BASIC PKI DISCLOSURE STATEMENT

AC CAMERFIRMA SA

LEGAL PERSONS

Version 1.0

Language: **English**
Date: March 2016

March 2016	V1.0	Document creation

Table of Contents

1. Introduction ____ *4*

2. CA Contact Info ____ *5*

3. Certificate type, validation, procedures and usage ____ *6*

4. Reliance limits ____ *7*

5. Obligations of subscribers ____ *8*

6. Obligations of the Relying Parties ____ *9*

7. Exclusion and liability limitation clauses ____ *10*

8. Applicable agreements, certification practice statement, certificate policy ____ *11*

9. Data protection directives ____ *12*

10. Reinbursement directives ____ *13*

11. Governing Law and settlement of disputes clauses ____ *14*

11.1. Governing Law ____ **14**

11.2. Settlement of disputes clauses ____ **14**

12. CA and certificate directory licenses, confidentiality trademarkas and audit ____ *15*

Annex I: Acronyms ____ *16*

1. Introduction

The present document introduces an excerpt of the characteristics and requirements of the PKI of Camerfirma, which are established in their entirety on the CPS and the CP that apply to the certificate for which one is applying or with which one is operating.

It is highly recommendable the reading of the CPS in its entirety as well as the applicable CP, to form a clear idea of the specifications, objectives, rules, rights, responsibilities and obligations by which the provision of the certification service is governed.

The present Basic Statement is elaborated conforming to the technical specification “ETSI TS 101 456: Policy Requirements for Certification Authorities issuing qualified certificates”. In particular the recommendations from its Annex B for the “PKI Disclosure Statement”.

2. CA Contact Info

This PKI is administrated and managed by the juridical department of Camerfirma, which can be contacted through the following means:

E-mail:	juridico@camerfirma.com
Telephone:	+34 902 361 207
Fax:	+34 914 119 661
Address:	Camerfirma – Departamento Jurídico C/ Ribera del Loira, 122 - 8042 Madrid
Location:	https://www.camerfirma.com/address

3. Certificate type, validation, procedures and usage

The Camerfirma Certificates for Legal Persons allow a juridical person to be identified within the scope of its activity.

The Camerfirma Certificates for Legal Persons within the "Chambers of Commerce Root" hierarchy are the following ones:

- Corporate digital stamp certificate.

The Camerfirma Certificates for Legal Persons can be used with the following purposes:

Identification of the entity: The Signer/Subscriber of the Certificate can authenticate, against a different party, its identity and linkage with the entity, proving the association of its private key with the corresponding public key, contained in the Certificate.

The Signer/Subscriber will be able to validly identify to any person by means of the signature of an e-mail or any other kind of data.

Integrity of the signed document: The usage of this Certificate guarantees that the signed document is intact, that is, it guarantees that the document was not altered or modified after being signed by the Signer/Subscriber. It is certified that the message received by the Relying Party is the same that was issued by the Signer/Subscriber.

Non-repudiation of the origin: The usage of this Certificate also guarantees that the person signing the document cannot repudiate it, that is, the Signer/Subscriber who has signed it cannot deny de authorship or integrity of it.

Although it may be possible to use the Certificate for data encryption, the CA cannot be held responsible for this activity, due to it not keeping a copy of the private key of the Signer/Bearer for security reasons, as stated in the CP. The recovery of the encrypted data in case of loss of the private key by the Signer/Subscriber or the Relying Party is, therefore, not guaranteed. This usage will be carried out, in every case, under the responsibility of the Signer/Subscriber.

4. Reliance limits

The certificates must be used for the functions and purposes established on its corresponding Certification Policy, without the possibility of them being used for other functions and purposes.

According to the governing law, the responsibility of CAMERFIRMA and the RA does not extend to those scenarios in which the improper use of the certificate originate from conducts ascribable to the Subscriber or the Relying Party for:

- Not providing the adequate information, initially or subsequently as a consequence of modifications of the circumstances reflected on the electronic certificate, when its inaccuracy could not be detected by the certification services provider.
- Committing negligence with regard to the conservation of the data for the creation of the signature and its confidentiality.
- Not requesting the suspension or revocation of the data of the electronic certificate in case of doubt about the preservation of the confidentiality.
- Using the signature after the expiry of the validity period of the electronic certificate.
- Exceeding the established limits of the electronic certificate.
- Demeanors imputable to the Relying Party if it takes action in a negligent way, that is, when it does not ascertain or take into account the restrictions that appear on the certificate about its possible usages and value of the transactions; or when the validity period of the certificate has not been taken into account.
- Damages caused to the Subscriber or Relying Parties by the inaccuracy of the data that appear on the electronic certificate if those have been certified by means of a public document, inscribed in a public registry if deemed demandable.

5. Obligations of subscribers

Bearers of a Camerfirma Certificate for Legal Persons will have the following obligations:

1. Provide the CA with the information required to perform a correct identification.
2. Make the efforts that can be reasonably required to confirm the accuracy and veracity of the provided information
3. Diligently safeguard his private key.
4. Notify the existence of any cause of revocation.
5. Notify any change of the data provided for the creation of the certificate during its validity period.
6. Not monitoring, modifying or performing acts of reverse engineering on the technical implementation of the certification services.

6. Obligations of the Relying Parties

Third parties relying on a Camerfirma Certificate for Legal Persons will have the following obligations:

1. Verify the validity of the certificates at the moment of performing any operation based on them.
2. Know and comply the warranties, limits and responsibilities applicable with the acceptance and usage of the trusted certificates and agree to abide by them.
3. Limit the trust of the certificates to their allowed uses, in conformity with the extensions of the certificates and the applicable CP
4. Notify of any anomalous event or situation relative to the certificate which could be considered a cause for its revocation.

7. Exclusion and liability limitation clauses

The CA will not be held responsible in any case when it faces any of the following circumstances:

1. States of war, natural disasters or any other case of force majeure.
2. Usage of the certificates provided that it goes beyond the provisions of the governing law and Certification Policy.
3. Improper or fraudulent usage of the certificates or CRL issued by the CA.
4. Usage of the information contained within the Certificate or the CRL.
5. Non-compliance of the obligations of Subscribers and Relying Parties established in the current regulations, the Certification Policy or the corresponding practices.
6. Damage caused in the period of verification of the causes of revocation.
7. Fraud on the information provided by the applicant.

8. Applicable agreements, certification practice statement, certificate policy

All the applicable agreements, CPS and CP can be found on the website created for that effect: http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

9. Data protection directives

The CA will establish the information that should be considered confidential, subject in every case to the governing law on data protection, and more precisely the terms of the Organic Law 15/1999 of December 13th of Protection of Personal Data (LOPD).

The RA that constitute the PKI of Camerfirma shall verify that the applicant for a certificate is informed and gives his consent to the treatment of his personal data, the finality they are going to be given, the recipients of the data and its incorporation into the repository declared by Camerfirma for said effect.

The owners of the data will be able to exercise their rights of Access, rectification and opposition by contacting the address stated in the present document.

The information contained in the Certificate Directory is considered personal data, subject to the terms of the LOPD and other additional rules, reason why the access by third parties is not allowed.

10. Reimbursement directives

Camerfirma CA does not have a specific reimbursement directive, and recourses to the general governing law.

11. Governing Law and settlement of disputes clauses

11.1. Governing Law

The operations and functioning of the PKI of Camerfirma, as well as the CPS that apply to each type of certificate will adhere to the applicable governing laws, with a special attention towards:

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- Law 59/2003, of 19 December on Electronic Signature.
- Organic Law 15/1999, of 13 December on Personal Data Protection.
- Royal Decree 994/1999, of 11 June, by which the Regulations on security measures of the automated repositories containing personal data are approved.

In the same vein, the internal rules and procedures dictated by Camerfirma aimed towards guaranteeing the security requirements of the aforementioned Royal Decree should be observed.

11.2. Settlement of disputes clauses

Every controversy or conflict derived from the present document will be solved permanently, by means of an arbitration at law of an arbiter in the framework of the Spanish Court of Arbitration, in accordance with its Rules and Statute, to which the administration of the arbitration and the designation of the arbiter or arbitration tribunal is entrusted. The parties hereby state their commitment to abide by the arbitration decision.

12. CA and certificate directory licenses, confidentiality trademarks and audit

The objectives of Camerfirma regarding security and quality have been fundamentally the attainment of the ISO/IEC 27001, ISO/IEC 20000 certifications and the biennial execution of internal audits of the Camerfirma Certification System, and mainly the RA, to guarantee the compliance of the internal procedures.

Camerfirma is subject to periodic WEBTRUST for CA, WEBTRUST SSL BR and WEBTRUST SSL EV audits, which ensure that the documents of policies and CPS have an adequate format and reach as well as they are aligned with their CP and CPS.

Camerfirma is also subject to the controls performed by the national regulating organism, being this the Ministry of Industry of the Government of Spain.

An audit will be held with a minimum periodicity of a year, unless a shorter period is established by the current regulations.

The audit will verify in every case that:

- The CA has a system that guarantees the quality of the offered service.
- The CA meets the requirements of the Certification Policy.
- The Certification Practices of the CA conform to the CP, the agreement with the Approving Authority of the Policy, and the terms of the current regulations.
- Camerfirma adequately manages the security of its information systems.

Annex I: Acronyms

CA Certification Authority.

CP Certification Policy.

CPS Certificate Practices Statement.

CRL Certificate Revocation List.

PKI Public Key Infrastructure.

RA Registration Authority.