Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SPECIFIC CERTIFICATION PRACTICES AND POLICY OF CERTIFICATES OF REPRESENTATIVES OF LEGAL ENTITIES AND OF INSTITUTIONS WITH NO LEGAL ENTITY FROM THE "AC REPRESENTACIÓN"

	NOMBRE	FECHA
Prepared by:	FNMT-RCM	15/10/2024
Revised by:	FNMT-RCM	18/10/2024
Approved by:	FNMT-RCM	18/10/2024

Version	Date	Description
1.0	10/07/2015	Document creation
1.1	20/11//2015	Issuing of certificates for representatives of Legal entities and of Institutions with no legal entity as acknowledged. creation
1.2	11/04//2016	Updating of profiles according to ETSI standards and guidelines of TIC Direction
1.3	24/06/2016	Updating in accordance with requirements of ETSI audit.
1.4	03/01/2017	Updating in accordance with requirements of ETSI 319 411.
1.5	22/12/2017	Annual revision of the document.
1.6	05/03/2019	Removal of certificate suspension practices
1.7	20/04/2020	Modifications in accordance with RFC3647 and Annual revision of the document

Version	Date	Description
1.8	18/08/2020	Extension of the scope of application of the certificates of Representatives and the possibility of identification with a qualified certificate.
1.9	28/04/2021	Annual revision of the document. Alignment with Law 6/2020 term "extinction" of the legal personality.
2.0	28/08/2021	Annual revision in compliance with the "S/MIME Baseline Requirements" v.1.0.1 and the "ETSI 119 411-6" standard, Inclusion of the policy and practice for issuing the Entity Seal
2.1	18/10/2024	Removal of all references and policies associated with S/MIME Certificates and "S/MIME Baseline Requirements"

Referencia: DPC/CPREP0201/SGPSC/2024

Documento clasificado como: Public

Index

Tables

1. INTRODUCTION

1.1. OVERVIEW

1. This document is an integral part of the *Trust Services Practices and Electronic Certification General Statement (using the acronym GCSP)* of the FNMT-RCM, and it aims to inform the public about the conditions and characteristics of the certification services and services for the issuing of electronic *Certificates* by the FNMT-RCM as a *Trust Services Provider*, containing the obligations and procedures that with which it agrees to comply in regard to the issuing of the *Certificates of Representatives of Legal Entities, Certificates of Representatives of Institutions with no Legal Entity, and Representative Certificates for Sole and Joint Administrators* and *Entity Seal*.

2. Specifically, for the purposes of the interpretation of these *Specific Certification Practices and Policy*, the "Definitions" section of the *GCSP*, and in such case, the *Issue Law of the Certificate* that corresponds to each entity that uses the certification services of the FNMT-RCM must be taken into account.

3. The Certificates of Representatives of Legal Entities and of Representatives of Institutions with no legal entity and of Representative for Sole or Joint Administrators issued by the FNMT-RCM, whose Specific Certification Practices and Certification Policy are defined in this document, are technically considered to be Recognized or qualified Certificates, in accordance with Regulation (EU) No 910/2014, of the European Parliament and Council, dated 23 July 2014, regarding electronic identification and Trust Services for electronic transactions in the interior market, which repeals Directive 1999/93/EC, and in accordance with the principles of security, integrity, confidentiality, authenticity, and non-repudiation stipulated in the Electronic Signature Act 29/2003, dated 19 December (art. 11.4 and concordant points).

4. The *Representative Certificates for Sole and Joint Administrators* are issued initially to cover the security needs in the legal traffic for these methods of organizing the administration of companies, and later, to be extended to other types of administration based on the state of the art and the possibilities of the *Trust Service Providers* and the persons and organisations who consume the services.

1.2. DOCUMENT NAME AND IDENTIFICATION

5. The *Certification Practices Statement* of the FNMT-RCM, as a *Provider of Trust Services*, is structured, on one hand, based on the common part of the *Trust Services Practices and Electronic Certification General Statement (GCSP)* of the FNMT-RCM, since there are similar levels of action for all of the Entity's services, and on the other, based on the *Specific Certification Practices and Certification Policies* that apply to each type of certificate issued by the Entity in question.

6. In accordance with the above, the structure of the *FNMT-RCM Certification Practices Statement* is as follows:

1. On one hand, the ***Trust Services Practices and Electronic Certification General Statement (GCSP)***, which should be considered to be the main body of the *Certification Practices Statement*, which describes, in addition to the provisions in Act 6/2020, of 11 November, regulating certain aspects of electronic trust services, the liability regime that applies to members of the *Electronic Community*, the security controls applied to the procedures and installations of the FNMT-RCM, in that which may be published without detriment to their effectiveness, secrecy and confidentiality standards, as well as questions related to the ownership of its property and assets, the protection of personal information, and other general information questions that must be made available to the public, regardless of the role in the Electronic Community.

2. And, on the other hand, the specific ***Certification Policy*** which describes the obligations of the parties, the limits of the use of the *Certificates*, and the responsibilities and ***Specific Certification Practices*** that develop the terms defined in the corresponding policy and grant additional or specific functions in addition to the general functions defined in the *GCSP.*

   These *Certification Policies* and *Specific Certification Practices* specify what is articulated in the main body of the *GCSP*, and therefore are an integral part of it, both making up the *Certification Practices Statement* of the FNMT-RCM.

7. This document aims to inform the public about the conditions and characteristics of the certification services provided by the FNMT-RCM as *a Trust Services Provider*, in regard to the life cycle of the electronic *Certificates of Representatives of Legal Entities, Certificates of Representatives of Institutions with no Legal Entity,* and *Representative Certificates for Sole and Joint Administrators* and *Entity Seals*.

8. The contents described in this document therefore apply to the group of *Certificates* that are characterized and identified in these *Specific Certification Practices and Policy* and may also cover special conditions defined in the *Issue Law* of the corresponding *Certificate* or group of *Certificates*, in the case of any specific characteristics or functions.

   Name: *Certification Policy* for *Representative Certificates for Sole and Joint Administrators*

   Reference / OID[1]: 1.3.6.1.4.1.5734.3.11.1

   Type of associated policy: QCP-n. OID: 0.4.0.194112.1.0

[1] *Nota*: El OID o identificador de política es una referencia que se incluye en el *Certificado* al objeto de determinar un conjunto de reglas que indican la aplicabilidad de un determinado tipo de *Certificado* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.

Name: *Certification Policy* for *Certificates of Representatives of Legal Entities*

Reference / OID: 1.3.6.1.4.1.5734.3.11.2.

Type of associated policy: QCP-n. OID: 0.4.0.194112.1.0

Name: *Certification Policy* for *Certificates of Representatives of Institutions with no legal entity*

Reference / OID: 1.3.6.1.4.1.5734.3.11.3.

Type of associated policy: QCP-n. OID: 0.4.0.194112.1.0

Name: *Certification Policy for Entity Seals*

Reference / OID: 1.3.6.1.4.1.5734.3.11.4.

Type of associated policy: QCP-l. OID: 0.4.0.194112.1.1

Version: 2.1

Date of issue: 18/10/2024

Location: http://www.cert.fnmt.es/dpcs/

Related CPS: GCSP of the FNMT-RCM

Location: http://www.cert.fnmt.es/dpcs/

9. The FNMT-RCM provides this document, as well as the *GCSP* document of the FNMT-RCM to the *Electronic Community* and other interested parties, specifying the following:

   1) The terms and conditions that regulate the use of the *Certificates* issued by the FNMT-RCM.
   2) The *Certification Policy* that applies to *Certificates* issued by the FNMT-RCM.
   3) The limits of usage for the *Certificates* issued under the terms of this *Certification Policy*.
   4) The obligations, guarantees and responsibilities of the parties involved in the issuing and use of the *Certificates*.
   5) The periods of conservation of the information gathered in the registration process and the events occurring in the systems of the Trust Services Provider in relation to the management of the life cycle of the *Certificates* issued under the terms of this *Certification Policy*.

10. This *Specific Certification Practices Statement* applies to *Certificates of Representatives of Legal Entities, Certificates of Representatives of Institutions with no Legal Entity,* and *Representative Certificates for Sole or Joint Administrators*, and *Entity Seals* and will take precedence over the provisions in the main body of the *GCSP*

11. Therefore, in the case of contradictions between this document and the provisions in the *GCSP*, the information indicated here shall take precedence.

1.3. PKI PARTICIPANTS

12. The following participants are involved in managing and using the *Trust Services* described in this *SPPS*:

    1. Certification Authority
    2. Registration Authority
    3. *Certificados Subscribers*
    4. Relying Parties
    5. Other participants

1.3.1. Certification Authority

13. FNMT-RCM is the *Certification Authority* issuing the electronic *Certificates* subject of this *SPPS*. The following Certification Authorities exist for these purposes:

    a) Root Certification Authority. This Authority issues subordinate Certification Authority *Certificates* only. This CA's root *Certificate* is identified by the following information

Table 1 – Root "AC Raíz FNMT"

AC FNMT raíz's Certificate	
Subject	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Issuer	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07
Validity	Not before: 29 October 2008. Not after: 1 January 2030
Public key length	RSA 4.096 bits
Signature Algorithm	RSA – SHA256
Key Identifier	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

b) Subordinate Certification Authority: it issues the end-entity Certificates subject of this *SPPS*. This Authority's *Certificate* is identified by the following information:

Table 2 – Subordinate CA Certificate

Subordinate CA Certificate	
Subject	CN = AC Representación, OU = CERES, O = FNMT-RCM, C = ES
Issuer	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Serial Number (hex)	61 C2 D4 D4 F6 A9 AE 77 55 92 66 B9 8D AF D6 21
Validity	Not before: 30 June 2015 Not after: 31 December 2029
Public key length	RSA 2048 bits
Signature Algorithm	RSA – SHA256
Key Identifier	8F D1 6A 17 99 44 D5 D1 D4 20 AF 09 40 5E DA 7A BF 2A 9C 74 28 83 E8 C2 F8 9E 0D 90 AF AF 75 4B

1.3.2. Registration Authority

14. The Registration Authority deals with identifying the applicant and with checking the documentation supporting the facts recorded in the Certificates, validating and approving applications for those Certificates to be issued, revoked and, where appropriate, renewed.

15. Registration Offices designated by the Certificate Subscriber body, agency or entity with which the Subscriber signs the relevant legal instrument for that purpose may act as FNMT-RCM registration entities. The validation and approval of requests for issuance for Entity Seals shall only be carried out from the *Registration Authority* of the FNMT-RCM itself.

1.3.3. Certificate Subscribers

16. The *Subscribers* for the *Certificates* issued under the present SPPS are natural person who shall maintain under their sole control the *Private Keys* associated to their *Certificates.*

17. *The Subscribers* for the *Entity Seals* issued under the present SPPS are legal person who are legally bound by an agreement that describes the terms of use of the *Certificate.*

1.3.4. Relying parties

18. Relying parties are natural or legal persons other than the *Subscriber* that receive and/or use *Certificates* issued by FNMT-RCM and, as such, are subject to the provisions of this *SPPS* where they decide to effectively rely on such *Certificates.*

1.3.5. Other participants

19. No stipulation.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

20. The *Electronic Signature Certificates* and *Electronic Seal Certificates* to which this *SPPS* applies are *Qualified Certificates* as defined in Regulation (EU) No. 910/2014 of the European Parliament and of Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 (eIDAS Regulation) and subject to the requirements established in European standards ETSI IN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI IN 319 412-2 "Certificate profile for certificates issued to natural persons" or ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons" respectively.

21. The *Certificates* issued under the terms of this *Certification Policy* will be considered to be valid as electronic signature and identification systems, in accordance with the Law 39/2015, of October 1st, on the Common Administrative procedures of public administrations based on *Qualified electronic certificates* that are admitted by virtue of their inclusion in the Trust Service lists (TSL) in accordance with the technical specifications specified in the Annex of Commission Decision 2009/767/EC, of 16 October (modified by Commission Decision 2010/425/EU, of 28 July 2010), which adopts measures that facilitate the use of electronic procedures through single-service windows, in accordance with Directive 2006/123/EC, of 12 December 2006, of the European Parliament and Council, regarding services of the internal market. These Trust Service lists contain information regarding *Certification Service Providers* that issues *Qualified electronic certificates* to the public, supervised in each member State, including the FNMT-RCM.

1.4.2. Prohibited certificate uses

22. In any case, if a third party wishes to rely on the *Electronic signature* affixed under one of these *Certificates* without accessing the *Status information service* for *Certificates* issued under this *Certification Policy*, no cover will be obtained under these *Specific Certification Policies and Certification Practices* and there will be no lawful basis whatsoever for any complaint or for legal actions to be taken against FNMT-RCM based on damages, losses or disputes resulting from the use of or reliance on a *Certificate.*

23. In addition, even within the sphere of the *Electronic Community*, this type of *Certificates* may not be used for the following:

- Particular or private uses, except to interact with the Administrations or between the parties when they admit it.
- To sign or seal any other Certificate, except where previously authorised on a case-by-case basis.
- To sign or seal software or components.
- To generate time stamps for *Electronic dating* procedures.
- To provide services for no consideration or for valuable consideration, except where previously authorised on a case-by-case basis, including, but not limited to:
    - Providing *OCSP* services.
    - Generating *Revocation Lists.*
    - Providing notification services.

1.5. POLICY ADMINISTRATION

1.5.1. Organisation administering the document

24. The Spanish mint Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, with Tax Identification Number Q2826004-J, is the *Certification Authority* issuing the *Certificates* to which this *Certification Policy and Practice Statement* applies

1.5.2. Contact details

25. FNMT-RCM's contact address as *Trust Service Provider* is as follows:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

E-mail: ceres@fnmt.es

Teléfono: +34 91 740 69 82

26. To report security issues such as suspected key compromise, certificate misuse, fraud or other matters, send us Certificate Problem Report to incidentes.ceres@fnmt.es

1.5.3. Person determining CPS suitability for the policy

27. The FNMT-RCM Management's remit includes the capacity to specify, revise and approve the procedures for revising and maintaining both Specific Certification Practices and the relevant Certification Policy.

1.5.4. CPS approval procedure

28. Through its *Trust Service Provider* Management Committee, FNMT-RCM oversees compliance with the *Certification Policy and Practice Statements*, and approves and then duly reviews the Statements on a yearly basis

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

29. For the purposes of the provisions of this *SPPS*, capitalised and italicised terms used herein will generally have the definitions given in the GCPS and, in particular, the following:

- *Electronic Signature Certificate:* For the purposes of this *SPPS*, this is a *qualified Certificate* entity that links the *Signer* to a series of *Signature verification data* and confirms his/her identity. The following are *Electronic Signature Certificates*:
  - *Certificate of Representatives of Institutions with no Legal Entity*
  - *Certificate of Representatives of Legal Entities*
  - *Representative certificate for sole and joint administrators*
- *Applicant:* individual over 18 years of age or an emancipated minor, who following identification requests an operation relating to a *Certificate* on behalf of the represented entity. For the purposes of these *Specific Certification Practices and Policy*, this shall be the same as the figure of the *Representative*.
- *Entity Seals*: An electronic statement linking seal validation data to a legal person and confirming that person's name. It is used for the automation of signature and authentication processes between IT components.
- *Certificate of Representatives of Institutions with no Legal Entity:* the *Electronic Signature Certificate* issued to an Institution with no legal entity and used in the area of taxes and other areas permitted by the legislation in force.
- *Certificate of Representatives of Legal Entities*: This *Electronic Signature Certificate* corresponds to the certificate that has traditionally been used by Public Administrations in the tax area, and which was later authorized for other areas. This *Certificate* is therefore issued to *Legal Entities* for use in their relations with Public Administrations, Entities, and Public Institutions that are associated with or dependent on them and for other uses admitted between the parties.
- *Institution with no legal entity:* entities to which article 35.4 of the General Tax Act the rest of the applicable legislation referenced.
- *Legal entity:* person or group of people who constitute a unit with its own purpose which acquires as an entity legal status and capacity to act which is different to those of its members.
- *Representative:* the natural person who legally or voluntarily acts on behalf of a Legal Entity or an Institution with no legal entity.

- *Representative certificate for sole and joint administrators: Electronic Signature Certificate* in which the Signer acts on behalf of a Legal entity in the role of legal representative with the position of sole or joint administrator registered in the Mercantile Registry.
- *Represented entity*: Legal entity or Institution with no legal entity on behalf of which the Signer of a Certificate of those covered by these *Specific Certification Practices and policy* is acting.
- *Signer:* the individual who creates an electronic signature on behalf of his or her own or on behalf of the Legal entity or of the Institution with no legal entity that they represent.
- *Trust Service:* an electronic service that consists of one of the following activities: the creation, verification, validation, management, and conservation of Electronic Signatures, electronic stamps, Timestamps, electronic documents, electronic delivery services, website authentication, and Electronic Certificates, including Electronic Signature and electronic stamp certificates.
- *Trust Services Provider:* the natural person or legal entity that provides one or more Trust Services, in accordance with the provisions in REGULATION (EU) N° 910/2014 OF THE EUROPEAN PARLIAMENT AND COUNCIL, dated 23 July 2014, regarding electronic identification and Trust Services for electronic transactions in the internal market and which replaces Directive 1999/93/EC.
- *Qualified certificate:* Electronic certificate issued by a Trust Services Provider that meets the requirements established in Act 59/2003 of electronic signature regarding identity verification, as well as all other circumstances concerning the applicants, and the reliability and guarantees of the certification services being provided.

(The terms marked in cursive are defined in this document or in the GCSP).

1.6.2. References

30. The following references apply for the purposes of the provisions of this *SPPS*, their meaning being in accordance with European standard ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates":

CA: Certification Authority

AR: Registration Authority

ARL: Certification Authority Revocation List

CN: Common Name

CRL: *Certificate* Revocation List

DN: Distinguished Name

CPS: Certification Practice Statement

GCPS: Trust Services Practices and Electronic Certification General Statement

eIDAS: Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

ETSI: European Telecommunications Standards Institute

HSM: Hardware Security Module. This is a security module that generates and protects cryptographic passwords.

LCP: Lightweight *Certificate* Policy

NCP: Normalised *Certificate* Policy

NCP+: Extended Normalised *Certificate* Policy

OCSP: Online *Certificate* Status Protocol

OID: Object IDentifier

PIN: Personal Identification Number

PKCS: Public Key Cryptography Standards developed by RSA Laboratories

TLS/SSL: Transport Layer Security/Secure Socket Layer protocol.

UTC: Coordinated Universal Time.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORY

31. Being a *Trust Service Provider*, FNMT-RCM has a public information repository available 24x7x365, with the characteristics set out in the following sections, and accessible at the following address:

https://www.sede.fnmt.gob.es/descargas

2.2. PUBLICATION OF CERTIFICATION INFORMATION

32. Information on the issuance of electronic *Certificates* subject of this *SPPS* is published at the following address:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

2.3. TIME AND FREQUENCY OF PUBLICATION

33. Any amendment to the *Trust Services Practices and Electronic Certification General Statement* or to the *Specific Certification Policy and Practice Statement* will be published immediately at the URL where they may be accessed. As stated in section 1.5.4. (CPS approval procedure) reviews frequency will be, at least, once per 365 days.

34. The CRL publication frequency is defined in section "4.9.7 Additional features. Time and frequency of publication".

2.4. ACCESS CONTROLS ON REPOSITORIES

35. The above repositories are all freely accessible to search for and, where appropriate, download information. In addition, FNMT-RCM has established controls to prevent unauthorised persons from adding, altering or deleting information included in its repositories and to protect the authenticity and integrity of that information.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

36. *Certificate* encoding is based on the RFC 5280 standard "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All the fields defined in the *Certificate* profile in the *Specific Certification Policies and Certification Practices,* other than fields specifically providing otherwise, use the UTF8String encoding.

3.1.1. Types of names

37. The end-entity electronic *Certificates* subject of this *SPPS* contain a distinguished name (*DN*) in the Subject Name field, composed as described in the information on the Certificate profile.

38. In processing proof of identity prior to issuing *Electronic Signature Certificates,* FNMT-RCM shall, through the *Registration Office,* ascertain the *Signatory's* true identity and retain the supporting documentation.

3.1.2. Need for names to be meaningful

39. All distinguished names (*DNs*) of the Subject Name field are meaningful. The description of the attributes associated with the *Certificate Subscriber* is human-readable (see section 7.1.4 Name forms hereof).

40. The Common Name field of *Electronic Signature Certificates* defines the *Natural person* to whom the *Certificate* has been issued

41. The Common Name field of an *Entity Seal* defines the name of the automatic process application or system. The name shall be checked to make sure that it is meaningful and unambiguous.

3.1.3. Anonymity or pseudonymity of subscribers

42. The use of pseudonyms as a method for identifying the *Subscriber* is not allowed for the *Certificates* issued under the present *SPPS.*

3.1.4. Rules for interpreting various name forms

43. The requirements defined by X.500 referred to in standard ISO/IEC 9594 are applied.

3.1.5. Uniqueness of names

44. The distinguished name (*DN*) assigned to *Certificates* issued to a *Subject* under these SPPS within the *Trust Service Provider's* domain will be unique.

3.1.6. Recognition, authentication and role of trademarks

45. FNMT–RCM makes no warranty whatsoever regarding the use of distinctive signs, whether registered or otherwise, with respect to *Certificates* issued under this *Certification Policy. Certificates* including distinctive signs may only be requested where the right to use the sign belongs or is duly licensed to the *Owner*. FNMT–RCM is under no obligation to previously check the ownership or registration of distinctive signs before issuing the *Certificates,* even where they are recorded in public registers.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Methods to prove possesion of Private Key

46. FNMT- RCM neither generates nor stores the *Private Keys* associated with *Certificates,* issued under these *SPPS*, the generation of which is exclusively controlled by the *Subscriber*.

3.2.2. Authentication of Organization and Domain Identity

47. FNMT-RCM, as a *Trust Services Provider*, before it issues the *Certificate*, will identify the *Applicant* of the *Certificate*, as well as the information regarding the legal entity of the *Represented entity* and the extent and validity of his/her powers of representation of the *Representative*, by physically visiting a *Registry Office* with which the FNMT-RCM has signed an agreement for this purpose or using a Qualified Certificate of electronic signature that confirms the identity of the requesting natural person. During this act, the *Applicant* and any other third party whose attendance is required, will provide the information and documents that are requested and will accredit their personal identity, as well as the extent and validity of their powers of representation of the *Represented entity*.

48. Likewise, the FNMT-RCM, specifically, will verify, directly or through a third party, the information regarding the incorporation, and in such case, the legal entity of the entity for which the issuing of the *Certificate* is being requested, and the validity of the powers of representation of the Applicant to make the aforementioned application, with the prior submission of the certified documentation that is required for this purpose, and which will be held by the *Trust Services Provider* itself or by the *Registry Office* authorised for this purpose to allow later consultation. The list of this documentation is published in the electronic office portal of the FNMT-RCM (http://www.cert.fnmt.es).

49. In the specific case of *Representative Certificates for sole and joint administrators*, once the FNMT-RCM has verified the personal identity of the *Representative*, it will verify the legal entity of the represented entity and the extent and validity of the powers of representation of the *Representative*, in other words, his/her appointment and entry in the Mercantile Registry

as sole or joint administrator, by means of telematic consultation of the records of the CORPME.

50. The communications between the FNMT-RCM and the CORPME are sent over the SARA inter-administrative network, using processes available 24/7 and secure communications.

51. The information sent by the CORPME to the FNMT-RCM will guarantee that the entity is registered with the Mercantile Register, that the *Applicant* of the *Certificate* is the sole or joint administrator of the *Represented entity*, and will provide the registry information that will be included in the *Certificate* when it is issued.

52. The FNMT-RCM verifies the legal existence, address and identity of the Certificate's subscribing organisation through different methods, depending on the type of organisation (private, public or business).

53. In cases where the Subscriber is a private entity, its identity and address, which is legally recognised, active at that moment, and formally registered, will be verified by direct consultation by the RA of the FNMT-RCM using service that the Mercantile Registry provides for this purpose.

54. For cases of public entities, such verifications will be carried out by direct consultation of the RA of the FNMT-RCM of the inventory of public sector entities contained at the General Intervention Board of the State Administration, under the Ministry of Finance, or in the corresponding Official Gazette.

55. If the nature of the Subscriber is different from the two previous examples, verifications related to its legal capacity, identity and address will be made by direct consultation with the corresponding official registry.

56. The list of Incorporating Agencies or Registration Agencies is published in the Legal Repository on FNMT-RCM's website (https://www.cert.fnmt.es/registro/utilidades).

3.2.3. Authentication of individual applicant identity

57. The FNMT-RCM, as a Trust Services Provider, before it issues the *Certificate*, will identify the *Applicant*, either by physical presence in front of a person with the capacity to carry out the accreditation with the participation of a Registry Office, with which the FNMT-RCM has signed an agreement, or to which a rule or administrative resolution applies, or by means of a valid Qualified Certificate of electronic signature that confirms the identity of the natural person making the application.

3.2.4.1 Direct check by physical presence

58. The accreditation officer will verify that the documents provided to prove the identity of the applicant, meet all the requirements to confirm their identity. *These documents are:* Spanish citizens: National Identity Document, Passport or with other means allowed by law for the purposes of identification (which indicate the National Identity Document Number). UE citizens: Foreign Identification Card or Citizen Registration Certificate of Union (where Tax ID number is included), and Passport or identity document of country of origin, or Official

document of grant of the Tax ID number and Passport or identity document of country of origin. Foreign citizens: Foreign Identification Card (where Tax ID number is included) or Official document of grant of the Tax ID number and Passport.

59. Once the identity of the *Applicant* has been confirmed by the *Registry Office*, the *Registry Office* will validate the information and send it to the FNMT-RCM, along with the application code sent to the *Applicant* by email. This information will be sent via secure communications established for such purpose between the *Registry Office* and the FNMT-RCM. The personal information and their processing, in such case, shall be subject to the specific legislation.

3.2.4.2 Verification using electronic identification means

60. The FNMT-RCM will issue the *Certificate* without the need for the applicant to visit a *Registry Office* in accordance with the process described in the previous section, if, during the application process for the *Certificate* in question, the *Applicant* is identified with a valid electronic *Certificate* that belongs to one of the following types:

- A *Natural Person Certificate* issued under the terms of this *Policy*.
- A *Representative Certificate for sole and joint administrators*..
- One of the electronic *Certificates* incorporated into the DNIe.

61. However, telematic applications for *Certificates* through the use of the electronic certificates listed in the previous section shall only be allowed if at the time of the application, the maximum term established by the current legislation has not been exceeded since the personification and physical identification of the *Subscriber*.

3.2.4. Non-verified Subscriber information

62. All information included in the electronic *Certificate* is verified by the *Registration Authority*.

3.2.5. Validation of the authority

63. Once the identity of the *Applicant* has been confirmed by the *Registry Office*, the *Registry Office* will validate the information and send it to the FNMT-RCM, along with the application code sent to the *Applicant* by email. This information will be sent via secure communications established for such purpose between the *Registry Office* and the FNMT-RCM. The personal information and their processing, in such case, shall be subject to the specific legislation.

64. Prior to the issuance of the Certificate, the FNMT_RCM establishes additional controls, such as confirming that the applicant is not registered as deceased in the records that the Ministry of Justice communicates to this Entity for this purpose.

65. *Certificates* will not be issued to minors, unless they hold and prove their emancipated status. The Registry Office will be in charge of carrying out the validations related to this point.

3.2.6. Criteria for interoperation

66. There are no interoperational relationships with Certification Authorities external to FNMT-RCM (The FNMT-RCM does not issue cross-certificates).

3.2.7. Reliability of verification sources

67. The FNMT-RCM assess the suitability of its Sources as a Reliable Data Sources

68. Prior to using any data source as a Reliable Data Source, the RA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

69. Under these Certification Policies, FNMT-RCM makes no provision for a re-keying process.

70. The authentication terms for a renewal request are set out in the section dealing with the Certificate renewal procedure hereof.

3.3.1. Requirements for routine re-key

71. Under these Certification Policies, FNMT-RCM makes no provision for routine renewal.

3.3.2. Requirements for re-key after certificate revocation

72. Under these Certification Policies, FNMT-RCM makes no provision for renewal after revocation.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

73. Before actually revoking the *Certificates*, the Registration Authority shall authoritatively identify who requested the Revocation to link them to the unique data of the *Certificate* to be revoked.

74. The authentication terms for a revocation request are set out in the relevant section hereof dealing with the *Certificate* revocation procedure.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who can submit a Certificate application

75. The Applicant for this type of Certificate can only be a natural person, of legal age or minor, who proves his emancipated status, in possession of his National Identity Document number or Foreigner Identification Number.

4.1.2. Registration process and responsabilities

4.1.2.1 For the electronic signature certificates :

76. The interested party visits the website of the *Trust Services Provider* of the FNMT-RCM at the URL http://www.cert.fnmt.es, where the instructions for the entire process for obtaining the *Certificate* will be displayed. The *Applicant* must enter their Tax Identification Number, first surname, and email address, and the Tax Identification Number of the represented entity in the information collection form provided for this. Likewise, the *Applicant* will express the desire to obtain the *Certificate* for which the application is being filed, and will give consent for the FNMT-RCM to query the Identity Information Verification System, as well as the pertinent query to the Mercantile Register, in order to verify the legal entity of the represented entity, and the extent and validity of the powers of representation.

77. In this same process, for the case of the *Representative Certificates for sole and joint administrators*, their consent will also be sought to carry out the pertinent consultation with the Mercantile Registry, in order to verify the legal personality of the represented Entity, and the extension and validity of its powers of representation.

78. Next, it is asked to validate the *Applicant*'s email, which it is included in the Application. In order to validate the email, a unique random number is sent to the provided email. To finish the validation process, the Applicant shall access his email and follow the given directions.

79. The *Applicant* must previously consult the General and Specific *Certification Practice Statements* at the URL http://www.ceres.fnmt.es/dpcs/ with the conditions of use and obligations of the parties.

80. When this application is made, the *Public Key* that is generated is sent to the FNMT-RCM, along with the corresponding proof of possession of the *Private Key*, for the later issuing of the *Certificate*. The sending of the *Public Key* to the CA for the generation of the *Certificate* is done using a standard format, PKCS#10 or SPKAC, using a secure channel for the transmission.

81. After the FNMT-RCM receives this information, it will use the applicant's *Public Key* to verify the validity of the information in the application, verifying only the possession and correspondence of the pair of *Cryptographic keys* by the applicant, the size of the generated keys, as well as the registration of the *Represented entity* and the *Representative's* role as sole or joint administrator with the CORPME.

82. This information shall not result in the generation of a *Certificate* by the FNMT-RCM until it receives confirmation from the *Registry Office* of the identification of the *Applicant*, and in addition, that it has verified the legal entity of the represented entity and the extent and validity of the powers of representation of the *Representative*.

83. The *Certificate* application procedure is completed with the transmission by the FNMT-RCM of an email to the address provided by the *Applicant*, specifying the unique application code assigned and informing the *Applicant* of the upcoming phases in the process to obtain the *Certificate*.

84. Section 9.8 "Responsibilities" hereof defines the parties' responsibilities in this process.

4.1.2.2 For the Entity Seals:

85. The FNMT-RCM require each Applicant to submit a Certificate request and application information prior to issuing an Entity Seal. The FNMT-RCM authenticates all communication from an Applicant and protects communication from modification.

86. The enrollment process includes:

- Submitting a complete Certificate application and agreeing to the applicable subscription agreement. By executing the subscription agreement, Subscribers warrant that all of the information contained in the Certificate request is correct.
- Se valida la dirección de correo electrónico del *Suscriptor,* enviando un código único y aleatorio al correo electrónico suministrado. Deberá acceder a su correo y seguir las indicaciones proporcionadas.
- Generating a key pair,
- Delivering the public key of the key pair to the CA and
- Paying any applicable fees.

87. The RA of the FNMT-RCM performs the verification of the identity of the subscribing Organisation and of the Subscriber Representative, and verifies that the application for the Certificate is both correct and duly authorised, in accordance with the requirements contained in section "3.2 Initial Validation of identity" of this document. The FNMT-RCM may carry out additional verification on the validation processes described in the aforementioned section.

88. FNMT-RCM will collect the evidence corresponding to the verifications made, which will be stored in a repository.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing identification and authentication functions

89. Applicants will supply the requested information and evidence of their personal identity. The FNMT-RCM, through the Registry Office, will verify the true identity of the Subscriber, the legal personality of the represented Entity and the extension and validity of the powers of representation of the Representative and will keep the documentation that accredits it. FNMTRCM will admit, in any case, the function and report made by the Registry Office.

90. For the issuance of Electronic Signature Certificates, the FNMT-RCM may identify the Applicant, as an alternative to appearing at the Registry Office, by using a qualified Electronic Signature Certificate as described in section "3.2.3.2. Verification using electronic identification means".

4.2.2. Approval or rejection of certificate applications

91. Once the aforementioned verifications have been completed and the FNMT-RCM has received the personal information from the *Applicant*, along with the application code, it will issue the requested *Certificate*.

92. The transmission of information to the FNMT-RCM will be carried out through secure communications established for this purpose between the Registry Office and the FNMT-RCM.

93. FNMT-RCM will have *Applicants* provide such information received from the *Registration Office* as may be necessary for the *Certificates* to be issued and for the identity to be checked, storing the information required by electronic signature laws for a period of fifteen (15) years, duly processing that information in compliance with the national personal data protection laws in force from time to time.

94. Personal information and processing of such information shall be subject to specific laws.

4.2.3. Time to Process Certificate Applications

95. An approved application for *Electronic Signature Certificates* is automatically processed by the system, so there is no stipulated time for this process.

96. For the Entity Seals, the FNMT-RCM will require the minimum time necessary from the receipt by the FNMT - RCM Registry Office of all the documentation necessary to carry out the required checks prior to the issuance of the Certificate.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions During Issuance

97. Once FNMT-RCM receives the Applicant's personal information, as well as the legal personality of the represented Entity and the extension and validity of the powers of

representation of the Representative, and the application code obtained at the application stage, the Certificate will be issued.

98. The issuance of Certificates results in the generation of electronic documents confirming the Subscribers identity, and that it matches the associated Public Key. FNMT-RCM Certificates may only be issued by FNMT-RCM in its capacity as Trust Service Provider, and no other entity or organisation has authority to issue the same. The FNMT-RCM Certification Authority only accepts Certificate generation applications from authorised sources.

99. The information contained in each application is fully protected against alterations through *Electronic Signature* or *Electronic Seal* mechanisms prepared using *Certificates* issued to those authorised sources.

100. FNMT-RCM will in no case have a Certificate include information other than that referred to herein, or any circumstances, specific attributes of the Signatories or restrictions other than the ones indicated in the present *SPPS*.

101. In any case, FNMT-RCM will use its best efforts:

- To check that the *Certificate Applicant* use the *Private Key* for the *Public Key* linked to the *Certificate.* FNMT-RCM will therefore check that the *Private Key* corresponds to the *Public Key*.
- To ensure that the information included in the Certificate is based on the information provided by the relevant Registration Office.
- Not to ignore known facts potentially affecting Certificate reliability.
- To ensure that the DN (distinguished name) assigned to a Subject under this SPPS is unique.

102. The following steps will be taken to issue the *Certificate*:

1. Certificate data structure composition

   The data collected when processing the Certificate application is used to compose the distinguished name (*DN*) based on standard *X.500*, making sure that the name is meaningful and unambiguous.

2. Composition of the alternative identity of the *Certificates*

   The alternative identity of these *Certificates* is distributed in a series of attributes, so that it is easier to obtain the information of the *Representative* of the *Certificate* and the *Represented* entity. To do this, the subjectAltName extension defined in *X.509* version 3 is used, containing the following information:

   - the email address of the *Applicant,*
   - in the DirectoryName subfield, name, surname, Tax ID number and Position or powers (*Sole or Joint Administrators*) of the representative, followed by the Company name and the Tax number of the *Represented entity.*

3. *Certificate* generation in accordance with the relevant *Certificate* profile.

103. The form of Certificates issued by FNMT-RCM under this Certification Policy, in keeping with standard UIT-T X.509 version 3 and under the laws applicable to Qualified Certificates, may be viewed at http://www.cert.fnmt.es/dpcs/

4.3.2. Notification of Issuance

104. Upon the *Certificate* being issued, FNMT-RCM will inform *Applicants* that the *Certificate* is available for download.

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1. Conduct constituting certificate acceptance

105. During the *Certificate* application process, *Applicants* accept the terms of use and express their willingness to obtain the *Certificate*, and the requirements necessary for the *Certificate* to be generated.

106. The FNMT-RCM will make available exclusively to the *Subscriber* for retrieval the *Certificate,* at the website http://www.cert.fnmt.es.

107. In this guided process, the *Applicant* will be asked to enter the National Identity Document (DNI) or Foreign Resident Identification Number (NIE), first surname, and the corresponding application code obtained in this process. This application code will be used as the accepted key for the generation by the *Holder* of an electronic signature of the conditions of use of the *Certificate*, as a mandatory requirement to download the certificate and accept the conditions of use, sending these signed conditions to the FNMT-RCM. If the *Natural Person Certificate* has not been generated yet for any reason, the process will inform the applicant of this.

108. The *Applicant* will pay the amount corresponding to the public prices approved by the FNMT-RCM for this type of *Certificate*. To do this, the FNMT-RCM provides citizens and organisations with secure methods of payment through the website from which the *Certificate* is downloaded.

109. Once payment has been made, the *Certificate* will be installed on the support on which the Keys will be generated during the application process (cryptographic token or if not, the *Browser* from which the application was made). The aforementioned website of the FNMT-RCM indicates the supported *Browsers* and the certificate installation requirements.

4.4.2. Publication of the certificate by the CA

110. *Certificates* generated are stored in a secure repository of FNMT-RCM, with restricted access.

4.4.3. Notification of issuance to other entities

111. Notification of issuance is not provided to other entities.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and certificate usage

112. FNMT-RCM neither generates nor stores the Private Keys associated with Certificates issued under this Certification Policy. Custody of and responsibility for controlling the Certificate keys lies with the Subscriber.

113. The Certificates issued under the terms of this Certification Policy will be considered to be valid as electronic signature and identification systems, in accordance with the Law 39/2015, of October 1st, on the Common Administrative procedures of public administrations based on Qualified electronic certificates.

4.5.2. Relying party public key and certificate usage

114. Third parties relying on Electronic signatures based on the Private Keys associated with the Certificate shall observe the representations and warranties defined in this SPPS.

4.6. CERTIFICATE RENEWAL

115. FNMT-RCM does not renew Certificates under these Certification Policies maintaining their Public key

4.6.1. Circumstance for certificate renewal

116. FNMT-RCM does not renew Certificates under these Certification Policies maintaining their Public key

4.6.2. Who may request renewal

117. FNMT-RCM does not renew Certificates under these Certification Policies maintaining their Public key

4.6.3. Processing certificate renewal requests

118. FNMT-RCM does not renew Certificates under these Certification Policies maintaining their Public key

4.6.4. Notification of new certificate issuance to subscriber

119. FNMT-RCM does not renew Certificates under these Certification Policies maintaining their Public key

4.6.5. Conduct constituting acceptance of a renewal certificate

120. FNMT-RCM does not renew Certificates under these Certification Policies maintaining their Public key

4.6.6. Publication of the renewal certificate by the CA

121. FNMT-RCM does not renew Certificates under these Certification Policies maintaining their Public key

4.6.7. Notification of certificate issuance by the CA to other entities

122. FNMT-RCM does not renew Certificates under these Certification Policies maintaining their Public key

4.7. CERTIFICATE RE-KEY

123. Under these Certification Policies, *Certificate* re-key in only intended for *Representative Certificates for sole and joint administrators* which will always be carried out by issuing new keys and following the same process as described for the issuance of a new Certificate.

124. *Representative Certificates for sole and joint administrators* may only be renewed a single time. *Subscribers* who have already renewed their *Certificates* and would like to continue using a *Representative Certificates for sole and joint administrators* under the terms of these *Specific Certification Practices and Policies*, must request a new *Certificate* and confirm their identity in accordance with the procedure described in the section "*3.2.3. Authentication of individual applicant identity*.

125. The renewal of the *Representative Certificates for sole and joint* issued by the FNMT-RCM to the *Subscribers* of the *Certificates* may be requested provided that at the time of the request they have a *Certificate* in force and the associated *Signature creation data*, and that this request is made during the sixty (60) days prior to the *Expiration* of the *Certificate*.

126. The renewal of a *Representative Certificates for sole and joint administrators* shall consist of the generation of new *Signature verification data* and *Signature creation data*, as well as the issuing of a new *Natural Person Certificate*. The renewal request will be made through the URL http://www.ceres.fnmt.es.

127. A *Certificates* that is close to expiration shall remain valid until its period of effectiveness expires. If the revocation of a *Certificate* is requested during the periods of time that the *Holder* has two active *Certificates*, the FNMT-RCM shall revoke both *Certificates*.

128. The identification of the *Representative*, as the *Applicant* for the renewal of the *Certificate* will be done telematically using the *Representative Certificate for Sole and Joint Administrators* that, while still active, is close to its expiration date, provided that at the time of the application, the maximum period of 5 years has not elapsed since the physical visit and identification of the *Representative*, as established in the Act 6/2020, of 11 November, regulating certain aspects of electronic trust services.

129. The renewal process of the *Certificate* will include, during the *Certificate* download phase, the payment by the *Applicant* of the amount corresponding to the public prices approved by the FNMT-RCM for this type of *Certificate.*

130. The use of renewed *Representative Certificates for sole and joint administrators* is subject to the same general and specific conditions that are in effect at any given time and that are established for this type of *Certificates* in their corresponding *Certification Practices Statement*.

4.7.1. Circumstances for certificate re-key

131. *Certificates* shall be re-keyed where the current keys are to expire soon, upon request by the renewal applicant or key compromiso or another circumstance in section 4.9

4.7.2. Who may request re-key

132. The same process described for the issuance of a new Certificate will be followed.

4.7.3. Processing certificate re-keying requests

133. The same process described for the issuance of a new Certificate will be followed.

4.7.4. Notification of certificate re-key

134. The same process described for the issuance of a new Certificate will be followed.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

135. The same process described for the issuance of a new Certificate will be followed.

4.7.6. Publication of the re-keyed certificate

136. The same process described for the issuance of a new Certificate will be followed.

4.7.7. Notification of certificate re-key to other entities

137. The same process described for the issuance of a new Certificate will be followed.er

4.8. CERTIFICATE MODIFICATION

138. Certificates issued cannot be modified. Therefore, any modification required shall result in a new Certificate being issued.

4.8.1. Circumstance for certificate modification

139. The modification is not stipulated.

4.8.2. Who may request certificate modification

140. The modification is not stipulated.

4.8.3. Processing certificate modification requests

141. The modification is not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

142. The modification is not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

143. The modification is not stipulated.

4.8.6. Publication of the modified certificate by the CA

144. The modification is not stipulated.

4.8.7. Notification of the certificate issuance by the CA to other entities

145. The modification is not stipulated.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

146. *Certificates* issued by FNMT-RCM will cease to be valid in the following cases:

a) Termination of the *Certificate* validity period.

b) Discontinuance of FNMT-RCM's activity as a *Trust Service Provider* unless, subject to the *Subscriber's* prior express consent, the *Certificates* issued by FNMT-RCM have been transferred to another *Trust Service Provider*.

In these two cases [a) and b)], the *Certificates* will cease to be valid forthwith upon the occurrence of these circumstances.

c) Revocation of the *Certificate* in any of the events provided for herein.

147. Revocation of the *Certificate*, i.e. termination of its validity, shall be effective from the date on which FNMT-RCM actually learns of the occurrence of any trigger events and records that in its *Certificate status information and checking service*.

148. For the aforementioned purposes, the issuing of a *Certificates*, when there is another for the same *Subscriber* in force shall immediately result in the revocation of the previous *Certificate*. The only exception to this occurs when the issuing of a *Representative Certificates for sole and joint administrators* is as a result of a renewal process for the certificate within a period of sixty (60) days prior to the expiration date, in which the *Certificate* that is close to expiring shall remain valid until its validity period has expired. During this time, if the *Certificate* in

question is revoked in accordance with the following section, the validity of both *Certificates* shall be extinguished.

149. FNMT-RCM provides Subscribers, relying parties, software providers and third parties with a communication channel through the FNMT-RCM website https://www.sede.fnmt.gob.es/.

4.9.1. Circumstances for revocation

4.9.1.1 Reasons for revoking a subscriber certificate

150. The Certificate revocation request may be made during the validity period specified in the Certificate.

151. The following are admissible grounds for a Certificate to be revoked:

a) The revocation request by the *Signer*, of the *Represented entity* represented by him/her, or by a duly authorized third party. This should be requested in all of the following cases:

- Loss of the *Certificate* support.
- Use by third parties of the *Signature Creation Data* corresponding to the *Signature Verification Data* contained in the *Certificate* and linked to the identity of the *Representative* and the *Represented entity*.
- The violation or endangerment of the secrecy of the *Signature Creation Data*.
- Failure to accept new conditions that may be included in the issuing of new *Certification Practice Statements*, within one month of publication..

b) Judicial or administrative resolutions that order this.

c) Decease of the *Representative*.

d) Total or partial supervening incapacity of the *Representative*.

e) Termination of the representation.

f) Extintion of the represented legal entity.

g) Inaccuracies in the information provided by the *Applicant* to obtain the *Certificate*, or the alteration of the information provided to obtain the *Certificate*, or the modification of the verified circumstances for the issuing of the *Certificate*, as well as the circumstances related to the position or powers of representation, in such a way that it is no longer consistent with reality.

h) Contravening of a significant obligation of this *Certification Practices Statement* by the *Represented entity,* the *Signer* or *Applicant* for the *Certificate*, if, in the latter case, this may have affected the procedure for the issuing of the *Certificate*.

i) Contravening of a significant obligation in this *Certification Practices Statement* by a *Registry Office*, if this may have affected the procedure for the issuing of the *Certificate*.

j) Termination of the contract signed between the *Represented entity* or the *Signer* and the FNMT-RCM, as well as the non-payment or retrocession of the payment of the amount associated with the obtaining of the Certificate.

k) Discontinuance of the *Trust Service Provider's activity* unless management of the electronic *Certificates* issued thereby is transferred to another *Trust Service Provider*.

152. Under no circumstances does the FNMT-RCM assume any obligation to verify the circumstances mentioned in letters c) to i) of this section; the FNMT-RCM must be notified by certified communication by delivery of the documents and information required to verify this. For the *Representative Certificates for sole and joint administrators* the aspects mentioned in letters e) and f) of this section shall be reported by the CORPME to the FNMT-RCM, at which time the FNMT-RCM will revoke the *Certificate* in question.

153. FNMT-RCM shall be liable for the consequences resulting from failure to revoke a Certificate in following cases only:

- The revocation should have been carried out by certified request by the *Signer* or the *Represented entity*, or by means of the systems provided by the FNMT-RCM for this purpose.
- The FNMT-RCM has been notified of the revocation request or the cause behind the request by a judicial or administrative resolution.
- Causes c) to i) of this section have been reported by certified communication, with prior identification of the *Represented entity*, *Representative*, and/or *Applicant* of the revocation (or the person with sufficient powers of representation, in the case of supervening incapacity of the *Representative*).
- For the *Representative Certificates for sole and joint administrators*, that causes e) and f) of this section have been reported by the CORPME by means of the systems provided for this purpose, or by a certified method of communication, with prior identification of the *Represented entity*, *Representative*, and/or *Applicant* of the revocation (or the person with sufficient powers of representation, in the case of cessation or supervening incapacity of the *Representative).*

154. Actions that constitute crime or omission of which the FNMT-RCM does not have knowledge that are carried out on the information and/or *Certificate* and inaccuracies or lack of diligence in notification of the FNMT-RCM shall release the FNMT-RCM of liability.

155. The revocation of the *Certificate*, in addition to the extinguishing of its effects, also supposes the termination of the relationship and usage regime for the *Certificate* in question with the FNMT-RCM.

4.9.1.2 Reasons for revoking a subordinate CA Certificate

156. The provisions of the "FNMT-RCM Public Key Infrastructure Compromise Action Plan" will be observed.

4.9.2. Who can request revocation

157. Revocation of a *Certificate* may only be requested:

- the *Certification Authority* and the *Registration Authority*
- the *Represented entity* or a person with sufficient powers of representation, at the *Registration Office*
- as the case may be, the *Subscriber,* calling the telephone number provided for that purpose (subject to identification of the *Applicant*) and posted at FNMT-RCM's website, which shall be operational 24x7, or through that *Registration Office*.

158. FNMT-RCM may revoke the *Certificates* of its own accord in the events referred to in this Certification Policy and Practice Statement and in the specific case of the *Representative Certificates for Sole and Joint Administrators* itself in cases in which the CORPME notifies it of the modification of any of the significant conditions included in the *Certificate*, in regard to the extinguishing of the legal entity of the represented entity or the extent and validity of the powers of representation of the *Representative*, and in the rest of the cases included in this *Certification Practices Statement*.

4.9.3. Procedure for revocation request

159. An Electronic Signature Certificates revocation request may be made during the validity period specified in the Certificate.

160. The revocation of a Certificate may only be requested by the Subscriber or person with sufficient powers of representation, in the case of supervening incapacity of the Holder, under the terms specified in these Specific Certification Practices and Policies.

161. Revocation may be processed continuously 24x7 through the telephone Revocation Service (+34 91 740 69 82) available to users for such purpose, and revocation of the Certificate is guaranteed within less than 24h.

162. During telephone revocation, the applicant shall have to provide whatever details may be required, and supply such information as may be essential to unequivocally validate the requestor's authority to request revocation.

163. If the Represented entity is in possession of the Representative Certificates for Sole and Joint Administrators and its associated Signature creation data, it is possible to authenticate the its identity based on this Certificate, so the revocation of the Certificate may be requested via Internet, or any other equivalent method that allows the connection to the URL http://www.ceres.fnmt.es, following the directions indicated on the website. This service shall be available twenty-four (24) hours a day, 365 days a year, except in circumstances beyond the control of FNMT-RCM or during maintenance operations. The FNMT-RCM will announce maintenance operations at the URL http://www.ceres.fnmt.es, if possible, with at least forty-eight (48) hours' notice, and will try to resolve the situation within a period of no more than twenty-four (24) hours.

164. Additionally, a request for revocation of any Electronic Signature Certificate may be made through the Registration Office. Personal information and processing of such information shall be subject to specific laws. The applicant shall go to the Registration Office, where the requestor's identity shall be established, along with the requestor's capacity to revoke that Certificate, and the ground for revocation shall be specified. The Office will send the information to FNMT-RCM electronically using registration software, and will process revocation of the Certificate.

165. For the Entity Seals, it is also possible to submit the revocation request to the Registration Area of the FNMT-RCM, adhering to the following procedure:

1. *Subscriber* request

   The *Subscriber's Representative* will submit the revocation request form the FNMT-RCM, completed and electronically signed with any of the *Certificates* admitted for the application and by the electronic channels enabled by this Entity.

2. Processing of the request by the FNMT-RCM

   The registrar of the FNMT-RCM will receive the revocation contract, and will carry out the same checks regarding the identity and capacity of the Subscriber's Representative as would be performed for cases of issuance requests and, if approved, will process the revocation of the Certificate.

166. As soon as revocation is effective, the *Applicant* and the *Subscriber* will be notified using the email address provided.

167. Once FNMT-RCM has processed *Certificate* revocation, the relevant *Certificate Revocation List* will be published in the secure *Directory,* including the revoked *Certificate* serial number, along with the date, time and reason for revocation. Once a *Certificate* is revoked, its validity shall definitively terminate and revocation may not be reversed.

168. To report about suspected Private Key Compromise, Certificate misuse or other types of frauds, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, you can send and email with a CPR to incidentes.ceres@fnmt as shown in section 1.5.2.

4.9.4. Revocation request grace period

169. No grace period is associated with this process, for revocation occurs forthwith upon verified receipt of the revocation request.

4.9.5. Time within which to process the revocation request

170. FNMT-RCM processes *Certificate* revocation immediately upon checking the *applicant's* identity or, as the case may be, once the authenticity of a request made by means of a court or administrative decision has been checked. In any case, the *Certificate* will be effectively revoked within less than 24 hours of the revocation request being received

171. Within 24 hours after receiving a CPR (via incidentes.ceres@fnmt.es) as seen in section 1.5.2, the CA will investigate the facts and circumstances related to the CPR and provide a preliminary report to both the Subscriber and the entity who filed the CPR.

172. After reviewing the facts and circumstances, the CA will work with the Subscriber and any entity reporting the CPR or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date which the CA will revoke the Certificate. The period from receipt of the CPR or revocation-related notice to published revocation will not exceed the timeframe set forth in section 4.9.1.1.

173. The date selected by the CA will consider the following criteria:

1. The nature of the alleged problem(scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of CPRs received about a particular Certificate or Subscriber;
4. The entity making the complaint; and
5. Relevant legislation.

4.9.6. Revocation checking requirement for relying parties

174. Third parties relying on and accepting the use of the Certificates issued by FNMT-RCM must check, by any of the available means (CRL Revocation Lists and/or OCSP), the status of the Certificates:,

- the *Advanced Electronic Signature* or *Advanced Electronic Seal* of the *Trust Service Provider* issuing the *Certificate,*
- that the *Certificate* is still valid and active, and
- the status of the *Certificates* included in the *Certification Chain.*

4.9.7. CRL issuance frequency

175. Electronic Signature and Electronic Seal Certificate Revocation Lists (CRLs) are issued at least every 12 hours, or whenever a revocation occurs, and they are valid for a period of 24 hours. Authority Certificate CRLs are issued every 6 months, or whenever a subordinate Certification Authority revocation occurs, and they are valid for a period of 6 months.

4.9.8. Maximum latency for CRLs

176. Revocation Lists are published upon being generated, and therefore there is no latency between CRL generation and publication.

4.9.9. On-line revocation/status checking availability

177. On-line Certificate revocation/status information will be available 24x7. In the event of system failure, the Business Continuity Plan shall be put in place to resolve the incident as soon as possible.

4.9.10. On-line revocation checking requirements

178. The revocation status of Electronic Signature and Electronic Seal Certificates may be checked on line through the OCSP Certificate status information service offered as described in section 4.10 below. The party interested in using that service must:

- Check the address contained in the *Certificate* AIA (Authority Information Access) extension.
- Check that the OCSP response is signed / sealed.

4.9.11. Other forms of revocation advertisements available

179. Not defined.

4.9.12. Special requirements related to key compromise

180. See the relevant section in the GCPS

4.9.13. Circumstances for suspension

181. Certificate suspension is not supported.

4.9.14. Who can request suspension

182. Certificate suspension is not supported.

4.9.15. Procedure for suspension request

183. Certificate suspension is not supported.

4.9.16. Limits on Suspension Period

184. Certificate suspension is not supported.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational characteristics

185. Validation information regarding the electronic Certificates subject of this SPPS is accessible using the means described in the GCPS.

4.10.2. Service availability

186. FNMT-RCM guarantees 24x7 access to this service by Certificate Users and relying parties securely, quickly and free of charge.

4.10.3. Optional features

187. Not stipulated.

4.11. END OF SUBSCRIPTION

188. Subscription will end when the Certificate ceases to be valid, whether upon the validity period ending or due to revocation thereof. If the Certificate is not renewed, the relationship between the Signatory and FNMT-RCM will be deemed to have terminated.

189. It is noted in the above connection that where an application for FNMT-RCM to issue an Electronic Signature Certificate and the same Signatory and same Subscriber have another Certificate in force under the same Issuance Law, the first Certificate obtained will be revoked.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policy and practices

190. FNMT-RCM will not recover the Private Keys associated with the Certificates.

4.12.2. Session key encapsulation and recovery policy and practices

191. No stipulation.

5. PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

192. See the relevant section in the GCPS

5.1. PHYSICAL SECURITY CONTROLS

193. See the relevant section in the GCPS

5.1.1. Site location and construction

194. See the relevant section in the GCPS

5.1.2. Physical access

195. See the relevant section in the GCPS

5.1.3. Power and air conditioning

196. See the relevant section in the GCPS

5.1.4. Water exposures

197. See the relevant section in the GCPS

5.1.5. Fire prevention and protection

198. See the relevant section in the GCPS

5.1.6. Media storage

199. See the relevant section in the GCPS

5.1.7. Waste disposal

200. See the relevant section in the GCPS

5.1.8. Off-site backup

201. See the relevant section in the GCPS

5.2. PROCEDURAL CONTROLS

202. See the relevant section in the GCPS

5.2.1. Trusted roles

203. See the relevant section in the GCPS

5.2.2. Number of persons required per task

204. See the relevant section in the GCPS

5.2.3. Identification and authentication for each role

205. See the relevant section in the GCPS

5.2.4. Roles requiring separation of duties

206. See the relevant section in the GCPS

5.3. PERSONNEL CONTROLS

207. See the relevant section in the GCPS

5.3.1. Qualifications, experience, and clearance requirements

208. See the relevant section in the GCPS

5.3.2. Background check procedures

209. Véase el apartado correspondiente en la *DGPC*

5.3.3. Training requirements

210. Véase el apartado correspondiente en la *DGPC*

5.3.4. Retraining frequency and requirements

211. Véase el apartado correspondiente en la *DGPC*

5.3.5. Job rotation frequency and sequence

212. See the relevant section in the GCPS

5.3.6. Sanctions for unauthorized actions

213. Véase el apartado correspondiente en la *DGPC*

5.3.7. Independent contractor requirements

214. See the relevant section in the GCPS

5.3.8. Documentation supplied to personnel

215. See the relevant section in the GCPS

5.4. AUDIT-LOGGING PROCEDURES

216. See the relevant section in the GCPS

5.4.1. Types of events recorded

217. See the relevant section in the GCPS

5.4.2. Frequency of processing log

218. See the relevant section in the GCPS

5.4.3. Retention period for audit log

219. See the relevant section in the GCPS

5.4.4. Protection of audit log

220. See the relevant section in the GCPS

5.4.5. Audit log backup procedures

221. See the relevant section in the GCPS

5.4.6. Audit collection system (internal vs. external)

222. See the relevant section in the GCPS

5.4.7. Notification to event-causing subject

223. See the relevant section in the GCPS

5.4.8. Vulnerability assessments

224. See the relevant section in the GCPS

5.5. RECORDS ARCHIVAL

225. See the relevant section in the GCPS

5.5.1. Types of records archived

226. See the relevant section in the GCPS

5.5.2. Retention period for archive

227. See the relevant section in the GCPS

5.5.3. Protection of archive

228. See the relevant section in the GCPS

5.5.4. Archive backup procedures

229. See the relevant section in the GCPS

5.5.5. Requirements for time-stamping of records

230. See the relevant section in the GCPS

5.5.6. Audit collection system (internal vs. external)

231. See the relevant section in the GCPS

5.5.7. Procedures to obtain and verify archive information

232. See the relevant section in the GCPS

5.6. CA KEY CHANGEOVER

233. See the relevant section in the GCPS

5.7. COMPROMISE AND DISASTER RECOVERY

234. See the relevant section in the GCPS

5.7.1. Incident and compromise handling procedures

235. See the relevant section in the GCPS

5.7.2. Computing resources, software, and/or data are corrupted

236. See the relevant section in the GCPS

5.7.3. Entity Private Key compromise procedures

237. See the relevant section in the GCPS

5.7.4. Business continuity capabilities after a disaster

238. See the relevant section in the GCPS

5.8. TRUST SERVICE PROVIDER TERMINATION

239. See the relevant section in the GCPS

6. TECHNICAL SECURITY CONTROLS

240. See the relevant section in the GCPS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key pair generation

6.1.1.1 CA key pair generation

241. As for the CA Key generation FNMT-RCM needs to carry out its activity as Trust Service provider, see the relevant section in the GCPS.

6.1.1.2 RA key pair generation

242. No estipulation.

6.1.1.3 Subscriber key pair generation

243. As for Subscriber Key generation FNMT-RCM neither generates nor stores the Private Keys associated with the Certificates issued under these Specific Certification Policies and Certification Practices, for Key generation is exclusively controlled by the Subscriber.

6.1.2. Private Key delivery to the subscriber

244. There is no Private Key delivery in the issuance of Certificates under these Certification Policies and Practices.

245. In any case, if FNMT-RCM or any registration office should become aware of unauthorised access to the Signatory's Private Key, the Certificate associated with that Private Key will be revoked.

6.1.3. Public key delivery to certificate issuer

246. The Public key generated with the Private Key on a key generation and custody device is delivered to the Certification Authority sending a certification request.

6.1.4. CA public key delivery to relying parties

247. See the relevant section in the GCPS

6.1.5. Key sizes and algorithms used

248. The algorithm used is RSA with SHA-256.

249. As for key size, depending on each case, that is:

- Root FNMT CA keys: 4096 bits.
- Subordinate AC Representación keys*:* 2.048 bits.
- *Electronic Signature Certificate* Keys*:* 2.048 bits.
- *Entity Seals:* 2.048 bits

6.1.6. Public key parameters generation and quality checking

250. See the relevant section in the GCPS

6.1.7. Key usage purposes (KeyUsage field X.509v3)

251. FNMT *Certificates* include the extension Key Usage and, as appropriate, Extended Key Usage, indicating *Key* usage purposes.

252. The root FNMT CA *Certificate Key* usage purposes are to sign/seal Subordinate FNMT CA *Certificates* and ARLs.

253. The *Certificate* usage purpose of Subordinate FNMT CAs issuing *Electronic Signature* and *Electronic Seal Certificates* is exclusively to sign/seal end-entity Certificates and CRLs.

254. The *Electronic Signature Certificates* key usage purposes are signature, authentication and encryption. These *Certificates* extended key usage include Client-Authentication, Adobe Authentic Documents Trust and Document Signing.

255. The *Entity Seal* usage purposes are signature, authentication and encryption. Entity Seals include the extended key usages Client-Authentication, Adobe Authentic Documents Trust and Document Signing

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic module standards and controls

256. See the relevant section in the GCPS

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

257. See the relevant section in the GCPS

6.2.3. Private Key escrow

258. Copying, safeguarding or recovery of FNMT-RCM Certification Authority Private Keys is exclusively controlled by authorised personnel, using at least dual control and in a secure environment.

6.2.4. Private Key backup

259. See the relevant section in the GCPS

6.2.5. Private Key archival

260. See the relevant section in the GCPS

6.2.6. Private Key transfer into or from a cryptographic module

261. See the relevant section in the GCPS

6.2.7. Private Key storage on cryptographic module

262. See the relevant section in the GCPS

6.2.8. Activating Private Keys

263. Certification Authority Private Keys are generated and held securely by a cryptographic device meeting the FIPS PUB 140-2 Level 3 security requirements.

264. The Certification Authority's Private Keys are activated and used based on management and operation role segmentation implemented by FNMT-RCM, including multi-person access based on cryptographic cards and related PINs based on an M out of N (2 out of 5) simultaneous use pattern.

6.2.9. Deactivating Private Keys

265. See the relevant section in the GCPS.

6.2.10. Destroying Private Keys

266. FNMT-RCM will destroy or appropriately store the Trust Service Provider's Keys when their validity period is over, in order to prevent their inappropriate use.

6.2.11. Cryptographic module capabilities

267. See the relevant section in the GCPS.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key archival

268. See the relevant section in the GCPS

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

269. Operational periods for the Certificates and their associated Keys:

- Root FNMT CA *Certificate* and Key pair: until 1 January 2030.
- *Certificate* of the Subordinate CA issuing *Electronic Signature* and Key pair: until 31 December 2029.
- *Electronic Signature Certificates* and Key pair: not in excess of 2 years.
- *Entity Seals* and Key pair: not in excess of 3 years.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

270. Key activation data generation for both the root FNMT CA and the subordinate CA issuing Electronic Signature and Electronic Seal Certificates takes place during those Certification Authorities' Key generation ceremony.

6.4.2. Activation data protection

271. The Certification Authority's Private Key activation data is protected, as described in section "6.2.8 Activating Private Keys" above, with multi-person access based on cryptographic cards and related PINs based on an M out of N (2 out of 5) simultaneous use pattern.

6.4.3. Other aspects of activation data

272. No estipulados.

6.5. COMPUTER SECURITY CONTROLS

273. See the relevant section in the GCPS

6.5.1. Specific computer security technical requirements

274. See the relevant section in the GCPS

6.5.2. Computer security rating

275. See the relevant section in the GCPS

6.6. LIFE CYCLE TECHNICAL CONTROLS

276. See the relevant section in the GCPS

6.6.1. System development controls

277. See the relevant section in the GCPS

6.6.2. Security management controls

278. See the relevant section in the GCPS

6.6.3. Life cycle security controls

279. See the relevant section in the GCPS

6.7. NETWORK SECURITY CONTROLS

280. See the relevant section in the GCPS

6.8. TIME-STAMPING

281. See the relevant section in the GCPS

6.9. OTHER ADDITIONAL CONTROLS

282. See the relevant section in the GCPS

6.9.1. Control of the ability to provide services.

283. See the relevant section in the GCPS

6.9.2. Control of systems development and computer applications

284. See the relevant section in the GCPS

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

285. *Electronic Signature Certificates* are issued as "qualified" *Certificates* in accordance with European standards ETSI IN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI IN 319 412-2 "Certificate profile for certificates issued to natural persons".

286. *Entity Seals* are issued as "qualified" Certificates in accordance with European standards ETSI IN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI IN 319 412-3 "Certificate profile for certificates issued to legal persons".

7.1.1. Version number

287. Electronic Signature Certificates conform to standard X.509 version 3.

7.1.2. Certificate extensions

288. The document describing the profile of *Electronic Signature and Electronic Seal Certificates* issued under this policy, including all extensions, is published at http://www.cert.fnmt.es/dpcs/ .

7.1.3. Algorithm object identifiers

289. The corresponding object identifier (OID) for the cryptographic algorithm used (SHA-256 with RSA Encryption) is 1.2.840.113549.1.1.11.

7.1.4. Name Forms

290. *Electronic Signature and Electronic Seal Certificate* encoding is based on the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Except where otherwise indicated in the relevant fields, the fields defined in the *Certificate* profile use UTF8String encoding.

291. The document describing the profile of *Electronic Signature and Electronic Seal Certificates* issued under this policy, including all extensions, is published at http://www.cert.fnmt.es/dpcs/.

7.1.5. Name constraints

292. The distinguished name (*DN*) assigned to the *Subject* of the *Certificate* under this *SPPS* shall be unique and be composed as defined in the *Certificate* profile.

7.1.6. Certificate policy object identifier

293. The *Electronic Certificate and Electronic Seal Signature* policy object identifier (OID) is defined in section "1.2 Document name and identification" above.

7.1.7. Usage of policy constraints extension

294. The root CA *Certificate* "Policy Constraints" extension is not used.

7.1.8. Policy qualifiers syntax and semantics

295. The "Certificate Policies" extension includes two "Policy Qualifier" fields":

- CPS Pointer: contains the URL where the *Certification Policies* and *Trust Service Practices* applicable to this service are posted.
- User notice: contains wording that may be displayed on the *Certificate* user's screen during verification.

7.1.9. Processing semantics for the critical certificate policies extension

296. The "Certificate Policy" extension includes the policy OID field, which identifies the policy associated with the *Certificate* by FNMT-RCM, as well as the two fields referred to in the preceding section.

7.2. CRL PROFILE

7.2.1. Version number

297. The CRL profile conforms to standard X.509 version 2.

7.2.2. CRL and CRL entry extensions

298. The CRL profile has the following structure:

Table 3 – CRL Profile

Fields and extensions	Value
Version	V2
Signature Algorithm	Sha256WithRSAEncryption
CRL number	Incremental value
Issuer	Issuer DN
Issuance date	Tiempo UTC de emisión.
Date of next upgrade	Issuance date + 24 hours
Authority key identifier	Issuer key hash
Distribution Point	Distribution point URLs and CRL scope
ExpiredCertsOnCRL	CA's NotBefore
Revoked Certificates	Certificate revocation list, containing at least serial number and revocation date for each entry

7.3. OCSP PROFILE

7.3.1. Version number

299. See the relevant section in the GCPS

7.3.2. OCSP extensions

300. See the relevant section in the GCPS

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

301. The *Certificate* issuance system is audited on a yearly basis in conformity with European standards ETSI EN 319 401 "General Policy Requirements for Trust Service Providers" and ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates".

302. In addition, the *Certificates* are deemed to be qualified *Certificates* and the audit therefore ensures compliance with the requirements set in European standard ETSI IN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates".

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

303. Audit plans will be regularly prepared, covering at least the following actions:

- Risk analysis as established in the Information Security Management System: Annual review and full analysis every three (3) years.
- Information Security Management System Review in conformity with UNE-ISO/IEC 27001 "Information Security Management Systems (ISMS). Requirements".
- Quality: ISO 9001: A partial annual external audit plus an annual internal preparatory audit and a full external audit every three (3) years, to maintain the certification.
- Data protection: An internal audit every two (2) years undertaken by the Information Systems Department.

304. The Certification Authority issuing the Electronic Signature Certificates and Entity Seals is subject to regular audits, respectively in accordance with European standard ETSI IN 319 401 "General Policy Requirements for Trust Service Providers", ETSI IN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI IN 319 412-2 "Certificate profile for certificates issued to natural persons" or ETSI IN 319 412-3 "Certificate profile for certificates issued to legal persons". The audit is carried out on a yearly basis by an external accredited firm.

- FNMT-RCM information systems used to provide Trust Services are audited once every two (2) years in conformity with the provisions of the National Security Scheme (Royal Decree 3/2010, 8 January, regulating the National Security Scheme for E-Government).

8.2. QUALIFICATIONS OF ASSESSOR

305. See the relevant section in the GCPS

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTINTY

306. See the relevant section in the GCPS

8.4. TOPICS COVERED BY ASSESSMENT

307. See the relevant section in the GCPS

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

308. See the relevant section in the GCPS

8.6. COMMUNICATION OF RESULTS

309. See the relevant section in the GCPS

8.7. AUTOEVALUATION

310. See the relevant section in the GCPS

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

311. The FNMT-RCM may apply rates and payment means which it considers appropriate at any time by issuing the *Certificates*. The price and terms of payment of the *Certificates* may be consulted on the website of the FNMT - RCM or will be provided by Commercial area on request to the email address comercial.ceres@fnmt.es .

312. See the relevant section in the GCPS

9.1.1. Certificate issuance or renewal fees

313. See the relevant section in the GCPS

9.1.2. Certificate access fees

314. No stipulation.

9.1.3. Revocation or status information access fees

315. FNMT-RCM offers CRL or OCSP certificate status information services free of charge.

9.1.4. Fees for other services

316. See the relevant section in the GCPS

9.1.5. Refund policy

317. FNMT-RCM has a refund policy whereby a refund request may be made within the set withdrawal period, and accepts that this will result in automatic revocation of the certificate. The procedure is published at the FNMT-RCM website.

9.2. FINANCIAL RESPONSIBILITY

318. See the relevant section in the GCPS

9.2.1. Insurance coverage

319. See the relevant section in the GCPS

9.2.2. Other assets

320. See the relevant section in the GCPS

9.2.3. Insurance or warranty coverage for end-entities

321. See the relevant section in the GCPS

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

322. See the relevant section in the GCPS

9.3.1. Scope of confidential information

323. See the relevant section in the GCPS

9.3.2. Information not within the scope of confidential information

324. See the relevant section in the GCPS

9.3.3. Responsibility to protect confidential information

325. See the relevant section in the GCPS

9.4. PRIVACY OF PERSONAL INFORMATION

326. See the relevant section in the GCPS

9.4.1. Privacy plan

327. See the relevant section in the GCPS

9.4.2. Information treated as private

328. See the relevant section in the GCPS

9.4.3. Information not deemed private

329. See the relevant section in the GCPS

9.4.4. Responsibility to protect private information

330. See the relevant section in the GCPS

9.4.5. Notice and consent to use private information

331. See the relevant section in the GCPS

9.4.6. Disclosure pursuant to judicial or administrative process

332. See the relevant section in the GCPS

9.4.7. Other information disclosure circumstances

333. See the relevant section in the GCPS

9.5. INTELLECTUAL PROPERTY RIGHTS

334. See the relevant section in the GCPS

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA representations and warranties

335. FNMT-RCM's representations and warranties as *Trust Service Provider* to the *Signatory*, and to the other members of the *Electronic Community*, shall be mainly set out in the document containing the terms of use or the *Certificate* issuance agreement, and, secondarily, in this *Certification Policy and Practice Statement*.

336. FNMT-RCM, through the *Registry Office* shall be responsible for properly identifying the *Represented entity* and the *Representative*, verifying the extrinsic legality of the documents provided to accredit the scope of their representation, including an indication of this information in the *Certificate*.

337. During the registration process for the *Representative Certificates for Sole and Joint Administrators*, verify the information related to powers of representation (sole or joint administrator) of the *Representative*, as well as the existence and legal entity of the entity, according to the information supplied by the CORPME. All of these verifications will be carried out in accordance with the *Specific Certification Practices* expressed in this document, and in accordance with the registration protocols and procedures of the FNMT-RCM.

338. FNMT-RCM meets the technical requirements for qualified *Certificate* issuance specified in standard ETSI EN 319 411 and agrees to continue complying with that standard or any replacement standards.

339. See the relevant section in the GCPS

9.6.2. RA representations and warranties

340. In addition to the participants' representations and warranties set out herein and in the GCPS, *Registration Offices* have the following obligations:

i) Certifiably verify the identity and any personal circumstances of the *Applicants* of the relevant *Certificates* for the purposes of the *Certificates*, using any of the means permitted by Law, and in accordance with the provisions in the *GCPS*, and specifically in this *Specific Certification Practices Statement*.

ii) Conserve all of the information and documentation related to the *Natural Person Certificates*, whose application, renewal or revocation it manages, for the period of time established in the legislation in effect.

iii) Allow the FNMT-RCM access to the files and to audit its procedures in relation to the data obtained in its role as a Registry Office.

iv) Inform the FNMT-RCM of any aspect that affects the *Certificates* issued by said Entity (eg: requests for issuance, renewal ...).

v) Notify the FNMT-RCM promptly of the applications for the issuing of *Certificates*.

vi) In regard to the expiration of the validity of the *Certificates :*

1. Duly verify the causes for the revocation that could affect the validity of the *Certificates*.

2. Notify the FNMT-RCM promptly of the applications for the revocation of the *Certificates*.

vii) In regard to the Protection of personal information, the provisions in the corresponding section of the *GCPS* shall apply.

viii) In regard to the Protection of personal information, the provisions in the corresponding section of the *GCPS* shall apply.

341. In any case, the FNMT-RCM may bring suit against the Registry Office that carried out the identification procedure, initiating the corresponding actions, if the cause of the damages originated through the culpable or negligent actions of the Registry Office.

342. See the relevant section in the GCPS

9.6.3. Subscriber representations and warranties

343. The *Applicant* shall be responsible for guaranteeing that the information submitted during the application for the *Certificate* is true and the *Certificate* application and download are realized with a high level of confidence, under his sole control.

344. Not request *Certificates* containing marks, names, or rights that are protected by industrial or intellectual property laws that the party in question does not hold, licence, or have demonstrable authorization to use.

345. *Applicant* shall hold the FNMT-RCM harmless and defend at his/her own expense against any action that may be undertaken against the Entity as a result of false information provided during the aforementioned *Certificate* issuing procedure, or against any damages suffered by the FNMT-RCM as a result of an action or omission of the *Applicant*.

346. In addition to the obligations and responsibilities of the parties listed in this the *GCPS*, the *Subscriber* of the C*ertificate*, as the signer of the *Certificate* and the *Keys*, has the following obligations:

- Not use the *Certificate* outside of the limitations specified in these *Specific Certification Practices and Policy*.
- Adequately store the *Certificate* and the *Signature Creation Data*, and in such case, the *Certificate* support or card, providing the means necessary to prevent their use by persons other than the *Holder* or the legitimate possessor of the *Certificate*..
- Not use the *Certificate* when any of the information included in the *Certificate* is incorrect or inaccurate, or there are security reasons that advise against the use of the *Certificate*.
- Notify the FNMT-RCM of the loss, theft, or suspected theft of the *Certificate*, the *Signature Creation Data*, the *Certificate* support or card of the *Holder*, in order to initiate, in such case, the process to revoke the *Certificate*.
- Act diligently with respect to the custody and conservation of the *Signature creation data* or any other sensitive information such as *Keys*, *Certificate* activation codes, access words, personal identification numbers, etc., as well as the *Certificate* supports, which in all cases include the non-disclosure of all of the aforementioned information.
- Understand and comply with the conditions of use of the *Certificate* specified in the usage conditions and in the *Certification Practices Statement*, and specifically the limitations on the use of the *Certificates*.
- Understand and comply with the modifications that are made to the *Certification Practices Statement*.

347. The *Subscriber* shall be responsible for notifying the FNMT-RCM regarding any variation in the status or information in regard to the information reflected in the *Certificate*, to revoke and reissue the *Certificate*.

348. Likewise, the *Subscriber* shall be responsible in relation to the members of the *Electronic Community* and other User Entities, or in such case, to third parties, for improper use of the *Certificate*, or false information in it, or actions or omissions that cause damages to the FNMT-RCM or third parties.

349. The *Subscriber* shall therefore be responsible and obliged not to use the *Certificate* if the *Trust Services Provider* has terminated its activity as a *Certificate* issuing Entity and the substitution stipulated by Law has not taken place. In any case, the *Subscriber* shall not use the *Certificate* in the cases in which the *Signature / Seal Creation Data* of the Provider may be threatened and/or compromised, and the Provider has communicated this, or in such case, if the *Subscriber* has become aware of these circumstances.

9.6.4. Relying party representations and warranties

350. See the relevant section in the GCPS

9.6.5. Representations and warranties of other participants

351. The CORPME, for the *Representative Certificates for Sole and joint Administrators*, will be responsible for the transmission of the information provided by the mercantile registers that hold the information that is presumed to be true in regard to the powers of representation (sole or joint administrator) of the *Representative* of the *Certificate*, as well as the existence of the *Represented entity* and its legal entity, in accordance with the information included in the Mercantile Register and that is made available to the FNMT-RCM.

352. The regime for the distribution of liability between the FNMT-RCM and the CORPME in relation to the information exchanged between them and the time covered in the issuing of the *Certificates*, and in such case, the revocation of the *Certificates*, shall be defined in the corresponding agreement formalized for this purpose between the two institutions.

9.7. DISCLAIMER OF WARRANTIES

353. No stipulation.

9.8. LIMITATIONS OF LIABILITY

354. The FNMT-RCM shall not be liable for any damages caused to the *Represented entity* or to third parties by the *Applicant* should the *Applicant* infringe on the obligations to provide credible documentation or if the documentation provided contains inaccuracies, errors, or false information, and the *Certificate* is issued. Nor shall the FNMT-RCM shall be liable if the *Representative* uses the *Certificate* unduly, in the case of invalidation, insufficient legal capacity, expiration, revocation, extinguishing of powers, or if the *Representative* uses it beyond its initial scope of application.

355. The FNMT-RCM is responsible for verifying that the powers of the *Representative* are in force in the databases of the Professional Association of Property and Mercantile Registries of Spain (CORPME) (entry as sole or joint administrator) for the *Represented entity*, as well

as the existence of the *Entity* in question and its legal entity at the time of the accreditation of the personal identity of the *Representative*.

356. The FNMT-RCM is limited only to express the information regarding the identity of the *Representative*, his/her powers of representation (sole or joint administrator) and the identity of the represented company, in an electronic *Certificate*. Under no circumstances will the FNMT-RCM be liable for errors or discrepancies between the information provided by the CORPME and reality.

357. See the relevant section in the GCPS

9.9. INDEMNITIES

358. See the relevant section in the GCPS

9.9.1. CA indemnity

359. No stipulation.

9.9.2. Subscribers indemnity

360. No stipulation.

9.9.3. Relying parties indemnity

361. No stipulation.

9.10. TERM AND TERMINATION

9.10.1. Term

362. This *Certification Policy and Practice Statement* shall enter into force upon being published.

9.10.2. Termination

363. This *Certification Policy and Practice Statement* shall be repealed when a new version of the document is published. The new version shall fully supersede the previous document. FNMT-RCM agrees to review that Statement on a yearly basis.

9.10.3. Effect of termination and survival

364. For valid Certificates issued under a previous Certification Policy and Practice Statement, the new version will prevail over the previous version to the extent not in conflict therewith.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

365. See the relevant section in the GCPS

9.12. AMENDMENTS

9.12.1. Procedure for amendment

366. See the relevant section in the GCPS

9.12.2. Notification mechanism and period

367. See the relevant section in the GCPS

9.12.3. Circumstances under which OID must be changed

368. See the relevant section in the GCPS

9.13. DISPUTE RESOLUTION PROVISIONS

369. See the relevant section in the GCPS

9.14. GOVERNING LAW

370. See the relevant section in the GCPS

9.15. COMPLIANCE WITH APPLICABLE LAW

371. FNMT-RCM declares that it complies with the applicable law.

9.16. MISCELLANEOUS PROVISIONS

372. See the relevant section in the GCPS

9.16.1. Entire agreement

373. See the relevant section in the GCPS

9.16.2. Assignment

374. See the relevant section in the GCPS

9.16.3. Severability

375. See the relevant section in the GCPS

9.16.4. Enforcement (attorneys' fees and waiver of rights)

376. See the relevant section in the GCPS

9.16.5. Force Majeure

377. See the relevant section in the GCPS

9.17. OTHER PROVISIONS

378. None stipulated.