policy addressed to legal entities or objects:

- **Qualified Certificate of Electronic Seal**:

  This qualified certificate identifies a legal entity (Holder / Creator of a Seal).

  The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the legal entity to which the certificate is issued.

  The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

  This certificate can be associated to a private key activated by a machine or application, to allow the operations that use it to be performed automatically and unassisted. It is also allowed as a machine or client application identification element in TLS secure electronic communication protocols.

- **Qualified Certificate of Electronic Stamp AAPP**

  This qualified certificate identifies a legal entity of the Public Administration type (Holder / Creator of a Seal), in accordance with the provisions of Article 40 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

  The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the Public Administration to which the certificate is issued.

  The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

  This certificate can be associated to a private key activated by a machine or application, to allow the operations that use it to be performed automatically and unassisted. It is also allowed as a machine or client application identification element in TLS secure electronic communication protocols.

  The certificates issued under these CPs can be used by signature systems for automated administrative action, in accordance with the provisions of Article 42 of Law 40/2015, of October 1, of the Public Sector Legal Regime.

- **Non Qualified Code Signing Certificate**

  This Non Qualified certificate identifies a legal entity (Holder / Creator of a Seal).

  The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the legal entity to which the certificate is issued.

This certificate allows developers to apply a digital signature on code (ActiveX, java applets, macros for Microsoft Office, etc.), thus establishing integrity and authenticity guarantees on such code.

- **Non Qualified Certificate of Electronic Seal**

This Non Qualified certificate identifies a legal entity (Holder / Creator of a Seal).

The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the legal entity to which the certificate is issued.

The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

This certificate can be associated to a private key activated by a machine or application, to allow the operations that use it to be performed automatically and unassisted. It is also allowed as a machine or client application identification element in TLS secure electronic communication protocols.

- **Non Qualified Certificate of Personnel AAPP**

This Non Qualified certificate identifies a legal entity of the Public Administration type (Holder / Creator of a Seal).

The Applicant for this certificate must have powers of representation that allow him/her to request the certificate on behalf of the legal entity to which the certificate is issued.

The use of the private key associated with this certificate provides integrity and authenticity to the documents and transactions to which it is applied.

This certificate can be associated to a private key activated by a machine or application, to allow the operations that use it to be performed automatically and unassisted. It is also allowed as a machine or client application identification element in TLS secure electronic communication protocols.

- **Non Qualified Certificate OCSP-HSM**

Each Root CA and each SubCA managed by Camerfirma within the hierarchies under this CPS issues an OCSP certificate, under the corresponding "PC Non Qualified OCSP Certificate", which will be used to sign the responses of the CA's OCSP service about the status of the certificates issued by the CA, while the CA is active.

The OIDs of these certificates can be consulted in the following table:

OID:	• **Qualified Certificate of Electronic Seal** CHAMBERS OF COMMERCE ROOT Hierarchy - 2016 AC CAMERFIRMA FOR LEGAL PERSONS - 2016 ○ 1.3.6.1.4.1.17326.10.16.2.1.1 QSCD Card/Token ○ 1.3.6.1.4.1.1.17326.10.16.2.1.2 Non QSCD ○ 1.3.6.1.4.1.17326.10.16.2.1.3 ○ 1.3.6.1.4.1.17326.10.16.2.1.4 Firma • **Qualified Certificate of Electronic Stamp AAPP** CHAMBERS OF COMMERCE ROOT Hierarchy - 2016 AC CAMERFIRMA FOR LEGAL PERSONS - 2016 ○ 1.3.6.1.4.1.17326.10.16.2.2.2.1.3.3.3.1 High Level QSCD Card/Token ○ 1.3.6.1.4.1.17326.10.16.2.2.2.1.4.3.1 Medium level- Non QSCD Hierarchy CHAMBERS OF COMMERCE ROOT - 2008 Camerfirma AAPP II - 2014 ○ 1.3.6.1.4.1.1.17326.1.3.3.2 (no new certificates are issued) • **Non Qualified Code Signing Certificates** Hierarchy CHAMBERS OF COMMERCE ROOT - 2008 Camerfirma Corporate Server II - 2015 ○ 1.3.6.1.4.1.17326.10.11.3.1.1 (P12) ○ 1.3.6.1.4.1.1.17326.10.11.3.1.1 (CSR) Camerfirma Codesign II - 2014 ○ 1.3.6.1.4.1.17326.10.12.2 • **Non Qualified Certificate of Electronic Seal** Hierarchy CHAMBERS OF COMMERCE ROOT - 2008 Camerfirma Corporate Server II - 2015 ○ 1.3.6.1.4.1.17326.10.11.3.1.1 (P12) ○ 1.3.6.1.4.1.17326.10.11.3.1.2 (P10) Camerfirma AAPP II - 2014 (Does not issue new certificates) ○ 1.3.6.1.4.1.17326.1.3.3.2 • **OCSP Non Qualified Certificates** Hierarchies Chambers of Commerce Root - 2008, CHAMBERS OF COMMERCE ROOT - 2016 GLOBAL CHAMBERSIGN ROOT - 2016 ○ 1.3.6.1.4.1.1.17326.10.9.8 (HSM) CAMERFIRMA ROOT 2021 Hierarchy ○ 1.3.6.1.4.1.17326.10.21.0.1 (HSM)
Location:	https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-CPS-CPS/

3 USES OF THE CERTIFICATE

3.1 APPROPRIATE USES OF CERTIFICATES

Certificates issued under these CPs are used for the following purposes:

- Signer Authentication.
- Qualified electronic seal or advanced electronic seal, depending on whether the certificate is issued on a qualified electronic signature creation device or not.
- Integrity of the sealed document: The use of these certificates guarantees that the signed document is complete, i.e. that the document was not altered or modified after it was signed by the Signatory/Subscriber.
- Asymmetric or mixed encryption without key recovery, under the responsibility of the owner/subscriber.

3.2 PROHIBITED USES OF CERTIFICATES

Certificates may only be used within the limits and for the purposes for which they were issued in each case.

The certificates are not designed (they are not intended and are not authorized for use or resale) as hazardous situation monitoring equipment or for uses requiring fail-safe performance, such as the operation of nuclear facilities, airborne navigation or communications systems, or weapons control systems, where failure could directly result in death, personal injury or severe environmental damage.

The use of the certificates in operations that contravene the CP applicable to each one of the certificates, the CPD, the Terms and Conditions or the CA's contracts with the RAs or with the Subscribers shall be considered as improper use, for the appropriate legal purposes, therefore exempting the CA, according to the legislation in force, from any liability for this improper use of the certificates made by the Holders or any third party.

4 OBLIGATIONS

4.1 OBLIGATIONS OF CAMERFIRMA

Camerfirma, as a Trust Service Provider that issues certificates, is obliged to the following:

a) Publish accurate and updated information.

b) Manage the issuance, delivery and revocation of certificates by itself or through its Registration Authorities (RA).

c) Execute the services with the appropriate technical and material means and personnel, with the required professional qualifications.

d) To comply with the quality levels in the services in accordance with those established in the CPS in terms of technical, operational and safety aspects.

e) Notify the subscriber, before the expiration date, of the possibility of renewing the certificate, as well as its revocation, if applicable.

f) To have a publicly accessible consultation service on the validity or revocation status of issued certificates.

g) Retain the information related to the issuance of the certificate for 15 years from the expiration of the certificate.

4.2 OBLIGATIONS AND RESPONSIBILITIES OF THE SUBSCRIBER , OF THE APPLICANT AND OF THE CERTIFICATE HOLDER

a) Comply with the applicable regulations, the Certification Practices Statement (CPS) and the Certification Policy (CP) and, if applicable, the contractual documents signed with the CA and/or RA.

b) Accept the General Terms and Conditions of the service.

c) Provide the CA with the necessary information for a correct identification.

d) Make reasonable efforts to confirm the accuracy and truthfulness of the information provided.

e) Diligently guarding your private key

f) Report the existence of any cause for revocation.

g) Notify any change in the data provided for the creation of the certificate during its period of validity.

h) Do not monitor, manipulate or reverse engineer the technical implementation of certification services.

4.3 OBLIGATIONS OF THIRD PARTIES RELYING ON CERTIFICATES

Third parties relying on a certificate issued by Camerfirma must:

a) Verify the validity of the certificates presented by the signatories.
b) To know and be subject to the guarantees, limits and responsibilities applicable to the acceptance and use of the certificates on which it relies.
c) Limit the reliability of the certificates to the permitted uses of the same, in accordance with what is expressed in the certificate extensions and the relevant CP.
d) Notify Camerfirma of any anomalous event or situation related to the certificate that may be considered a cause for revocation of the certificate.

5 LIMITATION OF LIABILITY

Camerfirma shall not be liable for damages caused to the person to whom it has provided its services or to third parties in good faith, if it incurs in any of the following cases:

a) Failure to provide Camerfirma with truthful, complete and accurate information for the issuance of the certificate, in particular, regarding the data that must be included in the electronic certificate or that are necessary for its issuance or for the termination or suspension of its validity.
b) Failure to notify Camerfirma without undue delay of any change in the circumstances reflected in the electronic certificate.
c) Negligence in the conservation of your signature creation data.
d) Not to request the suspension or revocation of the electronic certificate in case of doubt as to the maintenance of the confidentiality of its signature creation data.
e) Use the signature creation data when the validity period of the electronic certificate has expired or Camerfirma notifies the expiration or suspension of its validity.
f) Failure to verify revocation or expiration of the certificate, or failure to verify the signature by relying parties.
g) Camerfirma shall not be liable for damages in case of inaccuracy of the data contained in the electronic certificate if these have been accredited by means of a public or official document, registered in a public registry.

6 PROTECTION OF PERSONAL DATA

Camerfirma complies with the regulations in force at all times regarding data protection, in particular, it has adapted its procedures to the General Data Protection REGULATION (EU) 2016/679 (GDPR) and the Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights.

Personal information that is not publicly available in the content of a certificate or CRL is considered private.

Personal information about an individual available in the contents of a certificate or CRL, is considered non-private as it is necessary for the provision of the contracted service, without prejudice to the rights corresponding to the holder of the personal data under the LOPDGDD/RGPD legislation.

Before entering into a contractual relationship, Camerfirma shall provide the interested parties with prior information about the processing of their personal data and exercise of rights, and if applicable, shall obtain the mandatory consent for the processing differentiated from the main processing for the provision of the contracted services.

7 SERVICE FEES AND REFUND POLICY

The prices of certification services or any other related service are available and updated on Camerfirma's website https://www.camerfirma.com/certificados-digitales/ or after consultation with Camerfirma's support department at https://www.camerfirma.com/contacto-soporte/ or by calling +34 91 136 91 05.

Each type of certificate has a specific published retail price, except for those that are subject to prior commercial negotiation.

Camerfirma does not have a specific refund policy and abides by the general regulations in force.

8 APPLICABLE LAW

The execution, interpretation, modification or validity of these CPS and the CP shall be governed by the provisions of Spanish and European Union legislation in force from time to time. Specifically, this CPS and the CP are governed by the following regulations:

- Regulation (EU) 910/2014 of the Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 as regards the establishment of the European digital identity framework (eIDAS Regulation).
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (SRI Directive 2), (NIS2).
- Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down implementing provisions of Directive (EU) 2022/2555 on technical and methodological requirements for cybersecurity risk management measures and further specification of the cases in which an incident is considered significant with trust service providers and other obliged parties.
- Law 6/2020, of November 11, 1920, regulating certain aspects of electronic trust services.
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting minimum technical specifications and procedures for security levels of electronic identification means in accordance with Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC
- Organic Law 3/2018 of December 5, 2018, on the protection of personal data and guarantee of digital rights.
- Law 34/2002, of July 11, 2002, on information society services and electronic commerce.
- Order ETD/465/2021, of May 6, regulating remote video identification methods for issuing

qualified electronic certificates.

- Order ETD/743/2022, of July 26, amending Order ETD/465/2021, of May 6, regulating remote video identification methods for the issuance of qualified electronic certificates.

Apendice 1 History of the document

March 2016	V 1.0	Document creation
April 2025	V 1.1	Document update