Certification Practice Statement

General Information

Documentary Control

Security classification:	Public
Target entity:	UANATACA
Version:	1.0
Edition date:	17/03/2016
File:	UANATACA CPS v1r0_v04.docx
Format:	Open Office XML
Authors:	GA/AC

Formal state

Prepared by:	Reviewed by:	Approved by:
Name: GA/AC Date: 15/03/2016	Name: FA/NA Date: 22/03/2016	Name: Date:

Versions control

Version	Parts that change	Description of the change	Author of the change	Date of the change
1.0	Original	Document creation	GA/AC	22/03/2016

Index

1. Introduction

1.1. Presentation

This document declares the Certification Practice of the digital signature of UANATACA.

The issued certificates are the following:

- **Natural Person**
  - Natural Person in SOFT
  - Natural Person in SSCD Identification
  - Natural Person in SSCD signature
  - Natural Person in SSCD encryption

- **Representative**
  - Representative in SOFT
  - Representative in SSCD identification
  - Representative in SSCD signature
  - Representative in SSCD encryption

- **Electronic Seal**
  - Electronic Seal Medium level
  - Electronic Seal High level

- **Public Employee**
  - Public Employee Medium level
  - Public Employee High level (identification)
  - Public Employee High level (signature)
  - Public Employee High level (encryption)

1.2. Document Number and identification

This document is the “Certification Practice Statement of UANATACA”.

1.2.1. Certificates' identifiers

UANATACA has assigned an object identifier (OID) to each certificate policy, for their identification by requests.

Number OID	Type of certificates
	NATURAL PERSON
1.3.6.1.4.1.47286.1.1.1	*Natural Person in SOFT*
1.3.6.1.4.1.47286.1.1.2.1	*Natural Person in SSCD Identification*
1.3.6.1.4.1.47286.1.1.2.2	*Natural Person in SSCD signature*
1.3.6.1.4.1.47286.1.1.2.3	*Natural Person in SSCD encryption*
	REPRESENTATIVE
1.3.6.1.4.1.47286.1.2.1	*Representative in SOFT*
1.3.6.1.4.1.47286.1.2.2.1	*Representative in SSCD identification*
1.3.6.1.4.1.47286.1.2.2.2	*Representative in SSCD signature*
1.3.6.1.4.1.47286.1.2.2.3	*Representative in SSCD encryption*
	ELECTRONIC SEAL for the Public Administration
1.3.6.1.4.1.47286.1.3.1	*Electronic Seal Medium level (SOFT)*
1.3.6.1.4.1.47286.1.3.2	*Electronic Seal High level (SSCD)*
	PUBLIC EMPLOYEE
1.3.6.1.4.1.47286.1.4.1	*Public Employee Medium level*
1.3.6.1.4.1.47286.1.4.2.1	*Public Employee High level (identification)*
1.3.6.1.4.1.47286.1.4.2.2	*Public Employee High level (signature)*
1.3.6.1.4.1.47286.1.4.2.3	*Public Employee High level (encryption)*
1.3.6.1.4.1.47286.1.5	**Electronic Time Stamping Unit**

In case of contradiction between this Certification Practice Statement and other documents of practices and procedures, the established in this Pratice Statement shall prevail.

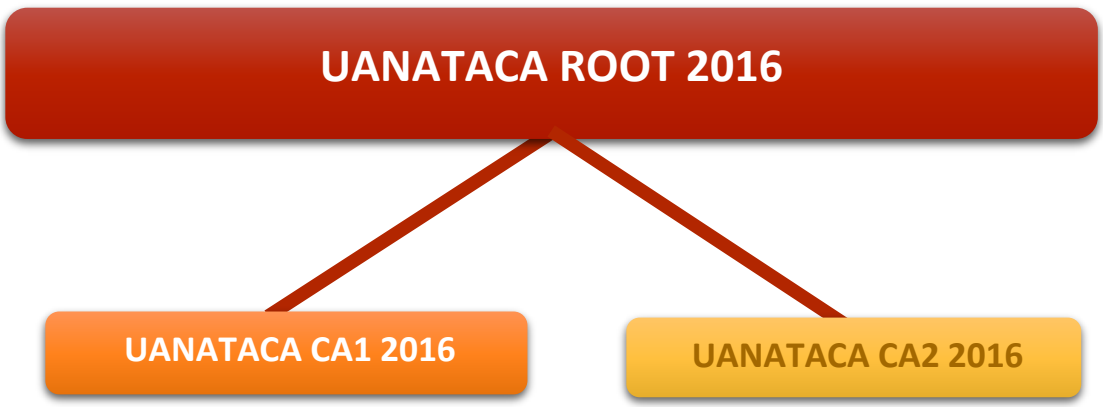
1.3. Participants in the certification services

1.3.1. Certification service provider

The certification service provider is the natural or legal person that issues and manages certificates for end entities, using a Certification Entity, or provides other services related to the electronic signature.

UANATACA is a certification service provider, acting in accordance with the provisions of the electronic signature Law 59/2003, December 19th, and the ETSI technical standards applicable to the issuance and management of recognized certificates, mainly the ETSI TS 101 456, EN 319 411-1 and EN 319 411-2, in order to facilitate the legal requirements and the international recognition of his services.

To provide certification services, UANATACA has established a hierarchy of certification entities:



1.3.1.1. UANATACA ROOT 2016

This is the certification authority root of the hierarchy that issues certificates to other CAs, and whose public key certificate has been self-signed.

Identification data:

CN:	UANATACA ROOT 2016
Digital fingerprint:	6d c 50 84 0a5 9c d 62 26 3c0 91 0f 8c 2d ce 0 23d 66 74ad
Valid from:	Friday, March 11th 2016
Valid until:	Monday, March 11th 2041
RSA key length:	4.096 bits

1.3.1.2. UANATACA CA1 2016

This is the certification authority within the hierarchy that issues certificates to end entities, whose public key certificate has been digitally signed by UANATACA ROOT 2016.

Identification data:

CN:	UANATACA CA1 2016
Digital fingerprint:	7f 2c b 4f4 22 69 7c b 0cf 8b 69 27 51 cb d4 cc 64 a2 c4 50
Valid from:	Friday, March 11th 2016
Valid until:	Sunday, March 11th 2029
RSA key length:	4.096 bits

1.3.1.3. UANATACA CA2 2016

This is the certification authority within the hierarchy that issues electronic time stamping certificates to end entities, among others, whose public key certificate has been digitally signed by UANATACA ROOT 2016.

Identification data:

CN:	UANATACA CA2 2016
Digital fingerprint:	0e ce 03 78 52c 9db 6e 63bc ea 36 55b3 9a e4 28 8e 8d 2d
Valid from:	Friday, March 11th 2016
Valid until:	Sunday, March 11th 2029
RSA key length:	4.096 bits

1.3.2. Registrars

Generally, the certification service provider acts as a registrar of the identities of the subscribers of certificates.

They are also registrars of certificates subject to this Certification Practice Statement, due to their condition/status of corporate certificates, the units designated for this function by the subscribers of the certificates, act like a human resources department, since they have authentic records about the entail of the signers to the subscribers.

The subscribers' record functions are performed by delegation and according to the instructions of the certification service provider, under the terms of Article 13.5 of the electronic signature Law 59/2003, December 19th, and under the sole responsibility of the certification service provider towards third parties.

1.3.3. End entities

The end entities are the persons and the organizations receivering the services of issuance, management and use of digital certificates, for identification and electronic signature.

The end entities of UANATACA of the certification services will be the following:

1. Subscribers of the certification service
2. Signers
3. Relying parties

1.3.3.1. Subscribers of the certification services

The subscribers of the certification services are companies, entities and organizations that acquire them from UANATACA for its use in its business or organizational corporate level.

The subscriber of the certification services acquires a license to use the certificate, for his own use – electronic seal certificates – or in order to facilitate the certification of the identity of a particular person duly authorized for various actions in the organizational area of the subscriber – electronic signature certificates. In this case, this person figures identified in the certificate as provided in the following section.

The subscriber of the certification services is, therefore, the client of the certification services provider, according to the commercial legislation, and has the rights and obligations defined by the certification services provider, which are additional and do not prejudice the rights and obligations of the signers, as it is authorized and regulated in the European technical standards applicable to the issuance of recognized electronic certificates, specially ETSI TS 101 456, section 4.4, kept in its later versions, and nowadays, in ETSI EN 319 411, sections 5.4.2 y 6.3.4.e).

1.3.3.2. Signers

The signers are natural persons who possess exclusively the digital signature keys for their identification and use the advanced or qualified electronic signature; being typically the employees, clients and other people binded to the subscribers, to the natural person certificates; the legal representatives and volunteers, to the representative certificates; or the Public Administrations' employees, to the public employee certificates.

The signers are properly authorized by the subscriber and properly identified in the certificate through their name and last name, their VAT number valid in the jurisdiction where the certificate has been issued, without being possible, in general, the use of pseudonyms.

The private key of a signer is not stored and, therefore, can't be recovered by the certification services provider, so the natural persons identified in the relevant certificates are the sole responsible for their protection and should consider the implications of losing a private key.

Given the existence of certificates for different uses of the electronic signature, as the identification, the more generic term “natural person identified in the certificate” is also used, with full respect to compliance the electronic signature legislation in relation with the signer’s rights and obligations.

1.3.3.3. Relying parties

The relying parties are persons and organizations that receive digital signatures and digital certificates.

To trust certificates, the relying parties must verify them, as it is established in the certification practice statement and in the corresponding instructions available in the web page of the Certification Authority.

1.4. Use of certificates

This section lists the requests for which each type of certificate can be used, sets limitations to certain requests and prohibits certain requests of certificates.

1.4.1. Uses permitted for certificates

The permitted uses specified in the various fields of the certificate profiles should be taken into consideration, visible on the webpage https://www.uanataca.com

1.4.1.1. Natural person certificate, issued on software

This certificate has the OID 1.3.6.1.4.1.47286.1.1.1.

This certificate is issued in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0.

Natural person certificates, issued on software, are legally recognized in accordance with Article 11.1, with the content prescribed by Article 11.2 and issued in compliance with the

obligations of Articles 12, 13 and 17 to 20 of the Electronic Signature Law 59/2003 of December 19th.

Natural person certificates, issued on software, do not guarantee their correct functionality as intended with secure signature creation devices, as referred to Article 24.3 Law 59/2003, December 19th.

These certificates guarantee the identity of the subscriber and the person named on the certificate, and they allow the generation of the "advanced electronic signature based on a recognized electronic certificates".

The certificates can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other digital signature requests, in accordance with the agreements between the interested parties or with legal rules applicable in each individual case.

These certificates allow the encryption of documents, content and data messages, under the sole responsibility of the signer, considering that UANATACA does not offer backup services nor key recovery. Thus, UANATACA won't respond in any case of loss of any encrypted information that can't be recovered.

The information of uses in the certificate's profile indicates the following:

a) The "key usage" field is actived and thereforee it allows us to perform the following functions:
    a. Digital Signature, for authentication
    b. Content commitment, for electronic signature
    c. Key Encipherment
    d. Data Encipherment

b) In the "Qualified Certificate Statements" field appears the following statement:

a. qCCompliance (0.4.0.1862.1.1), reports that the certificate is issued as recognized.

1.4.1.2. Natural person certificate, issued on SSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.1.2.1 for authentication, the OID 1.3.6.1.4.1.47286.1.1.2.2 for signature and the OID 1.3.6.1.4.1.47286.1.1.2.3 for encryption.

This certificate is issued in accordance with the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2.

Natural person certificates, issued on SSCD, are legally recognized in accordance with Article 11.1, with the content prescribed by Article 11.2 and issued in compliance with the obligations of Articles 12, 13 and 17 to 20 of the Electronic Signature Law 59/2003 of December 19th.

Natural person certificates, issued on SSCD work with secure signature creation device in accordance with Article 24.3 of Law 59/2003 of December 19th, and which comply with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference TS 101 456.

These certificates guaratee the identity of the signer and his entail with the subscriber of the certification service, and allow the generation of the "recognized electronic signature"; that is, the advanced electronic service that is based on a recognized certificate, therefore it is compared to the handwritten signature by legal effect, without having to meet any additional requirement.

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email
b) Other digital signature requests

These certificates allow the encryption of documents, content and data messages, under the sole responsibility of the signer, considering that UANATACA does not offer backup services nor key recovery. Thus, UANATACA won't respond in any case of the loss of any encrypted information that can't be recovered.

The information of uses in the certificate's profile indicates the following:

a) The "key usage" field is activated and thereforee it allows us to perform the following functions:
    a. In the authentication profile:
        i. Digital Signature, for authentication
    b. In the signature profile:
        i. Content commitment, for electronic signature
    c. In the encryption profile:
        i. Key Encipherment
        ii. Data Encipherment

b) In the "Qualified Certificate Statements" field appears the following statement:
    a. qCCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as recognized.
    b. QcSSCD (0.4.0.1862.1.4), which reports that the certificate is used exclusively in conjuction with a secure signature creation device.

1.4.1.3. Representative certificate, issued on software

This certificate has the OID 1.3.6.1.4.1.47286.1.2.1.

This certificate is issued in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0.

Representative certificates issued on software are legally recognized in accordance with the provisions of Article 11.1, with the content prescribed by Article 11.2 and 11.4, and issued in compliance with the obligations of Articles 12, 13 certificates and 17 to 20 of the Act 59/2003 of December 19th, on electronic signature and which compliance with the

provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference TS 101 456.

Representative certificates on software do not guarantee their correct functionality as intended with secure signature creation devices, as referred to Article 24.3 Law 59/2003, December 19th.

The certificates guarantee the identity of the subscriber and of the signer, and a legal representation or a general empowerment between the signer and the entity, company or organization described in the field "O" (Organization), and allow the generation of an "advanced electronic signature based on a recognized electronic certificate".

On the other hand, the representative certificates on software can be used in requests such as those listed below:

a) Authentication in access control systems
b) Signature of secure email
c) Other digital signature requests

These certificates allow the encryption of documents, content and data messages, under the sole responsibility of the signer, considering that UANATACA does not offer backup services nor key recovery. Thus, UANATACA won't respond in any case of loss of any encrypted information that can't be recovered.

The information of uses in the certificate's profile indicates the following:

a) The "key usage" field is activated and thereforee it allows us to perform the following functions:
    a. Digital Signature, for authentication
    b. Content commitment, for electronic signature
    c. Key Encipherment
    d. Data Encipherment

b) In the "Qualified Certificate Statements" field appears the following statement:

a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as recognized.

1.4.1.4. Representative certificate, issued on SSCD

This certificate has the OID 1.3.6.1.4.1.47286.1.2.2.1 for authentication, the OID 1.3.6.1.4.1.47286.1.2.2.2 for signature and the OID 1.3.6.1.4.1.47286.1.2.2.3 for encryption.

This certificate is issued in accordance with the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2

Representative certificates, issued on SSCD, are legally recognized in accordance with Article 11.1, with the content prescribed by Article 11.2 and 11.4, and issued in compliance with the obligations of Articles 12, 13 and 17 to 20 of the Electronic Signature Law 59/2003 of December 19th.

Representative certificates, issued on SSCD work with secure signature creation device in accordance with Article 24.3 of Law 59/2003 of December 19th, and which comply with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference TS 101 456.

The certificates guarantee the identity of the subscriber and of the signer, and a legal representation or a general empowerment between the signer and the entity, company or organization described in the field "O" (Organization), and allow the generation of a "recognized electronic signature" that is, the advanced electronic signature which is based in a recognized certificate and that has been generated using a secure device, and therefore it is compared to the handwritten signature by legal effect, without having to meet any additional requirement.

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email
b) Other digital signature requests

These certificates allow the encryption of documents, content and data messages, under the sole responsibility of the signer, considering that UANATACA does not offer backup services nor key recovery. Thus, UANATACA won't respond in any case of loss of any encrypted information that can't be recovered.

The information of uses in the certificate's profile indicates the following:

a) The "key usage" field is actived and thereforee it allows us to perform the following functions:
    a. In the authentication profile:
        i. Digital Signature, for authentication
    b. In the signature profile:
        i. Content commitment, for electronic signature
    c. In the encryption profile:
        i. Key Encipherment
        ii. Data Encipherment

b) In the "Qualified Certificate Statements" field appears the following statement:
    a. qCCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as recognized.
    b. QcSSCD (0.4.0.1862.1.4), which reports that the certificate is used exclusively in conjuction with a secure signature creation device.

1.4.1.5. Electronic seal, medium level

This certificate has the OID 1.3.6.1.4.1.47286.1.3.1.

This certificate is issued in accordance with the certification statement QCP-l with the OID 0.4.0.194112.1.1.

Electronic seal certificates, medium level, are legally recognized in accordance with Article 11.1, with the content prescribed by Article 11.2, and issued in compliance with the

obligations of Articles 12, 13 and 17 to 20 of the Electronic Signature Law 59/2003 of December 19th.

These certificates are issued for the identification and authentication of the exercise of the competition in the administrative automated action in accordance with Article 18.1 of electronic access of the citizens to the Public Services Law 11/2007, of June 22nd.

The electronic seal, medium level are issued in compliance with the identification Scheme and electronic signature of the public Administrations in its current version at the date of this document.

These certificates guarantee the identity of the subscriber, the public organization and, where relevant, the representative of the organization, included in the certificate.

These certificates allow the encryption of documents, content and data messages, under the sole responsibility of the signer, considering that UANATACA does not offer backup services nor key recovery. Thus, UANATACA won't respond in any case of loss of any encrypted information that can't be recovered.

The information of uses in the certificate's profile indicates the following:

a) The "key usage" field is activated and thereforee it allows us to perform the following functions:
    a. Digital Signature, for authentication
    b. Content commitment, for electronic signature
    c. Key Encipherment
    d. Data Encipherment

b) In the "Qualified Certificate Statements" field appears the following statement:
    a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as recognized.

1.4.1.6. Electronic seal, high level

This certificat has the OID 1.3.6.1.4.1.47286.1.3.2.

This certificate is issued in accordance with the certification statement QCP-l-qscd with the OID 0.4.0.194112.1.3.

Electronic seal certificates, high level, are legally recognized in accordance with Article 11.1, with the content prescribed by Article 11.2, and issued in compliance with the obligations of Articles 12, 13 and 17 to 20 of the Electronic Signature Law 59/2003 of December 19th.

These certificates are issued for the identification and authentication of the exercise of the competition in the administrative automated action in accordance with Article 18.1 of electronic access of the citizens to the Public Services Law 11/2007, of June 22nd.

The electronic seal, high level are issued in compliance with the identification Scheme and electronic signature of the public Administrations in its current version at the date of this document.

These certificates guarantee the identity of the subscriber, the public organization and, where relevant, the representative of the organization, included in the certificate.

These certificates allow the encryption of documents, content and data messages, under the sole responsibility of the signer, considering that UANATACA does not offer backup services nor key recovery. Thus, UANATACA won't respond in any case of loss of any encrypted information that can't be recovered.

The information of uses in the certificate's profile indicates the following:

a) The "key usage" field is actived and thereforee it allows us to perform the following functions:
    a. Digital Signature, for authentication
    b. Content commitment, for electronic signature
    c. Key Encipherment
    d. Data Encipherment

b) In the "Qualified Certificate Statements" field appears the following statement:
   a. QcCompliance (0.4.0.1862.1.1), it reports that the certificate is issued as recognized.
   b. QcSSCD (0.4.0.1862.1.4), which reports that the certificate is used exclusively in conjuction with a secure signature creation device.

1.4.1.7. Public employee certificate, medium level

This certificate has the OID 1.3.6.1.4.1.47286.1.4.1.

This certificate is issued in accordance with the certification statement QCP-n with the OID 0.4.0.194112.1.0.

Public employee certificates, medium level, are legally recognized in accordance with Article 11.1, with the content prescribed by Article 11.2, and issued in compliance with the obligations of Articles 12, 13 and 17 to 20 of the Electronic Signature Law 59/2003 of December 19th.

These certificates are issued for public employees to identify them as persons to the Public Administration service, binding them with it, with compliance to the requirements established in the electronic access of the citizens to the Public Services Law 11/2007, of June 22nd, and its development regulations.

Public employee certificates, medium level do not guarantee their correct functionality as intended with secure signature creation devices, as referred to Article 24.3 Law 59/2003, December 19th.

Public employee certificates, medium level are issued in compliance with the identification Scheme and electronic signature of the public Administrations in its current version at the date of this document.

These certificates guarantee the identity of the subscriber and the person named on the certificate, and they allow the generation of the "advanced electronic signature based on a recognized electronic certificates".

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email
b) Other digital signature requests

These certificates allow the encryption of documents, content and data messages, under the sole responsibility of the signer, considering that UANATACA does not offer backup services nor key recovery. Thus, UANATACA won't respond in any case of loss of any encrypted information that can't be recovered.

The information of uses in the certificate's profile indicates the following:

a) The "key usage" field is actived and thereforee it allows us to perform the following functions:
    a. Digital Signature, for authentication
    b. Content commitment, for electronic signature
    c. Key Encipherment
    d. Data Encipherment

b) In the "Qualified Certificate Statements" field appears the following statement:
    a. qCCompliance (0.4.0.1862.1.1), it reports that the certificate is issued as recognized.

1.4.1.8. Public employee certificate, high level

This certificate has the OID 1.3.6.1.4.1.47286.1.4.2.1 for identification, the OID 1.3.6.1.4.1.47286.1.4.2.2 for signature and the OID 1.3.6.1.4.1.47286.1.4.2.3 for encryption.

This certificate is issued in accordance with the certification statement QCP-n-qscd with the OID 0.4.0.194112.1.2.

Public employee certificates, high level, are legally recognized in accordance with Article 11.1, with the content prescribed by Article 11.2, and issued in compliance with the obligations of Articles 12, 13 and 17 to 20 of the Electronic Signature Law 59/2003 of December 19th.

These certificates are issued for public employees to identify them as persons to the Public Administration service, binding them with it, with compliance to the requirements established in the electronic access of the citizens to the Public Services Law 11/2007, of June 22nd, and its development regulations.

Public employee high level certificates work with secure signature creation device, in accordance with Article 24.3 of electronic signature Law 59/2003, of December 19th, which comply with the provisions of the technical standards of the European Telecommunications Standards Institute, identified with the reference TS 101 456. Likewise, the public employee high level certificates are issued in accordance with the identification Scheme and the electronic signature of the Public Administrations in its current version at the date of this document.

The certificates guarantee the identity of the subscriber and of the signer, and allow the generation of a "recognized electronic signature"; that is, the advanced electronic signature that is based in a recognized certificate and that has been generated using a secure device, and therefore in accordance with the Article 3 of Law 59/2003, of December 19th, which is compared to the handwritten signature by legal effect, without having to meet any additional requirement.

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of secure email
b) Other digital signature requests

These certificates allow the encryption of documents, content and data messages, under the sole responsibility of the signer, considering that UANATACA does not offer backup services nor key recovery. Thus, UANATACA won't respond in any case of loss of any encrypted information that can't be recovered.

The information of uses in the certificate's profile indicates the following:

a) The "key usage" field is activated and thereforee it allows us to perform the following functions:
    a. In the authentication profile:
        i. Digital Signature, for authentication
    b. In the signature profile:
        i. Content commitment, for electronic signature
    c. In the encryption profile:
        i. Key Encipherment
        ii. Data Encipherment

b) In the "Qualified Certificate Statements" field appears the following statement:
    a. QcCompliance (0.4.0.1862.1.1), which reports that the certificate is issued as recognized.
    b. QcSSCD (0.4.0.1862.1.4), which reports that the certificate is used exclusively in conjuction with a secure signature creation device.

1.4.1.9. Electronic timestamping unit certificate

This certificate has the OID 1.3.6.1.4.1.47286.1.5.

This certificate is issued in accordance with the certification statement QCP-l with the OID 0.4.0.194112.1.1.

The electronic seal certificates are qualified certificates issued for the timestamping authorities for signing the timestamps that they produce.

These certificates allow signing the timestamps issued, from the moment they have got a valid timestamping certificate, while it is in force.

The synchronization of the times in UANATACA is done with a time server NTP stratum 1.

This server, a Meinberg LANTIME M300 / GPS, with TCXO high stability, GPS receiver, is comprised of an internal GPS card to synchronize simultaneously with the satellites having visibility at all times (3 to 8), and anti –Ray.

1.4.2. Limits and forbidden uses of certificates

Certificates are used for their own function and the established purpose, not being able to be used for other functions or other purposes.

Likewise, certificates must be used only in accordance with the applicable law, especially taking into consideration the import and export restrictions prevailing at any given time.

Certificates can't be used to sign requests of issuance, renovation, suspension or revocation of certificates, nor public key certificates of any type, or Certificate Revocation List (CRL).

Certificates haven't been designed, can't be assigned and its use or resale as control equipment for dangerous situations isn't authorized nor for uses that require fail-safe actions, as the operation of nuclear installation, navigation systems or air communications, or weapons control systems, where a failure could lead directly to death , personal injury or severe environmental damage.

There must be taken into account the limits indicated in the various fields of the certificates profiles, visible in the web of UANATACA (https://www.uanataca.com).

The use of the digital certificates in operations that violate this Certification Practice Statement, the binding legal documents with each certificate, or the contracts with the Registration Authorities or their signers/subscribers, is considered to misuse the legal purposes, exempting therefore to UANATACA, according to the current legislation, of any liability for this misuse of the certificates made by the signer or any third party.

UANATACA doesn't have any access to the data on which the use of the certificate can be applied. Therefore, as a result of this technical impossibility to access to the content of the message, UANATACA can't issue any evaluation about the mentioned content, the subscriber, the signer or the person responsible of the custody, is the one who will assume any responsibility arising from the content rigged to the use of a certificate.

Likewise, any responsibility that could result from the use of the custody out of the limits and conditions of use included in this Certification Practice Statement, the binding legal documents with each certificate, or the contracts or agreements with the registration authorities or with their subscribers, and any other misuse thereof derived from this section or may be interpreted as such according to the law, will be attributable to the subscriber, signer or the responsible of it.

1.5. Policy management

1.5.1. Organization that administers the document

Uanataca, S.A.
Calle Riera de Can Todà, 24-26, 6º, 1ª
08024 Barcelona

1.5.2. Contact information of the organization

Uanataca, S.A.
Calle Riera de Can Todà, 24-26, 6º, 1ª
08024 Barcelona

1.5.3. Document management procedures

The documental and organization system of UANATACA S.A. guarantees, according to the existence and request of the corresponding procedures, the correct maintenance of this document and the specification of the service related to itself.

2. Publication of information and deposit of certificates

2.1. Deposit(s) of certificates

UANATACA has a Deposit of certificates, in which the information related to the certification services is published.

That service is available 24 hours, 7 days per week and, in case of the system failure was under UANATACA's control, it will make its best efforts to ensure that the service is back available within the prescribed time in the section 5.7.4 of this certification practice statement.

2.2. Publication of information of the certification services provider

UANATACA publishes the following information, in its Deposit:

- Issued certificates, when the consent of the natural person identified in the certificate has been obtained
- Revoked certificates list and other information about the status if the certificates revocation
- Applicable certificate policies
- Certification Practice Statement
- Policy Disclosure Statements - PDS, at least in Spanish and English.

2.3. Frecuency of publication

The information of the certification services provides, including the policies and the Certification Practice Statement, is published when available.

The Certification Practice Statement changes are governed by the established in the section **Error! Reference source not found.** of this document.

The information of the revocation status of the certificates will be published in accordance with the established in the sections 4.9.7 and 4.9.8 of this Certification Practice Statement.

2.4. Access control

UANATACA doesn't limit the read access to the information established in the section 2.2, but establishes controls to prevent non-authorized people to add, modify or delete registrations of the Deposit, to protect the integrity and authenticity of the information, especially information about the revocation status.

UANATACA uses reliable systems for the Deposit, in such a way that:

- Only authorized persons could do annotations and modifications
- The authenticity of the information could be verified
- The certificates would only be available for consulting if the natural person identified in the certificate induced his consent
- Any technical change affecting the security requirements could be detected.

3. Identification and authentication

3.1. Initial registration

3.1.1. Type of names

All certificates contain a distinguished name X.501 in the field *Subject* including a component *Common Name* (CN=), relative to the identity of the subscriber and the natural person identified on the certificate, as well as several additional identity information in the field *SubjectAlternativeName*.

The names on the certificates are as follows.

3.1.1.1. Natural person certificate, issued on software

Country (C)	State[1]
Organization (O)	Organization to which the signer is binded
Surname	Signer's surnames
Given Name	Signer's name
Serial Number	Signer's DNI/NIE
Common Name (CN)	Signer's name, surname

3.1.1.2. Natural person certificate, issued on SSCD

Country (C)	State[2]
Organization (O)	Organization to which the signer is binded
Surname	Signer's surnames

[1] The field "country" will correspond to the state where the contractual relationship take place between the signer and the entity to which it is binded (for being employee, member, partner or other link), regardless of the nationality of the employee.

[2] The field "country" will correspond to the state where the contractual relationship take place between the signer and the entity to which it is binded (for employee, member, partner or other link), regardless of the nationality of the employee.

Given Name	Signer's name
Serial Number	Signer's DNI/NIE
Common Name (CN)	Signer's name, surname

3.1.1.3. Representative certificate, issued on software

Country (C)	State[3]
Organization (O)	Organization to which the signer is binded
Surname	Signer's surnames
Given Name	Signer's name
Serial Number	Signer's DNI/NIE
Common Name (CN)	Signer's name, surname

3.1.1.4. Representative certificate, issued on SSCD

Country (C)	State [4]
Organization (O)	Organization to which the signer is binded
Surname	Signer's surnames
Given Name	Signer's name
Serial Number	Signer's DNI/NIE
Common Name (CN)	Signer's name, surname

[3] The field "country" will correspond to the state where the contractual relationship take place between the signer and the entity to which it represents, regardless of the nationality of the representative.

[4] The field "country" will correspond to the state where the contractual relationship take place between the signer and the entity to which it represents, regardless of the nationality of the representative.

3.1.1.5. Electronic seal, medium level

Country (C)	"ES"
Organization (O)	Subscriber denomination ("official" name of the organization)
Surname	Surname of responible seal
Given Name	Name of responible seal
Serial Number	Subscribing organization's ID
Common Name (CN)	Designation of automatic system or application process.
DNI/NIE of the responsible OID: 2.16.724.1.3.5.2.2.4	Seal responsible's ID
First Name OID: 2.16.724.1.3.5.2.2.6	Seal responsible's first name
Surname OID: 2.16.724.1.3.5.2.2.7	Seal responsible's first surname
Second Surname OID: 2.16.724.1.3.5.2.2.8	Seal responsible's second surname
Email OID: 2.16.724.1.3.5.2.2.9	Seal responsible's email

3.1.1.6. Electronic seal, high level

Country (C)	"ES"
Organization (O)	Subscriber denomination ("official" name of the organization)
Surname	Surname of responible seal
Given Name	Name of responible seal
Serial Number	Subscribing organization's ID
Common Name (CN)	Designation of automatic system or application process.
DNI/NIE of the responsible OID: 2.16.724.1.3.5.2.1.4	Seal responsible's ID

First Name OID: 2.16.724.1.3.5.2.1.6	Seal responsible's first name
Surname OID: 2.16.724.1.3.5.2.1.7	Seal responsible's first surname
Second surname OID: 2.16.724.1.3.5.2.1.8	Seal responsible's second surname
Email OID: 2.16.724.1.3.5.2.1.9	Seal responsible's email

3.1.1.7. Public employee certificate, medium level

Country (C)	"ES"
Organization (O)	Administration denomination ("official" name), public law organization or entity subscriber of the certificate, to which the employee is binded
Surname	First and second surname, according to the identity document (ID /Passport)
Given Name	Given Name, according to the identity document (DNI/Passport)
Serial Number	Employee's ID
Title	Occupation or position of the individual, that links with the government, agency or public entity underwriter certificate.
Common Name (CN)	Surname 1 Surname 2 – NIF of employee
DNI/NIE of the responsible OID: 2.16.724.1.3.5.3.2.4	Responsible's ID
Número de autenticación personal OID: 2.16.724.1.3.5.3.2.5	NRP o NIP of responsible of the certificate subscriber
First Name OID: 2.16.724.1.3.5.3.2.6	Certificate responsible's first name
Surname OID: 2.16.724.1.3.5.3.2.7	Certificate responsible's first surname

Second surname OID: 2.16.724.1.3.5.3.2.8	Certificate responsible's second surname
Email OID: 2.16.724.1.3.5.3.2.9	Certificate responsible's email

3.1.1.8. Public employee certificate, high level

Country (C)	"ES"
Organization (O)	Administration denomination ("official" name), public law organization or entity subscriber of the certificate, to which the employee is binded
Surname	First and second surname, according to the identity document (ID /Passport)
Given Name	Given Name, according to the identity document (ID /Passport)
Serial Number	Employee's ID
Title	Occupation or position of the individual, that links with the government, agency or public entity underwriter certificate.
Common Name (CN)	Surname 1 Surname 2 – NIF of employee
DNI/NIE of the responsible OID: 2.16.724.1.3.5.3.1.4	Responsible's ID
Número de autenticación personal OID: 2.16.724.1.3.5.3.1.5	NRP o NIP of responsible of the certificate subscriber
First Name OID: 2.16.724.1.3.5.3.1.6	Certificate responsible's first name
Surname OID: 2.16.724.1.3.5.3.1.7	Certificate responsible's first surname
Second surname OID: 2.16.724.1.3.5.3.1.8	Certificate responsible's second surname
Email OID: 2.16.724.1.3.5.3.1.9	Certificate responsible's email

3.1.2. Meaning of the names

The names in the fields of the certificates *SubjectName* and *SubjectAlternativeName* are understandable in natural language, in accordance with the provisions of the previous section.

3.1.3. Use of anonymous and pseudonymous

Under no circumstances can the pseudonymous be used for identifying an entity/Company/organization/signer.

Under no circumstances can anonymous certificates be issued.

3.1.4. Interpretation of name formats

Name formats will be interpreted in accordance with the law of the country in which the subscriber is established, on its own terms.

The field “country” will be the subscriber’s, and always be Spain for certificates issued in the Spanish Public Administrations.

The certificate shows the relation between a natural person and the company, entity or organization to which is binded, regardless the nationality of the natural person. This results from the corporate nature of the certificate, of which the subscriber is the entity, company or organization, and the natural person binded to the person authorized for its use.

The “serial number” field must include the signer’s NIF, in the certificates issued for Spanish subscribers, in order the certificate to be considered properly suitable for executing proceedings with the Spanish Public Administrations.

3.1.5. Uniqueness of names

The names of the subscribers of certificates will be unique, for each certification policy of UANATACA.

It won't be possible to assign a subscriber's name that already has been used, to a different subscriber, situation that, in theory, at first shouldn't happen, thanks to the tax identification number, or equivalent, in the names' scheme.

A subscriber can request more than one certificate whenever the combination of the following existing values in the request was different from a valid certificate:

- Tax Identification Number (NIF) or other valid legal identifier of the natural person.
- Tax Identification Number (NIF) or other valid legal identifier of the subscriber.
- Type of Certificate (Description of the certificate field).

3.1.6. Resolution of name conflicts

Certificate applicants won't include names in requests that may involve infringement, by the future subscriber, of third party rights.

UANATACA won't be required to first determine that an applicant of certificates has industrial property rights on the name of a certificate request, but at first will proceed to certify it.

Furthermore, it won't act as arbitrator or mediator, or in any other way to resolve any dispute concerning the property of names of persons or organizations, web domains, brands or commercial names.

However, in case of receiving a notification concerning a name conflict, according to the legislation of the subscriber's country, it may take appropriate actions to block or withdraw the certificate issued.

In any case, the certification services provider reserves the right to reject the certification request due to names conflict.

Any controversy or dispute arising out of this document will be solved definitively, by the arbitration law of an arbitrator within the framework of the Spanish Court of Arbitration, in accordance with its Regulation and Statute, to which the administration of the arbitration and the designation of the arbitrator or the arbitral court is entrusted.
The parties state their commitment to comply with the award rendered in the contractual document that formalizes the service.

3.2. Initial identity validation

The identity of the subscribers of the certificates is fixed at the time of signing the contract between UANATACA and the subscriber, the moment in which the existence of the subscriber and the enforcement powers of the person representing are verified. For the verification, public or notarial documentation can be use, or direct consultation to the corresponding public records.

The identity of the natural persons identified in the certificates is validated through the corporative records of the entity, Company or organization of public or private law, subscribers to the certificates. The subscriber will produce a certification of the necessary data, and will send it to UANATACA, through these methods it will enable, for registering the identity of the signers.

The files of the personal data of each identity, Company or organization of public or private law will have to be enrolled in the corresponding Data Protection Agency, for each of them, being its responsibility, and not UANATACA's, which acts as processor.

3.2.1. Proof of possession of private key

The possession of the private key is demonstrated under the reliable process of delivery and acceptance of the certificate by the subscriber, for seal certificates, and by the signer, for signature certificates.

3.2.2. Authentication of organization, company or entity identity through a representative

Natural persons who are capable of acting on behalf of public or private subscribers, will be able to act as representatives of them, as long as there exists a previous situation of legal or voluntary representation between the natural person and the public or private person, that requires their recognition by UANATACA, which will be made through the following face-to-face procedure:

1. The subscriber's representative will meet in person with an authorized representative of UANATACA, where he will have a form of authentication.

   Alternatively, the subscriber's representative will be able to get the form from UANATACA's web from its previous fulfilment.

2. The representative will fill the form, with the following information and documents:

   - His identification data, as representative:
     - Name and Surnames
     - Place and date of birth
     - Document: Representative Tax Identification Number

   - The identification data of the subscriber to which he is representing:
     - Name or business name.
     - All information existing records, including the data relative to the constitution and legal personality and the extension and validity of the representation faculty of the applicant.
     - Document: Tax Identification Number of the public or private person.
     - Document: Public documents that serve to certify the mentioned ends irrefutably and its inscription in the corresponding public registry if required. The mentioned checking can also be done through consultation in the public registry in which the constitution and empowerment documents are enrolled, being able to use the media provided by the mentioned public registries.

- The data relative to the representation or the capacity for action that holds:

    - The validity of the representation or the ability to act (the start and end date).
    - The field and the limits, in its case, of the representation or the capacity of action:
        - TOTAL. Representation or total capacity. This checking will be able to be made through a tele-consultation to the public registry stating the inscribed representation.
        - PARTIAL. Representation or partial capacity. This checking will be able to be made through an authentic electronic copy of the notarial empowerment deed, under the terms of the notarial law.

3. Once the form is completed and signed, it will be signed and delivered to UANATACA, together with supporting documentation indicated.

4. UANATACA's staff will check the identity of the representative through his ID with the content of the representation with the documents.

5. UANATACA's staff will deliver a proof of authentication and return the contributed documentation.

6. Alternatively, in accordance with the established in Article 13.1 of Law 59/2003, of December 19th, it will be possible to legitimize by legal process the signature in the form, and be delivered to UANATACA by certified post, in which case steps 3 to 5 above won't be necessary.

The certification service provision is formalized through the appropriate contract between UANATACA and the subscriber, duly represented.

3.2.3. Authentication of natural person identity

This section describes the testing methods of the identity of a natural person identify in the certificate.

3.2.3.1. In the certificates

The information of the identification of the natural persons identified in the certificates is validated comparing the information of the request with the registrations of the entity, company or organization of public or private law to which is binded, ensuring the correctness of the information to be certified.

3.2.3.2. Need of personal presence

There is no need of physical presence to request the certificates due to the already proven relationship between the natural person and the entity, Company or organization of public or private law to which is binded.

However, before delivering a certificate, the subscriber entity, Company or organization of public or private law, through their certification responsible, or other designated member, must contrast the identity of the natural person identified in the certificate though this physical presence.

During this proceedin the identity of the natural person identified in the certificate is appropriately confirmed.

Therefore, in all cases in which a certificate is issued the identity of the signer is verified in person.

3.2.3.3. Entail of the natural person

Documentary evidence of the entail of a natural person identified in a certificate with an entity, Company or organization of public or private law is determined by the persistence in the internal records (employee contract or commercial contract that links him, or the record where his position is indicated, or the request as a member of the organization…) of each public and private persons to which are binded.

3.2.4. Subscriber's not verified information

UANATACA doesn't include any information of the subscriber not verified in the certificates.

3.3. Identification and authentication of renewal requests

3.3.1. Validation for certificates routine renewal

Before renewing a certificate, UANATACA or a Registration Authority verifies that the information used to verify the identity and the remaining subscriber data and the natural person identified in the certificate remain valid.

The acceptable methods for such verifications are:

- The use of "identity verification phrase", or other methods of personal authentication, that consist in information that only the natural person identified in the certificate knows, and allows in an automatic way the renewal of the certificate, as long as the deadline legally established hasn't exceed.
- The use of the current certificate for its renewal, as long as it is a certificate issued by UANATACA and hasn't exceeded the deadline legally established for this possibility.

If any information of the subscriber or natural person identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section **Error! Reference source not found.**.

3.3.2. Identification and authentication of revocation request

Before generating a certificate to a subscriber whose certificate was renewed, UANATACA or a Registration Authority will verify that the information used that day to verify the identity and the rest of the data of the subscriber and the natural person identified in the certificate are still valid, in which case previous section shall apply.

The renewal of the certificates after their revocation won't be possible in the following cases:

- The certificate was revoked by erroneous issuance to a person different than the one identified in the certificate.
- The certificate was revoked by a non-authorized issuance by the natural person identified in the certificate.
- The certificate revoked may contain misleading or fake information.

If any information of the subscriber or natural person identified in the certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with the established in the section **Error! Reference source not found.**.

3.4. Identification and authentication of revocation request

UANATACA or a Registration Authority authenticate the requests and reports relative to certificate revocations, verifying that they come from an authorized person.

The acceptable methods for such verifications are:

- The delivery of a revocation request from the subscriber or the natural person identified in the certificate, signed electronically.
- The use of " identity verification phrase ", that consist in information that only the natural person identified in the certificate knows, and allows in an automatic way the revoke of the certificate.
- The natural person in an office of the Company, entity or organization subscriber.
- Other media, as telephone, when there is reasonable assurance of the identity of the applicant for revocation.

3.5. Authentication of a suspension request

The suspension request will be performed by the subscriber using the current form in UANATACA's web, indicating the suspension option (https://www.uanataca.com) in 24x7 schedule.

When the subscriber would want to initiate a revocation request and there were doubts for its identification, during office hours, his certificate would go onto suspension status.

4. Certificate life-cycle operational requirements

4.1. Certificate issuance request

4.1.1. Legitimation to apply for the issuance

The entity, Company or organization of public or private law concerned, must sign a certification services provision contract with UANATACA.

Likewise, before the issuance and delivery of a certificate, there must exist a request of a certificate either in the same contract or in a specific certificate request form.

When the applicant is a different person than the subscriber, there must be an authorization from the subscriber to allow the applicant to proceed with the request, which is legally implemented by a certificate request form subscribed by that applicant on behalf of the entity, Company or organization of public or private law.

4.1.2. Registration procedure and responsibilities

UANATACA receives certificates' request, made by entities, Companies or organizations of public or private law.

The requests are implemented by a document in electronic format, filled by an entity, Company or organization of public or private law, whose addressee is UANATACA, who will include the data of the persons to which the certificates will be issued. The request will be carried out by the operator authorized by the subscriber (responsible of the certification) and who has been identified in the contract between the subscriber and UANATACA.

The request will go together with the supporting documentation of the identity and other circumstances of the natural person identified in the certificate, in accordance with the established in the section 3.2.3. Also an address or other data that will allow contacting the natural person identified in the certificate.

4.2. Processing the certification request

4.2.1. Implementation of identification and authentication functions

Once the certificate applicant has been received, UANATACA ensures that the certificates' requests will be completed, precise and duly authorized, before processing them.

If so, UANATACA verifies the information provided, verifying the aspects described in section **Error! Reference source not found.**

In case of a recognized certificate, the supporting documentation of the approval of the request must be preserved and properly registered with guarantees of security and integrity during 15 years from the expiration of the certificate, even in case of early loss effective for renovation.

4.2.2. Approval or rejection of the request

In case the data is correctly verified, UANATACA should approve the request of the certificate and proceed with its issuance and delivery.

If the verification indicates that the information is not correct, or if it is suspected that it is not correct or it may affect the reputation of the Certification Authority, the Registration Authority or the subscribers, UANATACA will deny the request, or will stop its approval up to having made the additional checks that it considers appropriate.

UANATACA will definitely deny the request in case the additional checks won't help to correct the information to verify.

UANATACA notifies the approval or denial of the request to the applicant.

UANATACA will be able to automate the verification procedures of the information correction that will be in the certificates, and the approval of the requests.

4.2.3. Time to process certificate requests

UANATACA attends to the certificates' requests in order of arrival, in a reasonable time, being possible to specify a guarantee can specify a maximum guarantee in the contract certificate issuance.

Requests remain active until its approval or rejection.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

After approving the certification request, the CA proceeds to issue the certificate in a safe way and make it available to the signer for its acceptance.

The established procedures in this section are applicable in case of certification renewal, taking into consideration that the same involves the issuance of a new one.

During the process, UANATACA:

- Protects the confidentiality and integrity of the registration data that owns.
- Uses reliable systems and products that are protected against every disturbance and guarantee the technical security and, in its case, cryptographic security of the processes of certification to which they support.
- Generates a pair of keys, through a procedure of generation of certificates binded in a safe way with the procedure of generation of keys.
- Uses a procedure of generation of certificates that links in a safe way the certificate with the registration information, including the certified public key.
- It ensures that the certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the mentioned keys.
- Includes in the certificate the information established in Article 11 of Law 59/2003, of December 19th, in accordance with the established in the sections 3.1.1 y 7.1.
- Indicates the date and hour in which a certificate was issued.

4.3.2. Notification to the certificate issuance applicant

UANATACA notifies the issuance of the certificate to the subscriber and the natural person identified in the certificate.

4.4. Certificate delivery and acceptance

4.4.1. CA responsibilities

During this process, UANATACA must perform the following actions:

- Definitely confirm the identity of the natural person identified in the certificate, with the Registration Authority or subscriber collaboration, in accordance with the established in the sections 3.2.2 y 3.2.3.
- Deliver to the natural person identified in the certificate with the assistance, if any, of the Registration Authority, the sheet delivery and acceptance of the certificate with the following minimum contents:
    - Basic information about the use of the certificate, especially including information about the certification services provider and the applicable Certification Practice Statement, as his obligations, faculties and responsibilities.
    - Information about the certificate.
    - Recognition, from the signer, of receiving the certificate and the acceptance of the mentioned elements.
    - Signer liability regime.
    - Responsibility of the signer.
    - Imputation method exclusive to the signer, of its private key and its certificate activation data, in accordance with the established in the sections 6.2 y 6.4.
    - The date of the act of delivery and acceptance.
- To obtain the signature, handwritten or electronic, of the person identified in the certificate.

The Registration authority collaborates in these processes, having to register the previous acts, and preserves the mentioned original ones (delivery and acceptance sheets),

referring to UANATACA the electronic copy as well as the original when UANATACA required access to them.

4.4.2. Way in which the certificate is accepted

The acceptance of the certificate by the natural person identified in the certificate occurs when signing the delivery and acceptance sheet.

4.4.3. Publication of the certificates

UANATACA publishes the certificate in the Deposit referred in section 2.1, with the proper safety controls and whenever UANATACA had the authorization of the natural person identified in the certificate.

4.4.4. Notification of certificate issuance to third parties

UANATACA doesn't notify any issuance to third parties.

4.5. Key pair and certificate usage

4.5.1. Use by the signer

UANATACA forces him to:

- Provide to UANATACA complete and proper information, in accordance with the requirements of this Certification Practice Statement, especially on the registering procedure.
- Express his consent prior the certificate issuance and delivery.
- Use the certificate in accordance with the established in the section **Error! Reference source not found.**.
- When the certificate will work in conjunction with a SSCD, recognize its capacity of production of recognized electronic signatures; that is, equivalent to handwritten signatures, as well as other types of electronic signatures and information encryption mechanisms.

- Be especially diligent in the custody his private key, in order to prevent unauthorized uses, in accordance with the established in the sections 6.1, 6.2 and 6.4.
- Communicate to UANATACA and anyone who believes may trust the certificate , without unjustifiable delays :
    - The loss, theft or potential compromise of his private key.
    - The loss of control over his private key, due to the compromise of the activation data (ie. PIN) or any other reason.
    - The inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
- Stop using the private key once the period specified in the section 6.3.2. has elapsed.

UANATACA forces the signer to take responsibility to ensure:

- All the information in the certificate provided by the signer is correct.
- The certificate is used exclusively for legal and authorized uses, in accordance with the Certification Practice Statement.
- No unauthorized person has ever had access to the private key of the certificate, and that he is the sole responsible for any damage caused by his infringement of protecting the private key.
- The signer is an end entity and not a certification services provider, and won't use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification services provider title, nor any other case.

4.5.2. Use by the subscriber

4.5.2.1. Obligations of the certificate subscriber

UANATACA contractually forces the subscriber to:

- Provide complete and appropriate information to the Certification Authority, in accordance with the requirements of this Certification Practice Statement, especially on the registering procedure.
- Express his consent prior to the certificate issuance and delivery.

- Use the certificate in accordance with the established in the section **Error! Reference source not found.**.
- Communicate to UANATACA and anyone who believes may trust the certificate , without unjustifiable delays :
    - The loss, theft or potential compromise of his private key.
    - The loss of control over his private key, due to the compromise of the activation data (ie. PIN) or any other reason.
    - The inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
    - When there is a loss, alteration, unauthorized use, theft or compromise of the card.
- Communicate to the natural persons identified in the certificate the compliance of the specific obligations of them, and stablish mechanisms to guarantee the proper compliance of them.
- Not to monitor, manipulate or perform reverse engineer acts on the technical implantation of the certification services of UANATACA, without previous written permission.
- Not to compromise the safety of the certification services of the certification services provider of UANATACA, without prior written permission.

4.5.2.2. Civil liability of the certificate's subscriber

UANATACA contractually forces the subscriber to take responsibility to ensure:

- All the statements in the request are correct.
- All the information provided by the subscriber that is in the certificate is correct.
- The certificate is exclusively used for legal and authorized uses, in accordance with the Certification Practice Statement.
- No unauthorized person has ever had access to the private key of the certificate, and that he is the sole responsible for any damage caused by his infringement of protecting the private key
- The signer is an end entity and not a certification services provider, and won't use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification services provider title, nor any other case.

4.5.3. Use by the relying third party in certificates

4.5.3.1. Obligations of the relying third parties in certificates

UANATACA informs the relying third party in certificate of the following obligations he must assume:

- Consulting if the certificate is appropriate for the intending use, in an independient way.
- Verify the validity, suspension or revocation of the issued certificates, for which certificates status information will be used.
- Verify all certificates of the certificates hierarchy, before trusting the digital signature or any of the certificates of the hierarchy.
- Recognize that the verified electronic signatures, produced on a secure signature creation device (SSCD) have the legal consideration of recognized electronic signatures; that is, equivalent to handwritten signatures, as well as the certificate allows the creation of other types of electronic signatures and encryption mechanisms.
- Remember any limitation on the use of the certificate, regardless of whether in the own certificate or in the relying third party in certificates contract.
- Remember any caution established in a contract or other instrument, regardless of its legal nature.
- Not to monitor, manipulate or perform reverse engineer acts about the technical implementation of the certification services of UANATACA, without previous written permission.
- Not compromise the safety of the certification services of UANATACA, without previous written permission.

4.5.3.2. Civil liability of the relying third parties in certificates

UANATACA informs to the relying third party in certificates that he must assume the following responsibilities:

- He has enough information to make an informed decision in order to trust or not the certificate.
- He is the sole responsible of trusting or not of the information of the certificate.
- He will be the sole responsible if he breaches his obligations as a third party that trust the certificate.

4.6. Certificate renewal

The certificates renewal requires the renewal of keys, so that must comply with the established in section **Error! Reference source not found.**.

4.7. Key and certificate renewal

4.7.1. Circumstances for certificate and key renewal

The existing certificates can be renewed through a specific and simplified procedure of request, in order to keep the continuity of the certification service.

4.7.2. Legitimation to apply for renewal

Prior to the issuance and delivery of a renewed certificate, there must be a renewal application for a certificate, which can occur automatically or at the request of an interested party.

Likewise, an authorization of the subscriber is considered so the applicant can proceed with the request, which is legally implemented by a sheet of renewal of certificates subscribed by the Company, entity or organization.

4.7.3. Procedure for renewal request

4.7.3.1. Execution of the request

UANATACA receives certificates requests, carried out by the entities, companies or organizations of public or private law.

There is a document, either on paper or in electronic form, concerning the certificates renewal request, performed by the entity, company or organization of public or private law, that will include the data of the persons to which the certificates will be issued.

The request must indicate that the data of the certificates hasn't changed. Physical address or other data that could let contact the natural person identified in the certificate are the only changes that could be made.

4.7.3.2. Implementation of identification and authentication functions

Once UANATACA has received the certificate renewal request, will ensure that the certificate requests are complete, appropriate and duly authorized, before processing them.

4.7.3.3. Approval or rejection of the request

In case the data is correctly verified, UANATACA must approve the certificate renewal request and proceed with its issuance and delivery.

UANATACA notifies the approval or rejection of the request to the applicant.

UANATACA will be able to automate the procedures of verification of the information correction that will be in the certificate, and the approval of the requests.

4.7.3.4. Deadline for resolving the request

UANATACA responds to the requests of certificates renewal in order of arrival, in a reasonable term prior to the expiration of the certificates to revoke. A guarantee for the maximum time for renewal could be specified in the certificate issuance agreement.
Renewal requests remain active until its approval or rejection.

4.7.4. Notification of the renewed certificate issuance

UANATACA notifies the certificate issuance to the subscriber and the natural person identified in the certificate.

4.7.5. Conduct which institutes acceptance of the certificate

The acceptance of the certificate by the natural person identified in the certificate occurs when signing, either handwritten or electronic signature, the delivery or acceptance sheet before the responsible of the certification of the entity, Company or organization of public or private law.

4.7.6. Publication of the certificate

UANATACA publishes the renewed certificate in the Deposit to which refers in the section 2.1, with the relevant safety controls.

4.7.7. Notification of certificate issuance to third parties

UANATACA doesn't make any notification of the issuance to third entities.

4.8. Certificate modification

The modification of certificates, except the modification of the certified public key, which is considered renewal, will be treated as a new issue of certificate applied as described in sections 4.1, 4.2, 4.3 and 4.4.

4.9. Revocation and suspension of certificates

4.9.1. Causes of certificate revocation

UANATACA revokes a certificate when any of the following causes occur:

1) Circumstances affecting the information contained in the certificate:
   a) Modification of any of the data contained in the certificate, after the corresponding issue of the certificate including amendments.
   b) Discovery that any of the data contained in the certificate application is incorrect.
   c) Discovery that any of the data contained in the certificate is incorrect.

2) Circumstances affecting the security of the key or certificate:
   a) Compromise of the private key, infrastructure or systems certification service provider that issued the certificate, provided that it affects the reliability of the certificates issued from that incident.
   b) Infringement, by UANATACA, of the requirements of the certificate management procedures established in this Certification Practice Statement.
   c) Commitment or suspected compromise of the security key or certificate issued.
   d) Unauthorized access or use, by a third party private key corresponding to the public key contained in the certificate.
   e) Irregular use of the certificate by the natural person identified in the certificate or lack of diligence in the custody of the private key.
3) Circumstances affecting the subscriber or the natural person identified in the certificate:
   a) Completion of the legal relationship between UANATACA provision of services and the subscriber.
   b) Modification or termination of the underlying legal relationship or what caused the issuance of the certificate to the natural person identified in the certificate.
   c) Infringement by the certificate applicant of the preset requirements for the application thereof.
   d) Violation by the subscriber or by the person identified in the certificate, of their obligations, responsibility and guarantees established in the relevant legal document.
   e) Incapacity or death of key owner.
   f) The termination of the legal certificate underwriter _ and authorization to the holder by the subscriber key or termination of the relationship between subscriber and identified in the certificate.
   g) Request by the subscriber for certificate revocation in accordance with the provisions of section 3.4.
4) Other Circumstances:
   a) a) Termination of Certification Service Certification Entity UANATACA accordance with the provisions of section 5.8.
   b) b) The use of the certificate that is harmful and continued to UANATACA. In this case, it is considered that a use is harmful in terms of the following criteria:

- The nature and number of complaints received.
- The identity of the entities filing complaints.
- The relevant legislation in force at all times.
- The response of the subscriber or of the person identified in the certificate to complaints received.

4.9.2. Standing to request revocation

A certification revocation may be requested by:

- The identified person in the certificate.
- The subscriber of the certificate by the responsible of the certification service.

4.9.3. Request procedures for revocation

The entity required to revoke a certificate must apply to UANATACA. The revocation request shall include the following information:

- Date of application for the revocation.
- Identity of the Subscriber.
- Detailed reason for a revocation request.
- Name and title of the person requesting the revocation.
- Contact information for the person requesting the revocation.

The application must be authenticated by UANATACA, in accordance with the requirements of section 3.4 of this policy, prior to the revocation.

The revocation service can be found in the UANATACA website at: https://www.uanataca.com

If the recipient of a request for revocation by a natural person identified in the certificate is outside the subscribing entity, once authenticated the application must submit a request to that effect to UANATACA.

The revocation request will be processed upon receipt, and inform the subscriber and, where appropriate, physical person identified in the certificate about the change of status revoked certificate.

UANATACA may not reactivate the certificate once it has been revoked.

Both management service revocations as consultation service are considered critical services and thus contained in the Plan contingency and business continuity planning of UANATACA.

4.9.4. Temporary revocation application

Revocation requests shall be sent immediately when knowledge of the cause of revocation is known.

4.9.5. Temporary period of application processing

The revocation will occur immediately when received, within the regular hours of operation UANATACA.

4.9.6. Obligation to consult certificate revocation information

Third parties should check the status of those certificates in which they wish to rely.

A method by which you can check the certificate status is by consulting the List of Revoked Certificates latest issued by the Certification of UANATACA.

The Certificate Revocation Lists are published in the Deposit of the Certification, as well as the following web addresses indicated in certificates:

- http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
- http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

The status of the certificate validity can also be checked by the OCSP protocol.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.9.7. Frequency of issuance of certificate revocation lists (CRLs)

UANATACA issues an LRC at least every 24 hours.

The LRC indicates the scheduled time of issuance of a new LRC, although it may issue an LRC before the deadline stated in the previous LRC, to reflect revocations.

The LRC is obliged to maintain the revoked or suspended certificate until it expires.

4.9.8. Maximum period of publication of CRLs

The CRLs are published in the deposit within a reasonable period immediately after their generation, which in any case is no more than a few minutes.

4.9.9. Availability of online check certificate status

Alternatively, parties who rely on certificates may consult UANATACA deposit certificates, which is available 24 hours 7 days a week on the web:

- https://www.uanataca.com/public/pki/crtlist

To check the latest CRL issued in each CA, the following may be downloaded:

- *CA ROOT:*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *CA INTERMEDIA:*
  - *http://crl1.*uanataca.com/public/pki/crl/CA1subordinada.crl
  - http://crl2.uanataca.*com/public/pki/crl/CA1subordinada.crl*

In case of failure of systems checking certificate status for reasons beyond the control of UANATACA, it must make its best efforts to ensure that this service remains inactive for the minimum possible time, which may not exceed one day.

UANATACA provides information to third parties who rely on certificates on the operation of the service certificate status information.

4.9.10. Obligation to check the consultation certificate status service

It is mandatory to check the status of certificates before relying on them.

4.9.11. Other forms of certificate revocation information

UANATACA also reports the revocation status of certificates by the OCSP protocol, which allows the status of validity of the certificates online from these web addresses:

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.9.12. Special requirements in case of compromiso of the private key

The compromise of the private key UANATACA is notified to all participants in certification services, as far as possible, by posting this in the website UANATACA and, if deemed necessary, in other media, even on paper.

4.9.13. Reasons for suspension of certificates

UANATACA certificates may be suspended from the following causes:

- When so requested by the subscriber or the person identified in the certificate.
- When the documentation required in the request for revocation is sufficient but can not reasonably identify the subscriber or the person identified in the certificate.

- When the documentation required in the request for revocation is not sufficient, although it can reasonably identify the subscriber or the person identified in the certificate.
- When the required documentation in the request for revocation is not sufficient and not allow reasonably identify the undersigned or the person identified in the certificate.
- The lack of use of the certificate for an extended period of time, previously known
- If the key is suspected to have been compromised until it is confirmed. In this case, UANATACA will have to make sure that the certificate is not suspended for longer than necessary to confirm their commitment.

4.9.14. Suspension request

The certificate may be requested to be suspended by:

- The natural person identified in the certificate.
- The subscriber of the certificate, through authorized representatives.

4.9.15. Procedures for suspension request

The procedure consists of the following:

- The user accesses a web form found on the website of UANATACA.
- Once the form is filled with your number DNI / NIE a temporary password is sent by email, with which the user requested the certificate.
- The user must use this password to confirm the suspension request.
- Once the request is confirmed, UANATACA will proceed with the certificate suspension

The subscriber and the physical person identified in the certificate are informed about the changing state of the suspended certificate.

4.9.16. Maximum period of suspension

The maximum suspension will last for one week.

4.10. Completion of the subscription

After the period of validity of the certificate, the service subscription ends.

As an exception, the subscriber can maintain the existing service, requesting certificate renewal, in time determined by this Certification Practice Statement.

UANATACA can officially issue a new certificate, while subscribers maintain that state.

4.11. Services of certificate status checking

4.11.1. Operational characteristics of services

Services certificate status checking are provided through a web interface consultation, found here: https://www.uanataca.com

4.11.2. Availability of services

Services certificate status checking are available 24 hours a day, 7 days a week, throughout the year, except for scheduled breaks.

4.12. Deposit and recovery of keys

4.12.1. Policies and practices of deposit and key recovery

UANATACA does not provide deposit services and key recovery.

4.12.2. Policy and practices of encapsulation and recovery of key session

No stipulation.

5. Physical security controls, management and operations

5.1. Physical security controls

UANATACA has established physical and environmental security controls to protect the resources of the facilities where the systems, the systems themselves and the equipment used for operations of registration and approval of applications, technical generation of certificates and cryptographic hardware management.

Specifically, the security policy applicable to physical and environmental services certificate generation, cryptographic devices and revocation management has established requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Protective measures against fires.
- Failure of the support systems (electronic energy, telecommunications, etc.)
- Collapse of the building.
- Flooding.
- Antitheft protection.
- Unauthorized removal of equipment, information, media and applications relating to components used for the services of the service provider certification.

These measures are applicable to installations where the certificates are produced under the full responsibility of UANATACA, which lends from its both mainstream and, where appropriate, operating in contingency high security installations that are properly audited periodically.
Facilities include preventive and corrective maintenance systems with assistance 24/7 all year round with assistance in the following 24 hours notice.

5.1.1. Location and construction of facilities

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and strength of building materials facility ensures adequate levels of

protection against intrusion by brute force and located in an area of low risk of disasters and allows quick access.

The room where the cryptographic operations are performed in the Data Processing Center:

- It has redundancy in its infrastructure.
- It has several alternative sources of power and cooling in an emergency.
- Maintenance operations do not require that the Center is offline at any time.
- Availability of 99.99%.

UANATACA has facilities to physically protect the provision of services approval of applications for certificates and revocation management, compromise caused by unauthorized access to systems or data access and disclosure thereof.

5.1.2. Physical access

UANATACA has three levels of physical security (building entrance where the CPD is found, access to the room of the CPD and access to the RAC) for service of protecting the certificate generation, and must be accessed from the lower to the upper levels.

Physical access to the premises of UANATACA, where certification is processed, is limited and protected by a combination of physical and procedural measures are carried out as such:

- Limited to expressly authorized persons, with identification at the time of access and registration thereof, including filming by CCTV.
- Access to the rooms is done with ID card readers and managed by a computer system that keeps a log of inputs and outputs automatically.
- To access the rack where the cryptographic processes are located, prior authorization from UANATACA administrators hosting service is necessary to have the key to open the cage.

5.1.3. Electrical power and air conditioning

UANATACA facilities have current-stabilizing equipment and power system doubled with generator equipment.

The rooms housing IT equipment have temperature control systems with air conditioners.

5.1.4. Exposure to water

The facilities are located in an area of low risk of flooding.

The rooms where computers are housed have a moisture detection system.

5.1.5. Fire prevention and protection

The facilities and assets of UANATACA have automatic detection and firefighting systems.

5.1.6. Backup Storage

Only authorized individuals have Access to support storage.

The most highly-classified information is stored in a safe offsite Data Processing Centre.

5.1.7. Waste Management

The elimination of media, both paper and magnetic, is made by mechanisms that guarantee the impossibility of retrieving information.

In the case of magnetic media, it proceeds to formatting, permanent deletion, or physical destruction of the support, using specialized software to perform a minimum of 3 passes for erasing and variable data-erasing patterns.

For paper documents, paper shredders or specially-arranged bins for later destruction are used, under supervision.

5.1.8. Offsite backup

UANATACA uses a secure external storage for the safekeeping of documents, magnetic and electronic devices that are independent of the operations center.

At least two expressly authorized persons are required for the Access, deposit or withdrawal of devices.

5.2. Procedure controls

UANATACA guarantees that its systems are operated safely, for which it has establish and implemented procedures for the functions which affect the supply of its services.

The staff of UANATACA runs the administrative and management procedures according to the security policy procedures.

5.2.1. Reliable features

UANATACA has identified, according with its security policy, the following reliable functions and roles

- **Internal Auditor:** • Internal Auditor: Responsible for compliance with operating procedures. This is an external person to the Department of Information Systems. The tasks of Internal Auditor are incompatible in time with tasks and incompatible with Certification Systems. These functions will be subordinate to the head of operations, reporting both this technical direction.
- **System Administrator**: Responsible for the proper functioning of hardware and software support platform certification
- **Certification Authority Administrator**: Responsible for the actions to be executed with the cryptographic material, or performing any function involving the activation of private keys of certification authorities described in this document, or any of its elements.
- **Certification Authority Operator:** Necessary to be responsible, in conjunction with CA Manager, of the custody of material activation of cryptographic keys, and responsibility for backup operations and maintenance of AC.
- **Register Administrator:** Person responsible for approving the certification requests made by the subscriber.
- **Security Manager**: Responsible for coordinating, monitoring and enforcing security measures as defined by the security policies of UANATACA. This

individual should be responsible for aspects related to information security: logic, physics, networking, organization, etc.

Persons holding previous posts are subject to procedures of investigation and specific control.

5.2.2. Number of individuals per task

UANATACA guarantees at least two people to perform tasks that are stated in the Certification Policies corresponding, especially in handling the device custody of the keys of the Authority root and intermediate certification.

5.2.3. Identification and authentication for each role

The individuals assigned for each role are identified by the internal auditor will ensure that each person performs the operations for which they are assigned.

Each person only controls the assets required for its role, ensuring that no person access unallocated resources.

Access to resources is performed depending on the asset through cryptographic cards and activation codes.

5.2.4. Roles requiring separation of tasks

The following tasks are performed by at least two people:

- Issuance and revocation of certificates, and Access to the deposit.
- Generation, transmission and destruction of certificates by the Certification Entity.
- The start of production by the Certification Entity.

5.2.5. PKI management system

The PKI system is composed of the following modules:

- Component/module for Subordinate Certificate Authority management.

- Component/module for Registration Authority management.
- Component/module for solicitation management
- Component/module for key management (HSM)
- Component/module for databases
- Component/module for CRL management.
- Component/module for OCSP service management.

5.3. Personnel controls

5.3.1. History, qualification, experience and authorization requirements

All qualified personnel performing tasks as reliable have taken at least a year working on the production site and have fixed labor contracts.

All staff is qualified and has been properly instructed to perform operations that they have been assigned.

Staff in positions of trust has no personal interests that conflict with the development of the role that has been entrusted.

UANATACA ensures that personnel record is reliable for registration tasks.

Registration Manager has completed a course of preparation for the tasks of validation requests.

In general, UANATACA withdraws an employee from their duties when knowledge of the existence of the commission of any criminal act that could affect the performance of its functions it has.

UANATACA does not assign to a reliable site management a person who is not suitable for the position, especially for having been convicted of a crime or minor affecting their suitability for the position. For this reason a previous investigation, to the extent permitted by applicable law, on the following is done:

- Studies, including alleged degree.

- Previous work up to five years, including professional references and a check that the alleged work was actually performed.
- Delinquency.

5.3.2. Procedures of history investigation

UANATACA, before hiring a person or before that person has access to the job, performs the following checks:

- References of the past years jobs
- Professional references
- Studies, including qualifications

UANATACA obtains the unequivocal consent of the affected to such previous research, and processes and protects all his personal data in accordance with the Personal Data Protection Organic Law 15/1999, of December 13th, and the Royal Decree 1720/2007, of December 21st, by which it is approved the development Regulation of the Organic Law 15/1999, of December 13th, of Personal Data Protection.

The research will be repeated with enough frequency.

All checks are made up to be allowed by the applicable law. The reasons that may lead the candidate rejection of a job are the followings:

- Falsehoods on the job application, done by the candidate.
- Very negative professional references or not very reliable.

The need to undergo a preliminary investigation is reported on the application job, being notified that the refusal to submit to the investigation will imply the application rejection.

5.3.3. Training requirements

UANATACA trains the staff in reliable and management jobs, until they reach the required qualification, keeping reports of the training.

Training programs are updated and improved periodically.

Training includes, at least, the following contents:

- Principles and mechanisms of security of the certification hierarchy, and the user environment of the person to train.
- Tasks the person must do.
- Policies and security procedures of UANATACA. Use and operation of machinery and installed applications.
- Management and processing of incidents and security commitments.
- Procedures of business continuity and emergency.
- Process management and security regarding the processing of personal data.

5.3.4. Retraining frequency and requirements

UANATACA updates the staff training in accordance with the needs, and with enough frequency to comply their functions in a competent and satisfactory way, especially when doing the substancial modifications in the certification tasks.

5.3.5. Job rotation frequency and sequence

Not applicable.

5.3.6. Sanctions and unauthorized actions

UANATACA has a disciplinary system, to debug the responsibilities arising from unauthorized actions, appropriate to the applicable labor legislation and, in particular, coordinated with the disciplinary system of the collective agreement that is applicable to the staff.

Disciplinary actions include suspension and loss of employment of the person responsible for the harmful action, proportionate to the gravity of the unauthorized action.

5.3.7. Professionals contracting requirements

The staff hired to perform reliable tasks sign a previous confidentially agreement and the operational requirements used by UANATACA. Any action that may compromise the

security of the accepted processes could, once evaluated, lead to the termination of the employment contract.

In case all or part of the certification services were performed by a third party, the previsions and controls performed in this section, or other parts of the Certification Practice Statement, will be applied and complied by the third party who performs the operation functions of the certification services, notwithstanding, the certification authority will be responsible in any case for the effective implementation. These aspects are concretized in the legal instrument used to arrange the certification services provision by a third party different tan UANATACA.

5.3.8. Documentation supplied to personnel

The certification services provider will provide the documentation strictly needed by the staff at any moment, to perform their job in a competent and satisfactory form.

5.4. Security audit procedures

5.4.1. Types of recorded events

UANATACA produces and safely register, at least, of the following events related to the entity security:

- Booting and shutting down of systems.
- Attempts to create, delete, set passwords or change privileges.
- Attempts to login and logout.
- Unauthorized attempts to enter the CA network.
- Unauthorized attempts to access system files.
- Physical access to logs.
- System configuration maintenance and changes.
- Records of the CA applications.
- Booting and shutting down of CA application.
- Changes of the CA and/or keys details.
- Changes in certificate issuing policies.
- Generation of own keys.

- Creation and revocation of certificates.
- Records of destruction of materials containing key information, activation data or personal information.
- Events related to the certificate's lifecycle of the cryptographic module, as lobby, use and uninstallation of it.
- Generation keys ceremony and keys management databases.
- Physical access records.
- System configuration maintenance and changes.
- Staff changes.
- Informes de compromisos y discrepancias.
- Records of destruction of materials containing key information, activation data or personal information of the subscriber, in case of individuals certificates, or the natural person identified in the certificate, in case of organization certificates.
- Possession of activation information for operations with the private key of the certification Authority.
- Complete reports of the physical intrusion attempts in the infrastructures that support the certificates issuance and management.

Log entries include the following elements:

- Login date and time.
- Serial number or entry sequence, in the authomatic records.
- Identity of the entity entering in the register.
- Type of entrance.

5.4.2. Frequency of processing audit logs

UANATACA reviews its logs when a system alert motivated by the existence of any incident occurs.

Processing audit logs is a review of the records including the verification that confirm they have not been tampered, a brief inspection of all log entries and a deeper investigation of any alert or irregularities in the logs. The actions from the audit review are documented.

UANATACA keeps a system that guarantees:

- Enough space for logs storage.
- Logs files are not rewritten.
- Information held includes, at least: type of event, date and time, user running the event and result of the operation.
- Logs files will be held in structured files susceptible to incorporate into a BBDD for further exploration.

5.4.3. Period of retention of audit logs

UANATACA holds the logs information for a period of between 1 to 15 years, depending on the type of information recorded.

5.4.4. Audit logs protection

The systems logs:

- Are protected from manipulation by signing the files that contain them.
- Are stored in fireproof devices.
- Availability is protected through its storage in facilities out of the center where the CA is located.

Access to logs files is reserved only to authorized persons. Also, devices are handled at all times by authorized personnel.

There is an internal procedure where management processes devices containing the data of the audit logs are detailed.

5.4.5. Audit log back-up procedures

UANATACA has a proper backup procedure so that, in case of loss or destruction of relevant files, were available in a short period of time the corresponding logs backup.

UANATACA has implemented a secure backup procedure of audit logs, making a copy of all logs weekly in an external source. Additionally a copy is held in a custody external center.

5.4.6. Location of the audit logs storage system

The information of the audit events is collected internally and in an automated way by the operating system, network communications and software certificate management, in addition to the data generated manually, will be stored by the authorized personnel. All this composes the storage system of audit logs.

5.4.7. Notification of the audit event to the subject that caused the event

When the log audit accumulation system records an event, it is not necessary to send a notification to the individual, organization, device or application that caused the event.

5.4.8. Vulnerabily analysis

Vulnerability analysis is covered by the audit processes of UANATACA.

Vulnerability analysis must be run, reviewed and revised by an examination of these monitored events. This analysis must be run daily, monthly and annually.

Audit data systems are stored in order to be used in the investigation of any incident and to locate vulnerabilities.

5.5. Information files

UANATACA guarantees that all information relating to the certificates is heldfor an appropriate period of time as established in section 5.5.2 of this policy.

5.5.1. Types of records archived

The following documents involved in the life-cycle of the certificate are stored by UANATACA (or registration authorities):

- All audit data system.
- All data relating to certificates, including contracts with the signers and the data relating to their certification and location.
- Requests of issuance and revocation of certificates.
- Type of document presented in the certificate request.
- Identity of the Registration Authority that accepts the certificate request.
- Unique identification number provided by the previous document.
- All certificates issued or published.
- CRLs issued or logs of the status of the generated certificates.
- The history of generated keys.
- Communications between the elements of the PKI.
- Policies and Practices Certification.
- All audit data identified in section 5.4.
- Information of requests certification.
- Documentation provided to justify the certification requests.
- Life-cycle certificate information.

UANATACA is responsible for the correct file of all this material.

5.5.2. Retention period for the file

UANATACA saves the mentioned logs above for at least 15 years.

5.5.3. Protection of the file

UANATACA protects the file so only the duly authorized persons can access to it. The file is protected against visualization, modification erased or any other manipulation through its storage in a reliable system.

UANATACA ensures proper protection of the files by assigning qualified personnel for its treatment and its storage in secure fireproof boxes and external facilities.

5.5.4. File backup procedures

UANATACA has an external storage center to ensure the availability of the file backups of electronic files. The physical documents are stored in safe places restricted to authorized personnel.

UANATACA, at least, makes incremental daily backups of support of all its electronic documents and makes weekly full backups for data recovery cases.

In addition, UANATACA (or the organizations that make the registration functions) keeps a copy of the paper documents in a safe place different from the own Certification Authority.

5.5.5. Requirements of time-stamping

Records are dated with a reilable source via NTP.

There is no need to sign this information digitally.

5.5.6. Location of the file system

UANATACA has a centralized system of gathering information of the activity of the equipment involved in the certificate management service

5.5.7. Procedures to obtain and verify file information

UANATACA has a procedure which describes the process to verify that the stored information is correct and reachable.

5.6. Keys renewal

The CA keys will be changed before the use of the private key expires. The former CA and its private key will only be used for signing CRLs while there are active certificates issued by that CA. A new CA will be generated with a new private key and a new DN.

The key change of the subscriber is done by a new issuing process.

5.7. Compromised key and recovery of disaster

5.7.1. Management procedures of incidents and commitments

The backup of the following information is stored in external installations, which are available in case of compromise or disaster: technical data of the certificates request, audit data and database records of all issued certificates.

The backup of UANATACA private key is generated and held in accordance with the established in section 6.2.4.

5.7.2. Resources, applications or data corruption

When resources, applications or data corruption events happen, the incidences will be communicated to security, and the proper management procedures will begin, which contemplate scaling, investigation and response to the incident. Procedures of commitment of the keys or disaster recovery of UANATACA will begin, if necessary.

5.7.3. Compromised private key of the entity

In case of suspicion or knowledge of the commitment of UANATACA, key commitment procedures will be activate, led by a response team to assess the situation and will develop an action plan , to be implemented under the approval of the Certification Authority management.

UANATACA has developed a contingency Plan to recover the critics systems, in an alternative data center if necessary.

In the contingency and business continuity process, the commitment of the key root must be taken as a separate case. This issue affects, in case of replacement of the keys, the recognition for different features and private and public services.
A recovery of the effectiveness of the keys in terms of business will mainly depend on the duration of these processes. The contingency and business continuity document will only with purely operative terms in order to make available the new keys, not its recognition by others.

Any failure from achieving the goals set by this contingency Plan, will be treated as reasonably unaviodable unless such failure is due to a breach of the obligations of the CA to implement those processes.

5.7.4. Business continuity capabilities after a disaster

UANATACA will restore critical services (suspension and revocation, and publication of the information of the certificates status) in accordance with the contingency and business continuity plan restoring the normal operation of the previous services within 24 hours of the disaster.

UANATACA has an alternative center for the operation of certification schemes described in the business continuity plan, if necessary.

5.8. Service termination

UANATACA ensures that potential disruptions to subscribers and third parties are minimal due to the cessation of the certified services provider and, specially, ensures a continuous maintenance of the records required to provide certified evidence for civil or criminal investigation, by transfer to a notary deposit.

Before the services cessation, UANATACA develops a termination plan, with the following provisions:

- To provide the necessary funds (by civil liability insurance) to continue the completion of revotation activities.
- To inform all Signers/Subscribers, Relying third parties and other CA's with which it has agreements or another type of relation of the cessation with a minimum of 6 months.
- To revoke any authorization to outsourced entities to act on behalf of the CA in the process of certificates issuance.
- To transfer its obligations regarding the maintenance of the registry information and logs for the period of time indicated to subscribers and users.
- To destroy or disable for use the private keys of the CA.
- To keep active the certificates and verification system to extinction and revocation of all certificates issued.
- To run all necessary tasks to transfer the maintenance obligations of registration information and the files of events log during the respective time periods indicated to the subscriber and relying third parties in certificates.

6. Technical security controls

UANATACA uses reliable systems and products, protected against any alteration and guarantee the technical and cryptographic security of the certification which are used as support.

6.1. Generation and installation of the pair of keys

6.1.1. Generation of the pair of keys

The pair of keys of the intermediate Certification Authority "UANATACA CA1 2016" is created by the certification authority root "UANATACA ROOT 2016" in accordance with the ceremony procedures of UANATACA, within the high security perimeter addressee to this area.

The activities performed during the keys generation ceremony have been registered, dated and signed for all the individuals participating in it, with the presence of an Auditor CISA. Such records are guarded to the effects of audit and follow-up during an appropriate period determined by UANATACA.

Devices with FIPS 140-2 level 3 certifications are used for the certification authorities root and intermediate key generation.

UANATACA ROOT 2016	**4.096 bits**	**25 years**
UANATACA CA1 2016	4.096 bits	12 years
- Final entity certificates	2.048 bits	3 years
UANATACA CA2 2016	4.096 bits	12 years
- Timestamping Unit certificates	2.048 bits	3 years

Further information in the following location of the PDS:

CERTIFICATE	URLs
Natural Person on SOFT	http://www.uanataca.com/public/pki/PDS-PFsoft-EN/
Natural Person on SSCD authentication	http://www.uanataca.com/public/pki/PDS-PFSSCD-EN/
Natural Person on SSCD signature	
Natural Person on SSCD encryption	
REPRESENTATIVE on SOFT	http://www.uanataca.com/public/pki/PDS-REPsoft-EN/
REPRESENTATIVE on SSCD identification	http://www.uanataca.com/public/pki/PDS-REPSSCD-EN/
REPRESENTATIVE on SSCD signature	
REPRESENTATIVE on SSCD encryption	
Electronic seal Medium level	http://www.uanataca.com/public/pki/PDS-SLmedio-EN/
Electronic seal High level	http://www.uanataca.com/public/pki/PDS-SLalto-EN/
Public Employee Medium level	http://www.uanataca.com/public/pki/PDS-EPmedio-EN/
Public Employee High level (identification)	http://www.uanataca.com/public/pki/PDS-EPalto-EN/
Public Employee High level (signature)	
Public Employee High level (encryption)	
Timestamping Unit	http://www.uanataca.com/public/pki/TSA-DS/

6.1.1.1. Generation of the signer pair of keys

The keys of the signer are created by himself through devices hardware or software authorized by UANATACA or can be created by UANATACA.

The keys are created using public key algorithm RSA, with a minimum length of 2048 bits.

6.1.2. Sending the private key to the signer

In certificates, the private key of the secure signature creation device is properly protected in it.

In the software certificate the private key of the signer is created in the computer system that this signer uses when requesting the certification so the sending of the private key does not exist.

6.1.3. Sending of the public key to the certificate issuer

The method of remission of the public key to the certification services provider is PKCS#10, other equivalent cryptographic test or any other method approved by UANATACA.

6.1.4. Public key distribution of the certification services provider

UANATACA's keys are communicated to third parties who trust in certificates, ensuring the integrity of the key and authenticating its origin, through its publication in the Deposit.

Users can access to the Deposit to obtain the public keys, and additionally, in applications S/MIME, the data message may contain a chain of certificates, which are distributed to the users in this way.

The certificate of the CA root and subordinated will be available on the UANATACA web page.

6.1.5. Key sizes

The length of the Certification Authority root keys is 4096 bits.

The length of the Certification Authority subordinated keys is 4096 bits.

The end entity certificates keys are 2048 bits.

6.1.6. Generation of public key parameters

The CA Root, CA subordinated and the subscriber certificates public key are encrypted in accordance with RFC 5280.

6.1.7. Quality check of the public key parameters

- Module Length= 4096
- Algorithm of keys generation: rsagen1
- Cryptographic functions of Summary: SHA256.

6.1.8. Key generation in IT applications or in equipment goods

All keys are generated in equipment goods, in accordance with the indicated in section 6.1.1.

6.1.9. Key usage purposes

Key usage for the CA certificates is exclusively for signing certificates and CRLs.

Key usage for the end entity is exclusively for the digital signature and non-repudiation.

6.2. Private key protection

6.2.1. Cryptographic modules standards

In relation to the modules that manage the keys of UANATACA and the subscribers of the electronic signature certificates, the required level by the standards indicated in the above sections is ensured.

6.2.2. Private key multi-person (n of m) control

A multi-person control is required for activating the private key of the AC. In case of this Certification Practice Statement, in detail there is a policy of 3 of 6 persons for the keys activation.

Cryptographic devices are physically protected, as determined in this document.

6.2.3. Private Key Deposit

UANATACA doesn't store copies of the private key of the signers.

6.2.4. Private Key Backup

UANATACA makes backup copy of the CA private key that makes their recovery in case of disaster, loss or deterioration thereof. Both generation of the copy and the recovery thereof need at least two people participation.

These recovery files are stored in fireproof cabinets and in the external custody center.

Subscriber keys in software can be stored for possible recovery in case of contingency, in an external storage separate from the key setup.

Signer keys in hardware can not be copied because they can not leave the cryptographic device.

6.2.5. Private Key Storage

The CA private keys are archived for a period of **10 years** after the issuance of the last certificate. They will be stored in secure fireproof files and in the external custody center. At least the collaboration of two people will be needed to recover the CA private key in the initial cryptographic device.

The subscriber can store the private key during the time he thinks appropriate, just in case of encrypted certificates. In this case UANATACA also keep a copy of the private key associated to the encrypted certificate.

6.2.6. Private Key transfer into a cryptographic module

Private keys are directly generated in the cryptographic modules of production of UANATACA.

6.2.7. Method of activating private key

The Certification Authority private keys are encrypted stored in the cryptographic modules of UANACATA production.

6.2.8. Method of deactivating private key

UANATACA private key is activated by the running of the corresponding safe boot procedure of the cryptographic module, by the indicated persons in section 6.2.2.

The CA keys are activated by a process m of n (3 of 6).

The activation of the private keys of the Intermediate CA is managed with the same process of m of n of the CA keys.

6.2.9. Method of destroying private key

For deactivation of UANATACA the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

The signer must introduce the PIN for the new activation.

6.2.10. Cryptographic modules clasification

Before destroying the keys, a revocation of the certificate of the public keys associated with them will be issued.

Devices that have stored any part of UANATACA private keys are physically destroyed or reset to low level. For disposal the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

Finally the bakcups will be destroyed in a safety way.

The signer keys in software may be destroyed by deleting them following the instructions of the application.

The signer keys in hardware may be destroyed by a special computer application at the offices of the RA or UANATACA.

6.2.11. Cryptographic modules clasification

See section 6.2.1

6.3. Other aspects of key pair management

6.3.1. Public key file

UANATACA archives its public keys routinely, according to the established in section 5.5 of this document.

6.3.2. Public and private key usage periods

Periods of use of the keys are determinated by the duration of the certificate, after which theY can not continue to be used.

As an exception, the private key of decryption can continue being used even after the expiration of the certificate.

6.4. Activation data

6.4.1. Activation data generation and installation

Activation data of the devices that protect UANATACA private keys are generated in accordance with the established in section 6.2.2 and key procedures ceremony.

The creation and distribution of such devices is recorded.

Likewise, UANATACA generates the activation data in a safe way.

6.4.2. Activation data protection

Activation data devices that protect the private keys of the Certification Authority root and subordinated, are protected by the holders of cards managers of the cryptographic modules, as stated in the document of the keys ceremony.

The certificate signer is responsable for protecting his private key, with a password as complete as possible. The signer must remember the password.

6.5. Computer security controls

UANATACA uses reliable systems to provide certification services. UANATACA has made controls and computer audits to establish its proper computer activity management with the level of security required in the system management of electronic certification.

Regarding the information security, UANATACA applies the certification scheme controls on management systems ISO 27001.
Used equipments are initially configured with appropriate security profiles of UANATACA staff system, in the following aspects:

- Setting up the operating system.
- Setting up the application security.
- Correct sizing of the system.
- User and permissions settings.
- Setting event Log.
- Backup and recovery plan.
- Antivirus settings.
- Requirements of network traffic.

6.5.1. Specific computer security technical requirements

Each UANATACA server includes the following functionalities:

- Access control of the SubCA services and privilege management.
- Imposition of separation of duties for managing privileges.
- Identification and authentication of roles associated to identities.

- Archive of the subscriber and SubCA history and audit data.
- Audit events related to security.
- Self-diagnosis of safety related with the SubCA services.
- Recovery mechanisms of keys and SubCA system.

The exposed functionalities are performed through a combination of operating system, PKI software, physical protection and procedures.

6.5.2. Computer security rating

The CA and RA applications used by UANATACA are reliabale.

6.6. Life cycle technical controls

6.6.1. System development controls

The applications are developed and implemented by UANATACA in accordance with the development and change control standards.

The applications have methods for verifying the integrity and authenticity, as well as the correction of the version to use.

6.6.2. Life cycle security controls

UANATACA develops the precise activities for training and employee awareness of security. The materials used for training and descriptive documents processes are updates after approval by a group for security management. An anual training plan is used.

UANATACA requires by contract security measures equivalent to any external provider involved in the certification tasks.

6.6.2.1. Clasification and management of information and goods

UANATACA supports an inventory of assets and documentation and a procedure for the management of this material to guarantee its use.

UANATACA security policy details the procedures of information management where it is classified according to its level of confidentiality.

The documents are classified into three levels: UNCLASSIFIED, INTERNAL USE and CONFIDENTIAL.

6.6.2.2. Management operations

UANATACA has an appropriate process management and incident response, by implementing an early warning system and the generation of periodic reports.

In UANATACA security document the incident management process is developed in detail.

UANATACA has documented all the procedure relative to the roles and responsibilities of the staff involved in the control and manipulation of elements contained in the certification process.

6.6.2.3. Treatment of supports and safety

All supports are treated safely in accordance with the requirements of the classification of information. The supports that contain sensitive information are destroyed safely if they will not be required again.

Planning system

UANATACA Systems department keeps track of the capabilities of the equipment. In conjuction with the implementation of resources control each system can provide a possible downsizing.

Reports of incidents and response

UANATACA has a procedure for the follow-up of incidents and its resolution where the answers and an economic evaluation are registered which supposes the resolution of the incident.

Operational procedures and responsibilities

UANATACA defines activities assigned to persons with a role of trust, other than those responsible for performing daily operations that do not have charater of confidentiality.

6.6.2.4. Access system management

UANATACA makes all efforts that are reasonable available to confirm that the system access is limited to authorized persons.

Particularly:

CA general

- Controls based on firewalls, antivirus and IDS high availability are available.
- Sensitive data is protected by cryptografic techniques or controls with strong identification.
- UANATACA has a documented procedure for managing the users' authorizations and cancellations and access policy, detailed in its policy of security.
- UANATACA has procedures to ensure that operations are performed in accordance with policy roles.
- Each person has associated a role to perform the certification operations.
- UANATACA staff is responsible for its actions by the confidentiality agreement signed with the Company.

Certificate generation

Authentication for Issuance process is performed through a system of m of n operators for activating UANATACA private key.

Revocation management

Revocation will be performed by strong authentication to the applications of an authorized administrator. Logs systems will generate the tests that guarantee non-repudiation of the action taken by UANATACA administrator.

Revocation status

The application for the status of the revocation offers access control based on the authentication with certificates or dual factor identification to avoid the attempt to change of the status information of the revocation.

6.6.2.5. Life cycle management of cryptographic hardware

UANATACA ensures that the cryptographic hardware used for signing certificates is not handled during its transport by inspecting the delivered material.

The cryptographic harware moves on prepared supports to prevent any manipulation.

UANATACA records all relevant device information to add to the catalog of assets.

The use of the cryptographic hardware of signature certificates requires the use of at least two trusted employees.

UANATACA makes periodic tests to ensure the correct functioning of the device.

The cryptographic hardware device is manipulated only by reliable personnel.

UANATACA signature private key stored in the cryptographic hardware will be erased once the device is removed.

UANATACA system configuration, and its modifications and updates are documented and controlled.

UANATACA has a contract of maintenance of the device. Changes or updates are authorized by the security officer and are reflected in the corresponding team's working minutes. These settings are performed at least by two realiable persons.

6.7. Network security controls

UANATACA protects the physical access to network management devices, and has an architecture that directs the traffic generated based on its features of security, creating clearly defined network sections. This division is performed with firewalls.
Confidential information is transferred through unsecured networks, is performed in an encrypted way using SSL protocols or VPN system with dual factor authentication.

6.8. Engineering controls of cryptographic modules

Cryptographic modules are subjected to engineering controls provided in the standards indicated along this section.

The key generation algorithms used are commonly accepted for the use of the key to which they are intended.

All cryptographic operations of UANATACA are performed in modules with FIPS 140-2 level 3 certification.

6.9. Time sources

UANATACA has a procedure of time synchronization coordinated via NTP.

7. Certificates profiles and CRLs

7.1. Certificate profile

All recognized certificates issued under this policy comply the X.509 standard version 3, RFC 3739 and ETSI 101 862 “Qualified Certificate Profile”.

7.1.1. Version number

UANATACA issues certificates X.509 Version 3

7.1.2. Certificate extensions

Certificates extensions are detailed in the profiles documents which are reachable from the web (https://www.uanataca.com).

Thus it is allowed to keep more stable versions of the Certification Practice Statement and decouple from the frequent profiles ajustments.

7.1.3. Object identifier (OID) of the algorithms

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Names format

Certificates must contain the requiered information for its use, as determined by the appropriate policy.

7.1.5. Names restriction

Names contained in the certificates are restringed as “Distinguished Names” X.500, which are unique and not ambiguous.

7.1.6. Object identifier (OID) of the certificates types

All certificates include an identifier of the certificates policy under which have been issued, in accordance with the indicated structure in point **Error! Reference source not found.**.

7.2. CRL profile

7.2.1. Version number

CRLs issued by UANATACA are from version 2.

7.2.2. OCSP profile

In accordance with the standard IETF RFC 6960.

8. Compliance audit

UANATACA has communicated the beginning of its activity as certification services provider by the Ministry of Industry and subject to control the checks that the organism deems necessary.

8.1. Frequency of compliance audit

UANATACA conducts a compliance audit annually, plus internal audits carried out at its own discretion or at any time due to a suspected breach of any security measure.

8.2. Identification and qualification of the auditor

The audits are performed by an external independent audit signature that demonstrate technical competence and experience in computer security, security of information systems and compliance audits of public key certification services, and related elements.

8.3. Auditor relationship to audited entity

Audit firms are renowned, with specialized departments, in conducting IT audits, so there is no confilct of interest that could undermine its performance in relation to UANATACA.

8.4. Topics covered by audit

The audit checks regarding UANATACA:

a) That the entity has a managemet system which ensures the quality of service.
b) That the entity complies with the requirements of the Certification Practice Statement and other documentation related to the issuance of the various digital certificates.
c) That the Certification Practice Statement and other related legal documentation comply with the agreed with UANATACA and the established in the current regulation.

d) That the entity properly manages its information systems.

Specially, the auditing object elements are as follows:

a) CA, RA's and related elements processes.
b) Information systems.
c) Protection of the data processing center.
d) Documents.

8.5. Actions taken as a result of deficiency

Once an auditor's compliance report has been completed and received by the direction, the deficiences found, with the audit signature, are analyzed and develops and implements the corrective policies that tackle these deficiences.

If UANATACA is unable to develop and/or implement the corrective measures or if the deficiencies found suppose an immediate threat to the system security or integrity, shall immediately inform to the Security Committee of UANATACA which can perform the following actions:

- Cease operation temporarily.
- Revoke the CA key and regenerate the infrastructure.
- Terminate the CA service.
- Other complementary actions needed.

8.6. Treatment of audit reports

Audit reports results are delivered to the Security Committee of UANATACA within a maximum period of 15 days after completion of the audit.

9. Business and legal requirements

9.1. Fees

9.1.1. Certificate issuance or renewal fees

UANATACA can establish a certificate issuance or renewal fee, which, if any, will be reported to the subscribers.

9.1.2. Certificate access fees

UANATACA hasn't established any fee for certificates access.

9.1.3. Status information access fees

UANATACA hasn't established any fee for certificates status information access.

9.1.4. Fees for other services

Not stipulated.

9.1.5. Refund policy

Not stipulated.

9.2. Finantial capacity

UANATACA has enough economic resources to keep its operations, to comply with its obligations and to confront the risk of liability for claim and damages, as established in ETSI EN 319 401-1 7.12 c), in relation to the management of the services finalization and termination plan.

9.2.1. Insurance coverage

UANATACA has a warranty coverage of its civil liability, with an insurance of professional civil liability that complies with Article 20.2 of electronic signature Law 59/2003, December 19th, with the minimum insured of euros 3.000.000.

9.2.2. Other assets

Not stipulated.

9.2.3. Insurance coverage for subscribers and relying third parties in certificates

UANATACA has a warranty coverage of its civil liability, with an insurance of professional civil liability that complies with Article 20.2 of electronic signature Law 59/2003, December 19th, with the minimum insured of euros 3.000.000.

9.3. Confidentiality

9.3.1. Confidential information

UANATACA holds the following information:

- Certificates request, approved or rejected, and all other personal information obtained for issuing and keeping the certificates, except the information indicated in the next section.
- Private keys generated and/or stored by the certification services provider.
- Internal and external transactions records, created and/or kept by the Certification Authority and its auditors.
- Policy and security plans.
- Documentation of operations, file, monitorization and other similars.
- All other information identified as “Confidential”.

9.3.2. Non-confidential information

The following information is considered non-confidential:

- Certificates issued or pending issuance.

- Binding the subscriber to a certificate issued by the Certification Authority.
- Name and surnames of the person identified on the certificate, as well as any other circumstance or personal data of the holder, in case it is significant depending on the certificate finality.
- Email of the person identified on the certificate, or the email assigned to the subscriber, in case it is significant depending on the certificate finality.
- Uses and economic limitis outlined in the certificate.
- The validity period, the issuance date and the expiration date of the certificate.
- Serial number of the certificate.
- The different status or conditions of the certificate and the date of beginning of each of them, specifically: pending generation and/or delivery, valid, revoked, suspended or expired and the reason that caused the change of status.
- The Certificate Revocation Lists (CRLs), and the remaining revocation status information.
- The information contained in the certificates deposits.
- Any other information not indicated in the previous section.

9.3.3. Disclosure of suspension and revocation

See the previous section.

9.3.4. Legal disclosure of information

UANATACA only discloses the confidential information in the cases legally foreseen.

Specifically, records that support the reliability of the data contained in the certificate will be disclosed if required to prove the evidence of the certification in legal proceedings even without the consent of the certificate subscriber.

UANATACA will indicate these circumstances in the privacy policy under section 9.4.

9.3.5. Disclosure on request of the owner

UANATACA includes in the privacy policy under Section 9.4, requirements to allow the disclosure of subscriber information and, where appropriate, of the natural person identified on the certificate directly, to them or to third parties.

9.3.6. Other information disclosure circumstances

Not estipulated.

9.4. Personal data protection

UANATACA binds to comply with the regulation on protection of personal data, with appropriate security measures as listed in the Protection of Personal Data Organic Law 15/1999, and Royal Decree 1720/2007 of development of that Law.

UANATACA obtains the personal data contained in the files by data capture by the SUBSCRIBER, that must legally obtained from who correponds, as provided in the regulations on electronic signature and protection of personal data.

UANATACA has the status of processor while the purpose, content and use of the processing of personal data is not decided, while the SUBSCRIBER is responsable for the file.

UANATACA uses the data contained in its files, solely for the purposes set out in this Certification Practice Statement.

Also, UANATACA has developed a privacy policy, according to Protection of Personal Data Law 15/1999, of December 13th, and documented in this Certification Practice Statement the aspects and procedures of security corresponding to the security document in accordance with the provisions of Article 19.3 of electronic law 59/2003, of December 19th, and Articles 82 and 88 of Royal Decree 1720/2007, od December 21st, by which approves the Regulation of development of the Organic Law 15/1999, of December 13th of 1999, on the personal data protection. This Certification Practice Statement is therefore considering the document of security.

UANATACA does not disclose or lease personal data, except in cases provided in sections 9.3.2 to 9.3.6, and in section 5.8, in case of termination of the certification service.

Confidential information in accordance with the regulations on personal data protection is protected from loss, destruction, damage, forgery and ilegal or unauthorized processing in accordance with the requirements established in this document, that comply with the obligations established in Royal Decree 1720/2007, of December 21st, by which the Regulation of development of the Organic Law 15/1999, of December 13th of 1999, on the personal data protection is approved.

9.5. Intellectual property rights

9.5.1. Property of certificates and revocation information

UANATACA is the only one that has intellectual property rights on the certificates that issues, without any prejudice of the rights of the subscribers, key holders and third parties, to which it grants non exclusive license to reproduce and distribute certificates, free of charge, as long as the reproduction is full and does not alter any element of the certificate, and is necessary in relation with digital signatures and/or encryption systems within the scope of the certificate use, and according to the documentation that links them.

In addition, certificates issued by UANATACA have a legal notice concerning the ownership thereof.

The same rules are applicable to the use of the information of certificates revocation.

9.5.2. Property of the Certification Practice Statement

UANATACA is the only one that has intellectual property rights of this Certification Practice Statement.

9.5.3. Property of information relating to names

The subscriber and, where appropriate, the natural person identified on the certificate, preserves all rights on the brand, product or name on the certificate.

The subscriber owns the distinguished name of the certificate, consisting of the information specified in section 3.1.1.

9.5.4. Property of keys

Key peirs are owned by subscribers of certificates.

When a key is divided in parts, all parts of the key are property of the owner of the key.

9.6. Obligations and civil liability

9.6.1. UANATACA obligations

UANATACA guarantees, under full responsibility, that complies all requirements established in the Certification Practice Statement, being the sole responsable for compliance with the procedures described, even if part or all operations are externally outsourced.

UANATACA provides certification services in accordance with this Certification Practice Statement.

Previous issuance and delivery of the certificate to the subscriber, UANATACA informs the subscriber of the terms and conditions related to the use, price and limitations of use of the certificate, by a subscriber contract incorporating by reference the disclosure texts (PDS) of each of the certificates acquired.

The disclosure text document, also known as PDS[5], meets the contwnt of Annex A of ETSI EN 319 411-1 v1.1.1 (2016-02), document that can be transmitted by electronic media, using a durable in time communication media, and in an understandable language.

UANATACA binds subscribers, key holders and relying third parties in certificates by the disclosure text or PDS, in written and understandable language, with the minimum following contents:

- Requirements to comply with the provisions of sections **Error! Reference source not found.**, 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 y **Error! Reference source not found.**.
- Indication of the applicable policy, indicating that the certificates are not issued to the public.
- Manisfest that the information contained in the certificate is accurate, unless notification against by the subscriber.
- Consent for the publication of the certificate in the deposit and third party access to it.
- Consent for storing information used for the subscriber registration and the transfer of such information to third parties in case of termination of operations of the Certification Authority without revocation of valid certificates.
- Limits of use of the certificate, including those established in section 1.4.2.
- Information on how to validate a certificate, including the requirement to check the certificate status and the conditions under which it can reasonably trust the certificate, which applies when the subscriber acts as a relying third party in the certificate.
- How the liability of the Certification Authority is guaranteed.
- Limitations of liability, including the uses for which the Certification Authority accepts or excludes its liability.
- Certificates request information file period.
- Audit registry file period.
- Applicable procedures dispute settlement.
- Applicable Law and competent jurisdiction.

[5] "PKI Disclosure Statement", or PKI disclosure statement applicable.

- If the Certification Authority has been declared in accordance with the certification policy and, where appropriate, in accordance to which system.

9.6.2. Guarantees offered to subscribers and relying third parties in certificates

UANATACA, in the documentation that links the subscribers and relying third parties in certificates, establishes and rejects guarantees, and applicable disclaimers.

UANATACA, at least, guarantees to the subscriber:

- That there are not factual errors in the information in the certificates, known or made by the Certification Authority.
- That there are not factual errors in the information in the certificates, due to lack of diligence due to the management of the certificate request or creation of it.
- Thar the certificates comply with the material requirements established in the Certification Practice Statement.
- That the revocation services and the use of the Deposit comply with all material requirements established in the Certification Practice Statement.

UANATACA, at least, guarantees to the relying third party in the certificate:

- That the information contained or incorporated by reference in the certificate is accurate, except where indicated the opposite.
- In case of certificates published in the Deposit, the certificate has been issued to the subscriber identified in it and the certificate has been accepted, in accordance with section 4.4.
- That in the approval of the certificate request and in the certificate issuance all the material requirementd established in the Certification Practice Statement has been accomplished.
- The rapidity and security in the certification services provision, specially in the revocation services and Deposit.

In addition, UANATACA guarantees to the subscriber and the relying third party in the certificate:

- That the certificate has the information that a recognized certificate must have, in accordance with Article 11 of Law 59/2003, of December 19th.

- That, in case of private keys generated by the subscriber or, where appropriate, the natural person identified on the certificate, his confidentiality is preserved during the process.
- The responsibility of the Certification Authority, with the limits established.

9.6.3. Rejection of other guarantees

UANATACA rejects any other guarantee that is not legally exigible, except the comtemplated in section 9.6.2.

9.6.4. Limitation of liability

UANATACA limits its responsibility to the issuance and management of certificates and key pair subscribers supplied by the Certification Authority.

9.6.5. Indemnity clauses

9.6.5.1. Subscriber indemnity clause

UANATACA includes in the contract with the subscriber, a clause whereby the subscriber agrees to indemnify the Certification Authority of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including judicial and legal representation that may be incurred by the publication and use of the certificate, when occurs any of the following causes:

- False, incorrect or inaccurated statements committed by the certificate user.
- Certificate user error when administering enrollment request data, if there was fraud or negligence in the action or omission regarding the Certification Authority or any relying person in the certificate.
- Private key protection negligence, when using a trustworthy system or when keeping the necessary precautions to avoid its compromise, loss, disclosure, modification or the unauthorized use.
- Use a name (including names, email address and domain names), or other information in the certificate by the subscriber, that infringes intellectual or industrial property of others.

9.6.5.2. Relying third person in the certificate indemnity clause

UANATACA includes in the disclosure text or PDS, a clause whereby the relying third party in the certificate agrees to indemnify the Certification Authority of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including court and legal representation that may be incurred by the publication and use of the certificate, when any od the following causes occurs:

- Breach of the obligations of the relying third party in the certificate.
- Reckless confidence in a certificate, along with the circumstances.
- Lack of checking of the certificate status, to determine that it is not suspended or revoked.

9.6.6. Fortuitous event or force majeure

UANATACA includes in the disclosure text or PDS, clauses that limit its responsibility in fortuitous event or force majeure.

9.6.7. Applicable law

UANATACA establishes, in the subscriber contract and in the disclosure text or PDS, that the applicable law of services provision, including the policy and practices of certification, is the Spanish Law.

9.6.8. Severability, survival, entire agreement and notification clauses

UANATACA establishes, in the subscriber's contract and in the disclosure text or PDS, the severability, survival, entire agreement and notification clauses:

- Under the severability clause, the invalidity of a clause does not affect the rest of the contract.
- Under the survival clause, certain rules remain in force after the completion of the regulatory service of the legal relationship between the parties. For this purpose, the Certification Authority ensures that the requirements of sections 9.6.1 (Obligations and liability), 8 (Compliance audit) and 9.3 (Confidentiality), remain in force after the termination of the service and the general conditions of issuance/use.

- Under the entire agreement clause it is understood that the regulatory legal service contains the full will and all agreements between the parties.
- Under the notification clause the procedure by which the parties do mutually notify facts is established.

9.6.9. Jurisdiction clause

UANATACA establishes, in the subscriber's contract and in the disclosure text or PDS, a jurisdiction clause, indicating that the international jurisdiction corresponds to the Spanish judges.

The territorial and functional jurisdiction shall be determined under the regulations of international private law and procedural law that may be applied.

9.6.10. Resolution of conflicts

UANATACA establishes, in the subscriber's contract, and in the disclosure text or PDS, the procedures for mediation and resolution conflicts applicable.