PKI DISCLOUSURE STATEMENT

Título del documento:	PKI Disclousure Statement
Tipo de documento:	Política
Nombre del fichero:	PDS.docx
Versión:	1.1
Estado:	Aprobado
Confidencialidad:	Público
Fecha:	19/04/2017
Autor:	Javier Marcos

Revisión, Aprobación		
Revisado por:	Enric Hernández	Fecha: 16/05/2018
Aprobado por:	Enric Hernández	Fecha: 16/05/2018

Historial de cambios			
Versión	**Fecha**	**Descripción de la acción**	**Páginas**
1.0	19/04/2017	Creación del documento.	
1.1	15/05/2018	Changes to fulfill the GDPR requirements. Add FEREN certificate with remote key.	

TOC

1. Information and contact info

This document is about PKI disclosure statements, hereinafter PDS, and it aims to describe in a basic and brief manner the Certification Practise Statement, hereinafter CPS, and Certification Policy (CP) of Agencia Notarial de Certificación, S.L.U.

The corporate contact details and information are the following:

Agencia Notarial de Certificación S.L.U.

Paseo del General Martínez Campos, 46, 6th floor, Building Elcano

28010 Madrid (Spain)

NIF number: B-83395988

Phone number: 902 348 347

E-mail: ancert@ancert.com

Website: http://www.ancert.com

2. Certificate type, validation procedures and usage

2.1. Types of certificates

The following tables show the certificates classes that are issued for each root belonging to ANCERT. The table is composed by certificate name (Certificate) and purpose, certificate identification (OID), use and validity.

Class "**General Council of Notaries**": includes certificates issued by the Notarial Certification Agency to Notaries working in Spain (FEREN certificates), Notaries who hold positions within the organization of the General Council of Notaries (CGN) or Notarial Colleges (title certificates) and employees of Notaries and Notarial Colleges of Spanish territory (certificates of employees). All of them are qualified certificates on Electronic Signatures.

Certificate	OID	Use	Validity
FEREN Certificates (for signature)	ANCERT.4.1.1.2.1	Generation of qualified electronic signature	3 years
FEREN certificates (for authentication)	ANCERT.4.1.1.2.2	Personal authentication in electronic information systems	3 years
FEREN certificates (for encryption)	ANCERT.4.1.1.2.3	Encryption and decryption of electronic documents, with	3 years

		key recovery.	
FEREN certificates (remote signature)	ANCERT.4.1.1.3.2	Electronic signature with remote keys.	3 years
Title Certificates (for signature)	ANCERT.4.1.2.2.1	Generation of qualified electronic signature	3 years
Title Certificates (for authentication)	ANCERT.4.1.2.2.2	Personal authentication in electronic information systems	3 years
Title Certificates (for encryption)	ANCERT.4.1.2.2.3	Encryption and decryption of electronic documents, with key recovery	3 years
Certificates of employees (for signature)	ANCERT.4.2.1.2.1	Generation of qualified electronic signature,	3 years
Certificates of employees (for authentication)	ANCERT.4.2.1.2.2	Personal authentication in electronic information systems	3 years
Certificates of employees (for encryption)	ANCERT.4.2.1.2.3	Encryption and decryption of electronic documents, with key recovery	3 years

Class "**Notarial Certificates**": includes groups certificates issued to the general public for which a notary has acted as the Registration Entity, thus providing the highest level of legal security.

Certificate	**OID**	**Use**	**Validity**
Notarial personal certificate (qualified signature)	ANCERT.1.1.1.2.1	Generation of qualified electronic signature	3 years
Notarial personal certificate (authentication)	ANCERT.1.1.1.2.2	Personal authentication in electronic information systems, in the physical presence or remotely.	3 years
Notarial personal certificate (encryption)	ANCERT.1.1.1.2.3	Encryption and decryption of electronic documents, with key recovery.	3 years
Notarial personal representation certificate (qualified signature)	ANCERT.1.1.2.2.1	Generation of qualified electronic signature	3 years
Notarial personal representation certificate (authentication)	ANCERT.1.1.2.2.2	Personal authentication in electronic information systems, in the physical presence or remotely	3 years

Notarial personal representation certificate (encryption)	ANCERT.1.1.2.2.3	Encryption and decryption of electronic documents, with key recovery.	3 years
Hardware notarial certificate of secure server	ANCERT.1.2.1.2.1	To natural or legal persons, as owners of SSL servers, in order to establish secure communications between the server and SSL/TLS client	825 days
Software notarial certificate of secure server	ANCERT.1.2.1.2.2	To natural or legal persons, as owners of SSL servers, in order to establish secure communications between the server and SSL/TLS client	825 days
Hardware notarial certificate of timestamping	ANCERT.1.2.3.2.1	To natural or legal persons, as owners of timestamping servers	3 years
Software notarial certificate of timestamping	ANCERT.1.2.3.2.2	To natural or legal persons, as owners of timestamping servers	3 years
Hardware notarial certificate of code signing	ANCERT.1.2.5.2.1	To natural or legal persons, as editors of source code for public distribution	3 years
Software notarial certificate of code signing	ANCERT.1.2.5.2.2	To natural or legal persons, as editors of source code for public distribution	3 years
Hardware notarial certificate of secure application	ANCERT.1.2.6.1.1	To natural or legal persons, as owners of software applications requiring authentication, digital signature or encryption features	3 years
Software notarial certificate of secure application	ANCERT.1.2.6.1.2	To natural or legal persons, as owners of software applications requiring authentication, digital signature or encryption features	3 years
Notarial certificate of OCSP trusted responder	ANCERT.1.2.7.1.2	Issued to natural or legal persons, as owners of OCSP servers	3 years
Notarial corporate certificate (qualified signature)	ANCERT.1.3.1.2.1	Generation of qualified electronic signature	3 years

Notarial corporate certificate (authentication)	ANCERT.1.3.1.2.2	Personal authentication in electronic information systems, in the physical presence or remotely	3 years
Notarial corporate certificate (encryption)	ANCERT.1.3.1.2.3	Encryption and decryption of electronic documents, with key recovery	3 years
Notarial corporate representation certificate (qualified signature)	ANCERT.1.3.2.2.1	Generation of qualified electronic signature	3 years
Notarial corporate representation certificate (authentication)	ANCERT.1.3.2.2.2	Personal authentication in electronic information systems, in the physical presence or remotely	3 years
Notarial corporate representation certificate (encryption)	ANCERT.1.3.2.2.3	Encryption and decryption of electronic documents, with key recovery	3 years
Notarial certificate for electronic invoicing.	ANCERT.1.3.3.1.2	To natural or legal persons, requiring a natural person acting as legal representative of the legal person	3 years

Class "**Public Law Corporation Personal certificates**": includes groups certificates issued to private Corporations that act as Registration Authorities.

Certificate	OID	Use	Validity
Hardware Personal Corporate Certificates (qualified signature)	ANCERT 2.1.1.2.1	Generation of electronic signature	3 years
Hardware Personal Corporate Certificates (authentication)	ANCERT 2.1.1.2.2	Personal authentication in electronic information systems, in the physical presence or remotely	3 years
Hardware Personal Corporate Certificates (encryption)	ANCERT 2.1.1.2.3	Encryption and decryption of electronic documents, with key recovery	3 years

Software Personal Corporate Certificates	ANCERT 2.1.1.2.4	Generation of electronic signature Personal authentication in electronic information systems, in physical presence or distance Encryption and decryption of electronic documents, with key recovery	3 years
Software Corporate Certificates of Secure Application	ANCERT 2.2.1.1.2	To private corporations, as owners of software applications requiring authentication, digital signature or encryption features	3 years
Software Corporate Certificates of Secure Server	ANCERT.2.2.2.1.2	To private corporations, as owners of SSL servers, in order to establish secure communications between the server and SSL/TLS client	3 years

Class "**Public Law Corporation certificates**": includes groups certificates issued to Public Law Corporations that act as Registration Authorities.

Certificate	OID	Use	Validity
Public Law Corporation Personal certificates for electronic signature.	ANCERT.3.1.1.2.1	Generation of electronic signature	3 years
Public Law Corporation Personal certificates for authentication.	ANCERT.3.1.1.2.2	Personal authentication in electronic information systems, in the physical presence or remotely	3 years
Public Law Corporation Personal certificates for encryption.	ANCERT.3.1.1.2.3	Encryption and decryption of electronic documents, with key recovery	3 years
Public Law Corporation certificates of secure application	ANCERT.3.2.1.1.2	Authentication in electronic information systems. Generation of electronic signatures. Encryption and decryption of electronic documents	3 years

The Notarial Certification Agency publishes, in its repository, a document containing the OIDs for certification practices and current certificates

2.2. Permitted uses for certificates

The certificates issued are only permitted to use in the following cases:

- **Authenticity of origin:** ensures that the document or electronic communication comes from the person or entity who claims to be from.
- **Server authentication**: the electronic communication comes from the server that claims to be from Users can verify server authenticity by verify the certificate of secure server.
- **Acceptance of content by the issuer**: Prevents that the sender of a message can deny, the issuance.
- **Integrity:** allows the verification that an electronic document has not been modified by any external agent.
- **Confidentiality:** ensures that the data transmitted cannot be read by unauthorized third parties since data are encrypted.

All these features are accomplished by use of electronic signature. The recipient of a digitally signed message can verify the signature using the certificate.

2.3. Limits and prohibitions on use of certificates

All certificates must be used for their proper function and purpose as set out in this document, and may not be used in other functions and for other purposes.

- Certificates should be used only in accordance with applicable law, taking into account the restrictions on imports and exports in each moment.
- Certificates may contain additional limits within the field *Subject Directory Attributes*, as described in the Certification Practice Statement, as well as the general conditions of use of the certificates.
- Corporate certificates cannot be used to sign public key certificates of any kind, or sign revocation lists (CRLs) or certificate status information (OCSP or similar), except where expressly permitted.
- Certificates are not designed; neither can be used or resold for control equipment in dangerous situations or for uses requiring fail-safe performance, such as operation of nuclear, air navigation and communication systems, or weapon control systems, where failure could lead directly to death, personal injury or severe environmental damage.

All legal liabilities, contractual or extra contractual, direct or indirect damages derived from limited and/or prohibited uses fall under the responsibility of the subscriber. Under no circumstances may the subscriber, the key holder or injured third parties claim the Notarial Certification Agency or the General Council of Notaries any compensation for damages or liabilities derived from the use of keys or certificates for limited and/or prohibited uses

3. Reliance limits

The CA does not set reliance limits for the Certificates it issues, we will abstain to civil liability coverage, by professional civil liability insurance or through a bond or guarantee.

The guaranteed amount is, at least, 3,000,000 Euros or higher.

See Section 7 below for limitation of liability.

4. Obligations of subscribers

4.1. General conditions

Subscribers should:

- If the subscriber generates his own keys, it shall be required to:
  - Generate subscriber keys using an algorithm recognized as acceptable for qualified electronic signature.
  - Create the keys within the secure signature creation device.
  - Use key lengths and algorithms recognized as acceptable for qualified electronic signature.
- Provide the Notarial Certification Agency and their registration entities complete and proper information, in accordance with the requirements of this certificate policy and specific policies, especially regarding the registration procedure.
- Give the consent prior to the issuance and delivery of a certificate, for the publication in the repository and when appropriate, for the notification of the issue to third parties.
- Fulfil the obligations provided for the subscriber in the Certificate Practice Statement.
- Use the certificate in accordance with the provisions of section 3.4 of the Certificate Practice Statement.
- Be diligent in keeping the private key to prevent unauthorized use, not allowing the use of the private key to anyone else.
- Communicate to the Notarial Certification Agency and any person that the subscriber or the key holder believes may trust the certificate, without unjustifiable delays:
  - The loss, theft or potential compromise of the private key or the secure device.
  - Loss of control over the private key or the security device, due to the potential compromise of activation data or any other cause.
  - Inaccuracies or changes to the content of the certificate that might be known by the subscriber or the key holder.
- Cease in the use of the private key after the period specified in section 8.3.2. of the Certificate Practice Statement.
- Transfer, to the key holders, specific obligations.
- Do not monitor, manipulate or reverse-engineer on the technical implementation of the certification services of the Notarial Certification Agency or the General Council of Notaries, without prior written permission.

- Do not intentionally compromise the security of certification services of the Notarial Certification Agency or the General Council of Notaries, without prior written permission.

4.2. Digital signatures generation by subscribers

Subscribers generating digital signatures using the private key corresponding to their public key included in the certificate, shall recognize, in due legal document that such signatures are electronic signatures equivalent to handwritten signatures. Civil liability of the subscriber Notarial Certification Agency requires the subscriber and, if applicable, the holder of keys, to ensure:

- If the subscriber was the requestor for the certificate that all statements made in the request are correct.
- That all information supplied by the subscriber and contained in the certificate is correct.
- That the certificate is used exclusively for authorized and legal uses, according to the corresponding Certificate Practice Statement.
- That each digital signature generated using the public key included in the certificate is the digital signature of the subscriber, and the certificate has been accepted and is operational (not expired or been revoked) at the time of signature creation.
- That the subscriber is an end entity and not a certification service provider, and will not use the private key corresponding to the public key included in the certificate to sign any certificate (or any other certified public key format) or Certificate Revocation List, or for acting on behalf of other certification service provider or any other case.
- Those digital signatures will only be generated while having the certainty that no unauthorized person has ever had access to the private key.
- That the subscriber is solely responsible for damage caused by its breach of duty to protect the private key.

5. Certificates status checking obligations of relying parties

The services for certificate status checking are provided through a web query interface, through the repository, and through the OCSP service. The services should be available 24 hours a day, 7 days a week, year round, except for scheduled downtime.

In the other hand, the obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

- The verifier is notified, who has access to sufficient information to make an informed decision at the time of verifying a certificate and relying on the information contained in the certificate.

- The verifier recognizes that the use of the Repository and Certificate Revocation Lists of ANCERT, is governed by the DCP, and undertakes to fulfil the technical, operational and security requirements described in the DCP.
- The verifier must validate two signatures, to trust a message or document:
    - It has to be verified the authentication electronic signature of the message or document.
    - It has to be verified the electronic signature of the title certificate belonging to the subscriber.
- The verifier is obliged to use software for electronic signature verification with the technical, security and operational capacity enough to perform the signature verification process correctly, and will remain solely responsible for the damage it may suffer from the incorrect choice of the software.
- It is strictly forbidden trusting a non verified signature or certificate.
- If the verifier trusts a certificate that has not been verified, he will assume all risks associated with this action.
- The verifier can rely on the identification and, where appropriate, in the public key of the subscriber, within the limitations for use.
- The verifier is obliged not to use any type of status information of certificates (or any other type) that has been provided by ANCERT, in performing any act prohibited by applicable law.
- The verifier is obliged not to inspect, interfere with or reverse engineer the technical implementation of the public certification services provided by ANCERT, without prior written consent of ANCERT.
- The verifier agrees not to intentionally compromise the security of the public certification services provided by ANCERT.

6. Limited warranty and disclaimer/Limitation of liability

6.1. Limited warranty

The Notarial Certification Agency ensures, at least, the subscriber:

- That there are no factual errors in the information contained in the certificates known.
- That there is no factual errors in the information contained in the certificates due to lack of due diligence in the management of the certificate request or the generation.
- That the certificates meet all requirements established in the Certificate Practice Statement.
- That revocation services and the repository meet all requirements established in the Certificate Practice Statement.

The Notarial Certification Agency guarantees, at least, to third parties trusting the certificates:

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise indicated.
- In case of certificates published in the repository, that the certificate has been issued to the subscriber identified in it and that the certificate has been accepted.
- That the approval of the certificate request and the issuance has met the requirements established in the Certificate Practice Statement.
- The speed and security in the provision of services, especially revocation and repository services.

The Notarial Certification Agency may reject any other warranty not legally enforceable, except as provided in above.

6.2. Disclaimer/Limitation of liability

The Notarial Certification Agency will limit its liability to the issuing and managing of certificates and, where appropriate, managing of subscriber's key pairs and cryptographic devices supplied by the Notarial Certification Agency.

The Notarial Certification Agency limits its liability by including usage limits, and limits of the value of transactions for which the certificate can be used.

All legal liabilities, contractual or extra contractual, direct or indirect damages derived from limited and/or prohibited uses fall under the responsibility of the subscriber.

Under no circumstances may the subscriber, the key holder or injured third parties claim the Notarial Certification Agency or the General Council of Notaries any compensation for damages or liabilities derived from the use of keys or certificates for limited and/or prohibited uses.

7. Applicable agreements, Certification Practise Statement, Certificate Policy

The Notarial Certification Agency publishes at the repositories located in his website http://www.ancert.com the following documents:

- Certification Policy (CP)
- Certification Practise Statement (CPS)
-
- Certificates directory
- Certificate validation services

8. Privacy policy

In order to provide certification services, the Notarial Certification Agency (ANCERT) needs to collect, process and store certain information, including personal information.

The Notarial Certification Agency develops a privacy policy in accordance with Regulation (EU) 2016/679 o the European Parliament and of the Council 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 (General Data Protection Regulation),Organic Law 15/99 of December 13th on the Protection of Personal Data (LOPD), and describes it in its Declaration of Certification Practices, together with aspects and security procedures corresponding to the Security Document, as described in Royal Decree 1720/2007 of December 13 (RD 1720/2007).

The Notarial Certification Agency will protect the data processing in the course of his business as trust service providers (hereinafter Files) in accordance with the provisions of the regulations referred to above.

To perform its certification activity, Registration Authorities will access these files.

The Notarial Certification Agency will have the status of Controller, being the decision maker on the content and use of the processing of personal data, and the Registration Authorities shall be deemed responsible for the processing, which must use the data contained in those files only and exclusively for the purposes listed in its Certification Practice Statement.

9. Refund policy

The Notarial Certification Agency has the following refund policy:

When a correction or amendment of the Certificate Practice Statement implies a limitation of rights of use or restriction on the scope of an existing certificate, the subscriber may claim a refund, limited to the value of the certificate.

In other cases, the subscriber shall have no right to refund the cost of the certificate.

10. Applicable law, complaints and dispute resolution

10.1. Applicable law

The Notarial Certification Agency specifies, in the conditions of issue and use of certificates, that the law applicable to the provision of services, including policy and certification practices, is the Spanish law.

10.2. Dispute resolution

The Notarial Certification Agency specifies, in the conditions of issue and use of certificates, procedures for mediation and conflict resolution.

The situations of dispute arising from use of the certificates are resolved by applying the same criteria of competence that in case of signed handwritten documents.

10.3. Jurisdiction clause

The Notarial Certification Agency specifies, in the conditions of issue and use of certificates, a jurisdiction clause stating that international jurisdiction is for the Spanish judges.

The territorial and functional jurisdiction is determined under the rules of international private law rules that may apply.

11. TSP and repository licenses, trust mark and audit

The Notarial Certification Agency has passed the following audits for the last year:

- WebTrust for audit the service and the PKI process.
- WebTrust SSL for the issuing of secure server certificates
- eIDAS. Regulation of digital signature.