Tinexta Infocert

PDS - CAMERFIRMA'S 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 from the address:
https://pds.camerfirma.com/

Language: English

Code: PUB-2025-18-07

INDICE

1 TRUSTED SERVICE PROVIDER INFORMATION

1.1 ORGANIZATION

The corporate data of the Trusted 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 PERSONAL CERTIFICATE POLICY

Camerfirma issues the following types of certificates under the Personal Certificate Policy:

- **Qualified Citizen Certificate**:
  This qualified certificate identifies a natural person (Holder/Signatory) only to act in his/her own name.

- **Corporate Qualified Certificate**
  This qualified certificate identifies a natural person (Holder/Signatory) and determines, as specific attributes, its relationship (labor, mercantile, collegial, etc.) with an Entity.

- **Qualified Certificate of Self-Employment**
  This qualified certificate identifies a natural person (Holder/Signatory) and determines, as specific attributes, his/her status as a self-employed person, his/her economic activity and, if applicable, the registered trade name under which the self-employed person carries out his/her profession.

- **Qualified Certificate of Self-Employment**
  This qualified certificate identifies a natural person (Holder/Signatory) and determines, as specific attributes, his status as a self-employed person, his economic activity, his status as a registered professional, and if applicable, the registered trade name under which the self-employed person practices his profession.

- **Certificate of Legal Representative of an Entity with/without Legal Personality**

  This qualified certificate identifies a natural person (Holder/Signatory) and determines, as specific attributes, his condition of legal representative or attorney-in-fact with full powers, with capacity to act on behalf of a legal or unincorporated entity.

  It is aimed at legal representatives of Entities with legal personality (Sole Administrator, Joint and Several Administrator, Managing Director, Managing Director, etc.), legal representatives of Entities without legal personality (Sole Administrator, Joint and Several Administrator, Director/Manager, President of the Community of Owners, etc.), and attorneys-in-fact with very broad powers of representation of Entities with or without legal personality (similar to those of a legal representative), which allow them to act both in the area of relations and procedures of the Entities with or without legal personality.), and to proxies with very broad powers of representation of Entities with or without legal personality (similar to those of a legal representative) that allow them to act both in the scope of the relations and procedures of the Entity with the Public Administrations (uses of authentication and signature) and in the scope of the contracting of goods or services related to the ordinary operation of the Entity (uses of signature).

The joint legal representatives who wish to apply for this certificate must hold the joint and several or specific general power to act before the Public Administrations, on behalf of the Entity with or without legal personality.

- **Certificate of Voluntary Representative of an Entity with/without Legal Personality before the AAPP (Public Administration)**

  This qualified certificate identifies a natural person (Holder/Signatory) and determines, as specific attributes, its capacity to represent an Entity with or without legal personality in the scope of its relations and procedures with the Public Administrations (authentication and signature uses).

  It is aimed at attorneys-in-fact with general power of attorney or specific power of attorney that includes powers that allow them to carry out, on behalf of the entity with or without legal personality, actions and procedures before the Public Administrations that require the use of the electronic signature or the electronic certificate.

  Joint attorneys-in-fact who wish to apply for this certificate must hold powers of attorney that include the joint and several power of attorney to represent the Entity with or without legal personality in its dealings and procedures with the Public Administrations. Alternatively, they can provide a specific power of attorney or a reliable document signed by all the attorneys-in-fact jointly in favor of one of them.

- **Certificate of proxy for an entity with/without legal personality**

  This qualified certificate identifies a natural person (Holder/Signatory) and determines, as specific attributes, its capacity to act on behalf of an Entity with or without legal personality only for certain powers framed in its function or department in the Entity (uses of signature of private documents of the ordinary commercial traffic of the Entity).

  This certificate is not valid for authentication or signature uses on behalf of the Entity with or without legal personality in platforms of the Public Administration, due to the implicit limitation of the powers whose exact scope cannot be known by the Relying Party.
  Joint attorneys-in-fact who wish to apply for this certificate must hold powers of attorney that include the corresponding joint and several powers within the framework of their function or department in the Entity. Alternatively, they may provide a specific power of attorney or a reliable document signed by all the attorneys-in-fact jointly in favor of one of them.

- **Public Employee Certificates With/without Pseudonym**

  These certificates identify a natural person (Holder/Signatory) as a public employee.

  The qualified certificates issued under this CP can be used by the electronic signature systems

of the personnel at the service of the Public Administrations, in accordance with the provisions of Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

Camerfirma issues Non-Qualified public employee certificates with and without authentication and encryption pseudonym, always in the cloud.

The purpose of these certificates is to identify the signatories and to be able to sign documents and electronic transactions.

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

OID:

- **Qualified Citizen Certificate**
  CHAMBERS OF COMMERCE ROOT Hierarchy - 2016
  - 1.3.6.1.4.1.1.17326.10.16.1.1.1: QSCD Card/Token
  - 1.3.6.1.1.4.1.1.17326.10.16.1.1.1, 1.3.6.1.4.1.1.17326.99.18.1: QSCD Cloud
  - 1.3.6.1.4.1.1.17326.10.16.1.1.2: No QSCD

  CAMERFIRMA ROOT 2021 Hierarchy
  - 1.3.6.1.4.1.1.17326.10.21.1.1.1: QSCD Card/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.1.3: QSCD Cloud

  INFOCERT-CAMERFIRMA ROOT 2024 Hierarchy
  - 1.3.6.1.4.1.1.17326.10.21.1.1.2: No QSCD
- **Qualified Corporate / Self-Employed / Chartered Self-Employed Certificate**
  CHAMBERS OF COMMERCE ROOT Hierarchy - 2016
  - 1.3.6.1.4.1.1.17326.10.16.1.2.1: QSCD Card/Token
  - 1.3.6.1.1.4.1.17326.10.16.1.2.1, 1.3.6.1.4.1.1.17326.99.18.1: QSCD Cloud
  - 1.3.6.1.4.1.1.17326.10.16.1.2.2 - No QSCD

  CAMERFIRMA ROOT 2021 Hierarchy
  - 1.3.6.1.4.1.1.17326.10.21.1.2.1: QSCD Card/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.2.3: QSCD Cloud
- **Qualified Representative Certificates**
  CHAMBERS OF COMMERCE ROOT Hierarchy - 2016
  - Legal Representative of Entity with/without Legal Personality
    - 1.3.6.1.4.1.17326.10.16.1.3.1.1: QSCD Card/Token
    - 1.3.6.1.1.4.1.17326.10.16.1.3.1.1, 1.3.6.1.4.1.1.17326.99.18.1: QSCD Cloud
    - 1.3.6.1.4.1.1.17326.10.16.1.3.1.2: No QSCD
  - Voluntary Representative of Entity with/without Legal Personality before the Public Administrations
    - 1.3.6.1.4.1.17326.10.16.1.3.2.1: QSCD Card/Token
    - 1.3.6.1.1.4.1.17326.10.16.1.3.2.1, 1.3.6.1.4.1.17326.99.18.1: Cloud QSCD
    - 1.3.6.1.4.1.17326.10.16.1.3.3.2.2: No QSCD
  - Proxy of Entity With/without Legal Personality
    - 1.3.6.1.4.1.17326.10.16.1.3.3.1: QSCD Card/Token
    - 1.3.6.1.1.4.1.17326.10.16.1.3.3.1, 1.3.6.1.4.1.1.17326.99.18.1: QSCD Cloud
    - 1.3.6.1.4.1.17326.10.16.1.3.3.2: No QSCD

  CAMERFIRMA ROOT 2021 Hierarchy

- Legal Representative of Entity with Legal Capacity
  - 1.3.6.1.4.1.1.17326.10.21.1.3.1: QSCD Card/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.3.3: QSCD Cloud
- Legal Representative of an Unincorporated Entity
  - 1.3.6.1.4.1.17326.10.21.1.4.1: QSCD Card/Token
  - 1.3.6.1.4.1.17326.10.21.1.4.3: QSCD Cloud
- Voluntary Representative of a Legal Entity before the Public Authorities
  - 1.3.6.1.4.1.1.17326.10.21.1.5.1: QSCD Card/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.5.3: QSCD Cloud
- Voluntary Representative of an Unincorporated Entity before the Public Authorities
  - 1.3.6.1.4.1.1.17326.10.21.1.6.1: QSCD Card/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.6.3: QSCD Cloud
- Proxy of Entity with Legal Capacity
  - 1.3.6.1.4.1.1.17326.10.21.1.7.1: QSCD Card/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.7.3: QSCD Cloud
- Proxy of Unincorporated Entity
  - 1.3.6.1.4.1.1.17326.10.21.1.8.1: QSCD Card/Token
  - 1.3.6.1.4.1.1.17326.10.21.1.8.3: QSCD Cloud

- **Certificates of Public Employee with/without pseudonym**
  CHAMBERS OF COMMERCE ROOT Hierarchy - 2016
  - Qualified Certificate of Signature - High Level
    - 1.3.6.1.1.4.1.17326.10.16.1.5.1.3.4.1: QSCD Card/Token
    - 1.3.6.1.1.4.1.17326.10.16.1.5.1.3.4.1, 1.3.6.1.4.1.17326.99.18.1: Cloud QSCD
  - Non-Qualified Authentication Certificate - High Level
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2: Tarjeta/Token
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2, 1.3.6.1.4.1.17326.99.18.1: Nube
  - Non-Qualified Certificate of Encryption - High Level
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3: Tarjeta/Token
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3, 1.3.6.1.4.1.17326.99.18.1: Nube
  - Qualified Certificate - Intermediate Level
    - 1.3.6.1.4.1.17326.10.16.1.5.1.1.3.4.4: QSCD Card/Token / No QSCD
    - 1.3.6.1.1.4.1.17326.10.16.1.5.1.3.4.4, 1.3.6.1.4.1.17326.99.18.1: QSCD Cloud
  -

Location: https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

3 USES OF THE CERTIFICATE

3.1 APPROPRIATE USES OF CERTIFICATES

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

- Authentication of the Holder.
- Qualified electronic signature or advanced electronic signature, depending on whether the certificate is issued in a qualified electronic signature creation device or not.
- Asymmetric or mixed encryption without key recovery.

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 CAMERFIRMA'S OBLIGATIONS

Camerfirma, as a Trusted 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) 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 renewal of its certificate, as well as its revocation, if applicable e.

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, APPLICANT AND 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 RA with the information and/or documentation necessary for its correct identification, guaranteeing its authenticity, accuracy and truthfulness.

d) Inform the RA or CA of any change in the data provided for the issuance of the certificate and contained therein, during the period of validity of the certificate.

e) Request the RA or CA as soon as possible to revoke the certificate when it becomes aware of the existence of any cause for revocation, in accordance with the provisions of the CPS and the applicable CP.

f) Immediately notify the CA or RA in the event that, before the end of the period of validity of the certificate, it detects or is notified that any incorrect or inaccurate information has been included in the certificate or that, unexpectedly, the information in the certificate does not correspond to reality or has changed subsequent to the issuance of the certificate.

g) Immediately inform the CA or RA of any situation, before the end of the certificate's validity period, that may affect the security of the private key associated with the certificate, such as the loss, theft or potential compromise of the private key, or the loss of control of the private key by the HOLDER due to the compromise of its activation data.

h) Use and safeguard the certificate and its private key, the private key activation data and the means that give access to them, and the associated device if applicable (for certificates issued on a card or QSCD token), diligently, taking reasonable precautions to prevent their loss, disclosure, modification or unauthorized use, which ensures the exclusive control of the private key by the HOLDER (signatory) in the case of electronic signature certificates.

i) Not to disclose the private key associated with the certificate, nor the activation data of the private key, nor the means that give access to them to third parties.

j) Keep and guard the revocation PIN with the utmost diligence, and do not communicate or disclose it to unauthorized third parties.

k) Check the validity and valid revocation status of the certificate used as indicated in the CPS/CP.

l) Not to use the private key, the certificate or any other technical support delivered by the CA or the RA to perform any transaction prohibited by applicable law, or for any use prohibited or not authorized in the applicable CPS or CP or in the certificate itself.

m) In case of loss or misplacement of the Card/Token, QSCD or Non-QSCD device containing the certificate issued by CAMERFRIRMA, the HOLDER/RESPONSIBLE PARTY must inform the RA or CA as soon as possible and, in any case, within 24 hours of the occurrence of the aforementioned circumstance.

n) Not to use the private key or the certificate after knowledge of the compromise of the private key, or after the validity period of the certificate has expired, or after having requested the suspension or revocation of the certificate, or after having been informed of the revocation of the certificate or the compromise of the private key of the issuing CA, except, if applicable, for the decryption of keys.

o) If the Holder or the Responsible Party generates the Holder's keys, when the certificate issuance process so requires, the Holder and, if applicable, the Responsible Party are obliged to:

   i Generate the keys using an algorithm recognized as acceptable for the use of the certificate and the private key, including, if applicable, the advanced or qualified electronic signature, or the advanced or qualified electronic seal, during the period of validity of the certificate, and in accordance with the requirements of the corresponding CP.

   ii Use key lengths and algorithms recognized as acceptable for the use of the certificate and the private key, including, if applicable, the advanced or qualified electronic signature, or the advanced or qualified electronic seal, during the period of validity of the certificate, and in accordance with the requirements of the corresponding CP.

p) For certificates issued on secure cryptographic devices, QSCD or Non-QSCD, generate the keys inside the secure cryptographic device, QSCD or Non-QSCD.

q) Pay the fees for the issuance services for the type of certificate requested as set forth in the applicable CPS/CP.

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 preservation of your signature creation data, in ensuring their confidentiality and in the protection of any access or disclosure of them or, where appropriate, of the means giving access to them.
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 data subjects with prior information about the processing of their personal data and the exercise of their rights and, where applicable, shall obtain the mandatory consent for the processing, which is different 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 trusted 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