Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERTIFICATION POLICIES AND PRACTICES OF ENTITY SEALS

	NOMBRE	FECHA
Prepared by:	FNMT-RCM	19/01/2026
Revised by:	FNMT-RCM	19/01/2026
Approved by:	FNMT-RCM	19/01/2026

Version	Date	Description
1.0	19/01/2026	Document creation

Referencia: DPC/CPSEL0100/SGPSC/2026

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 *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 *Entity Seal* Certificates, issued by the FNMT-RCM which 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).

1.2. DOCUMENT NAME AND IDENTIFICATION

4. 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.

5. 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.

6. 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 *Entity Seals*.

7. 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 Entity Seals*

Reference / OID[1]: 1.3.6.1.4.1.5734.3.11.4.

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

Name: *Certification Policy for Entity Seals G2*

Reference / OID: 1.3.6.1.4.1.5734.3.22.1.0

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

Version: 1.0

Date of issue: 19/01/2026

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

Related CPS: Trust Services Practices and Electronic Certification General Statement of the FNMT-RCM

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

[1] *Note: The OID or policy identifier is a reference that is included in the Certificate in order to determine a set of rules that indicate the applicability of a particular type of Certificate to the Electronic Community and/or application class with common security requirements..*

8. 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*.

9. This *Specific Certification Practices Statement* applies to *Entity Seals* and will take precedence over the provisions in the main body of the *GCSP*

10. 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

11. 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

12. 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, RSA hierarchy. 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 RAIZ FNMT-RCM 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, RSA hierarchy: 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

Subordinate CA Certificate	
Key Identifier	DC 50 96 9F D7 31 89 C9 11 E4 EF 96 5F F6 5F 82 52 46 62 53

c) Root Certification Authority, Elliptic Curve hierarchy: this Authority issues subordinate Certification Authority *Certificates* only using elliptic curve cryptography. This CA's root *Certificate* is identified by the following information

Table 3 – Root "AC RAIZ FNMT-RCM G2"

AC FNMT raíz's Certificate	
Subject	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM, C=ES
Issuer	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM, C=ES
Serial number (hex)	1F B6 4F 91 9E C5 01 EA B1 21 28 BB 11 7A 00 3C 7C 5A EF 1A
Validity	Not before: 10 October 2024. Not after: 04 October 2049
Public key length	EC 384 bits (P-384)
Signature Algorithm	ecdsa-with-SHA384
Key Identifier	E2 29 99 47 2A FF 5B 26 8A C8 34 41 66 45 AF 52 3A 08 F1 80

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

Table 4 – Subordinate CA Certificate

Subordinate CA Certificate	
Subject	CN=AC ENTIDADES G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM,C=ES

Subordinate CA Certificate	
Issuer	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM, C=ES
Serial Number (hex)	18 BF C8 71 81 3B C9 80 31 03 F1 5B 70 50 70 C0 56 20 4F 3D
Validity	Not before: 10 October 2024. Not after: 07 October 2039
Public key length	EC 256 bits (P-256)
Signature Algorithm	ecdsa-with-SHA384
Key Identifier	E5 36 ED E0 98 12 92 DA 14 1B AE E1 97 50 98 FF 05 C9 5B 30

1.3.2. Registration Authority

13. 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.

14. 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

15. *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

16. 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

17. No stipulation.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

18. The *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 EN 319 412-3 "Certificate profile for certificates issued to legal persons".

1.4.2. Prohibited certificate uses

19. 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.*

20. 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

21. 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

22. 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

23. 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

24. 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

25. Through its Trust Service Provider Management Committee, FNMT-RCM oversees compliance with the Certification Policy and Practice Statements. It approves, reviews, and updates it at least every 365 days to keep it aligned with the latest version of the applicable requirements, increasing the version number and adding a change log entry with the date, even if no other changes were made to the document.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

26. 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:

- *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.
- *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.
- *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.

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

1.6.2. References

27. 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

28. 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

29. 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

30. 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.

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

2.4. ACCESS CONTROLS ON REPOSITORIES

32. 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

33. *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

34. 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.

35. In processing proof of identity prior to issuing *Entity Seals,* 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

36. 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).

37. 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

38. 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

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

3.1.5. Uniqueness of names

40. 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

41. 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

42. 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

43. FNMT-RCM, as a *Trust Services Provider*, before issuing the *Certificate*, it 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*, through the use of 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*.

44. 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).

45. 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).

46. 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.

47. 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.

48. 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.

49. 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

50. The FNMT-RCM, as a Trust Services Provider, before issuing the *Entity Seal Certificate*, it will identify the *Applicant* by verifying their identity through the use of a valid Qualified Certificate of electronic signature that confirms the identity of the natural person applying.

3.2.4. Non-verified Subscriber information

51. All information included in the electronic *Entity Seal Certificate* is verified by the *Registration Authority*.

3.2.5. Validation of the authority

52. The RA of the FNMT-RCM verifies that the *Applicant* has been granted sufficient representation capacity through the electronic signature of the application form, as described in section 3.2.3 of this DPPP, accepting the use of a qualified *Certificate* of sole or joint administrator representative of the subscribing legal person or a qualified *Certificate* of *Personnel at the service of the Public Administration*, for whose issuance the capacity of representation has been accredited.

53. When the aforementioned form is signed by a qualified *Certificate* different from those mentioned in the previous section, the RA of the FNMT-RCM is able to verify the power of representation of the signatory of the request by consulting official records (Commercial Registry, Official Gazettes, etc., depending on the nature of the representation). In the event that the results of these consultations do not provide sufficient evidence of representation, the RA of the FNMT-RCM will contact the *Subscriber* to collect such evidence.

3.2.6. Criteria for interoperation

54. 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

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

56. 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

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

58. 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

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

3.3.2. Requirements for re-key after certificate revocation

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

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

61. 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.

62. 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

63. Only *Subscriber* representatives *or* individual duly authorized to request *Certificates* on behalf of the applicant may apply for *Certificates* issued under these policies.

4.1.2. Registration process and responsabilities

64. 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.

65. 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

66. 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.

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

68. Section 9.6 "Respresentation and warranties" of this document establishes the responsibilities of the parties involved in this process

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing identification and authentication functions

69. 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. FNMT-RCM will admit, in any case, the function and report made by the *Registry Office*.

4.2.2. Approval or rejection of certificate applications

70. The Registration Authority involved in the certificate issuance process is always the FNMT-RCM itself and, therefore, does not delegate validation to any other RA.

71. Once the FNMT-RCM Registration Authority has carried out the necessary verifications regarding proof of possession of the private key by the Subscriber's Representative, as well as the authentication of the Organization's identity and that of the Certificate Applicant, as described in section "3.2 Initial Identity Validation" of this DPPP, it will determine whether to approve or reject the application.

72. If the information is incorrect or cannot be confirmed, the RA will reject the application and reserves the right not to disclose the reasons for the denial. Otherwise, the certificate will be issued.

73. 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.

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

4.2.3. Time to Process Certificate Applications

75. 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. The FNMT-RCM will provide the *Applicant* with a mechanism to download the *Certificate*.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions During Issuance

76. 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.

77. The issuance of Entity Seal Certificates involves the generation of electronic documents that confirm the identity of the Subscriber, as well as the identity of the natural person representing the subscribing entity, and verify their correspondence with 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.

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

79. 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*.

80. 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.

81. 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:

- in the DirectoryName subfield the Company name, component denomination and the Tax number of the *Represented entity.*

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

82. 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

83. 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

84. 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.

85. In this guided process, the *Subscriber's Representative* will be asked to enter the component's name and the corresponding application code obtained in this process.

86. If the *Entity Seal Certificate* has not been generated yet for any reason, the process will inform the applicant of this.

4.4.2. Publication of the certificate by the CA

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

4.4.3. Notification of issuance to other entities

88. 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

89. 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.

4.5.2. Relying party public key and certificate usage

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

4.6. CERTIFICATE RENEWAL

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

4.6.1. Circumstance for certificate renewal

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

4.6.2. Who may request renewal

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

4.6.3. Processing certificate renewal requests

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

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

96. 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

97. 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

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

4.7. CERTIFICATE RE-KEY

99. Under these Certification Policies, Certificate re-key is always carried out issuing new keys, following the same process described for a new Certificate to be issued..

4.7.1. Circumstances for certificate re-key

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

4.7.2. Who may request re-key

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

4.7.3. Processing certificate re-keying requests

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

4.7.4. Notification of certificate re-key

103. 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

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

4.7.6. Publication of the re-keyed certificate

105. 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

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

4.8. CERTIFICATE MODIFICATION

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

4.8.1. Circumstance for certificate modification

108. The modification is not stipulated.

4.8.2. Who may request certificate modification

109. The modification is not stipulated.

4.8.3. Processing certificate modification requests

110. The modification is not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

111. The modification is not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

112. The modification is not stipulated.

4.8.6. Publication of the modified certificate by the CA

113. The modification is not stipulated.

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

114. The modification is not stipulated.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

115. *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.

116. 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*.

117. 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

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

119. The following admissible grounds for a *Certificate* to be revoked:

a) Revocation request by authorised persons. This request shall in any case be based on:

- Third-party use of the *Private Key* associated with the *Certificate.*
- Breach or compromise of the *Signature Creation Data* or of the private key associated with the *Certificate.*
- The failure to accept new terms resulting from the issuance of new *Certification Policy and Practice Statements*, during a period of one month after publication.

b) Court or administrative ruling ordering revocation.

c) Termination or dissolution of the *Subscriber's* legal personality.

d) Death or subsequent total or partial incapacity of the *Signatory* or of the *Subscriber's* representative.

e) Inaccurate data supplied by the *Applicant* to obtain the *Certificate*, or alteration of the data supplied to obtain the *Certificate* or change of the circumstances checked for the *Certificate* to be issued, and in relation to the position held or powers conferred, to the extent that the *Certificate* no longer reflects the true facts.

f) Breach of a material obligation provided for in this *Certification Policy and Practice Statement* by the *Certificate Signatory* or *Applicant*, or by a *Registration Office* if, in the latter case, that may have affected the procedure to issue the *Certificate*.

g) Breach or compromise of the Private Key Signature Creation Data.

h) Termination of the agreement entered into between the *Signatory* or the Subscriber and FNMT-RCM.

i) Breach of a material obligation provided for in this *Certification Policy and Practice Statement* by a *Registration Office* where that may have affected the process to issue the *Certificate*.

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

k) Failure to comply with the requirements defined by the audit schemes to which the Certification Authority that issues the Certificates covered by this CPS determines, with special attention to those of algorithms and key sizes, which pose an unacceptable risk to the interests of parties that rely on these Certificateson these Certificates

120. 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.

121. 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.
- The revocation should have been carried out due to the termination of the contract signed with the *Subscriber*.
- 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*).

122. 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.

123. 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

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

4.9.2. Who can request revocation

125. 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*.

126. FNMT-RCM may revoke the *Certificates* of its own accord in the events referred to in this Certification Policy and Practice Statement.

4.9.3. Procedure for revocation request

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

128. Revocation may be processed continuously 24x7 through the telephone Revocation Service available to users for such purpose, and revocation of the Certificate is guaranteed within less than 24h.

129. 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.

130. 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.

131. If the person who is requesting revocation cannot provide the required data or it is resolved that this person does not fulfill the requirements to ask for a revocation, the request for the revocation will be dismissed.

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

133. 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.

134. 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

135. 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

136. 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

137. 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.

138. 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.

139. 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

140. 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

141. *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

142. 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

143. 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

144. 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

145. Not defined.

4.9.12. Special requirements related to key compromise

146. See the relevant section in the GCPS

4.9.13. Circumstances for suspension

147. Certificate suspension is not supported.

4.9.14. Who can request suspension

148. Certificate suspension is not supported.

4.9.15. Procedure for suspension request

149. Certificate suspension is not supported.

4.9.16. Limits on Suspension Period

150. Certificate suspension is not supported.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational characteristics

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

4.10.2. Service availability

152. 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

153. Not stipulated.

4.11. END OF SUBSCRIPTION

154. 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.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policy and practices

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

4.12.2. Session key encapsulation and recovery policy and practices

156. No stipulation.

5. PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

157. See the relevant section in the GCPS

5.1. PHYSICAL SECURITY CONTROLS

158. See the relevant section in the GCPS

5.1.1. Site location and construction

159. See the relevant section in the GCPS

5.1.2. Physical access

160. See the relevant section in the GCPS

5.1.3. Power and air conditioning

161. See the relevant section in the GCPS

5.1.4. Water exposures

162. See the relevant section in the GCPS

5.1.5. Fire prevention and protection

163. See the relevant section in the GCPS

5.1.6. Media storage

164. See the relevant section in the GCPS

5.1.7. Waste disposal

165. See the relevant section in the GCPS

5.1.8. Off-site backup

166. See the relevant section in the GCPS

5.2. PROCEDURAL CONTROLS

167. See the relevant section in the GCPS

5.2.1. Trusted roles

168. See the relevant section in the GCPS

5.2.2. Number of persons required per task

169. See the relevant section in the GCPS

5.2.3. Identification and authentication for each role

170. See the relevant section in the GCPS

5.2.4. Roles requiring separation of duties

171. See the relevant section in the GCPS

5.3. PERSONNEL CONTROLS

172. See the relevant section in the GCPS

5.3.1. Qualifications, experience, and clearance requirements

173. See the relevant section in the GCPS

5.3.2. Background check procedures

174. Véase el apartado correspondiente en la *DGPC*

5.3.3. Training requirements

175. Véase el apartado correspondiente en la *DGPC*

5.3.4. Retraining frequency and requirements

176. Véase el apartado correspondiente en la *DGPC*

5.3.5. Job rotation frequency and sequence

177. See the relevant section in the GCPS

5.3.6. Sanctions for unauthorized actions

178. Véase el apartado correspondiente en la *DGPC*

5.3.7. Independent contractor requirements

179. See the relevant section in the GCPS

5.3.8. Documentation supplied to personnel

180. See the relevant section in the GCPS

5.4. AUDIT-LOGGING PROCEDURES

181. See the relevant section in the GCPS

5.4.1. Types of events recorded

182. See the relevant section in the GCPS

5.4.2. Frequency of processing log

183. See the relevant section in the GCPS

5.4.3. Retention period for audit log

184. See the relevant section in the GCPS

5.4.4. Protection of audit log

185. See the relevant section in the GCPS

5.4.5. Audit log backup procedures

186. See the relevant section in the GCPS

5.4.6. Audit collection system (internal vs. external)

187. See the relevant section in the GCPS

5.4.7. Notification to event-causing subject

188. See the relevant section in the GCPS

5.4.8. Vulnerability assessments

189. See the relevant section in the GCPS

5.5. RECORDS ARCHIVAL

190. See the relevant section in the GCPS

5.5.1. Types of records archived

191. See the relevant section in the GCPS

5.5.2. Retention period for archive

192. See the relevant section in the GCPS

5.5.3. Protection of archive

193. See the relevant section in the GCPS

5.5.4. Archive backup procedures

194. See the relevant section in the GCPS

5.5.5. Requirements for time-stamping of records

195. See the relevant section in the GCPS

5.5.6. Audit collection system (internal vs. external)

196. See the relevant section in the GCPS

5.5.7. Procedures to obtain and verify archive information

197. See the relevant section in the GCPS

5.6. CA KEY CHANGEOVER

198. See the relevant section in the GCPS

5.7. COMPROMISE AND DISASTER RECOVERY

199. See the relevant section in the GCPS

5.7.1. Incident and compromise handling procedures

200. See the relevant section in the GCPS

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

201. See the relevant section in the GCPS

5.7.3. Entity Private Key compromise procedures

202. See the relevant section in the GCPS

5.7.4. Business continuity capabilities after a disaster

203. See the relevant section in the GCPS

5.8. TRUST SERVICE PROVIDER TERMINATION

204. See the relevant section in the GCPS

6. TECHNICAL SECURITY CONTROLS

205. 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

206. 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

207. No estipulation.

6.1.1.3 Subscriber key pair generation

208. 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

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

210. 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

211. 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

212. See the relevant section in the GCPS

6.1.5. Key sizes and algorithms used

213. The algorithms used in this CPS are:

- RSA with SHA 256.
- ECDSA with SHA-384 and ECDSA with SHA-256

214. Regarding Keys sizes:

- At least 2048 bits RSA keys
- At least 256 bits ECDSA keys

6.1.6. Public key parameters generation and quality checking

215. See the relevant section in the GCPS

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

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

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

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

219. The key usage purposes of *Electronic Seal Certificates* can be exclusively for encryption, authentication and signature purposes.

220. The details of end entity certificate's Profiles and Key usage purposes are defined in the Certificate Profiles Document available at http://www.cert.fnmt.es/dpcs/

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic module standards and controls

221. See the relevant section in the GCPS

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

222. See the relevant section in the GCPS

6.2.3. Private Key escrow

223. 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

224. See the relevant section in the GCPS

6.2.5. Private Key archival

225. See the relevant section in the GCPS

6.2.6. Private Key transfer into or from a cryptographic module

226. See the relevant section in the GCPS

6.2.7. Private Key storage on cryptographic module

227. See the relevant section in the GCPS

6.2.8. Activating Private Keys

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

229. 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 simultaneous use pattern.

6.2.9. Deactivating Private Keys

230. See the relevant section in the GCPS.

6.2.10. Destroying Private Keys

231. 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

232. See the relevant section in the GCPS.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key archival

233. See the relevant section in the GCPS

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

234. Operational periods for the *Certificates* and their associated *Keys*:

- RSA hierarchy
  - *Root FNMT CA Certificate and Key pair:* until 1 January 2030.
  - *Certificate of the Subordinate CA issuing Electronic Signature and Electronic Seal Certificates and Key pair:* until 31 December 2029.
  - *Electronic Seal Certificates and Key pair:* not in excess of 2 years.
- Elliptic curve hierarchy
  - Root FNMT CA *Certificate* and Key pair: until 4 October 2049.
  - El *Certificate* of the Subordinate CA issuing *Entity Seal Certificates* and Key pair: until 07 October 2039.
  - *Entity Seal Certificates and Key pair: not in excess of 3 years.*

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

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

6.4.2. Activation data protection

236. 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 simultaneous use pattern.

6.4.3. Other aspects of activation data

237. No estipulados.

6.5. COMPUTER SECURITY CONTROLS

238. See the relevant section in the GCPS

6.5.1. Specific computer security technical requirements

239. See the relevant section in the GCPS

6.5.2. Computer security rating

240. See the relevant section in the GCPS

6.6. LIFE CYCLE TECHNICAL CONTROLS

241. See the relevant section in the GCPS

6.6.1. System development controls

242. See the relevant section in the GCPS

6.6.2. Security management controls

243. See the relevant section in the GCPS

6.6.3. Life cycle security controls

244. See the relevant section in the GCPS

6.7. NETWORK SECURITY CONTROLS

245. See the relevant section in the GCPS

6.8. TIME-STAMPING

246. See the relevant section in the GCPS

6.9. OTHER ADDITIONAL CONTROLS

247. See the relevant section in the GCPS

6.9.1. Control of the ability to provide services.

248. See the relevant section in the GCPS

6.9.2. Control of systems development and computer applications

249. See the relevant section in the GCPS

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

250. *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

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

7.1.2. Certificate extensions

252. The document describing the profile of *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

253. The corresponding object identifier (OID) for the cryptographic algorithms are:

- RSA hierarchy
  - Algorithm *SHA-256 with RSA Encryption* with its corresponding OID 1.2.840.113549.1.1.11
- Elliptic Curve hierarchy:
  - Algorithm *SHA-384 with ECDSA Encryption* with its corresponding OID 1.2.840.10045.4.3.3
  - Algorithm *SHA-256 with ECDSA Encryption* with its corresponding OID 1.2.840.10045.4.3.2

7.1.4. Name Forms

254. *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.

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

7.1.5. Name constraints

256. 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

257. The *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

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

7.1.8. Policy qualifiers syntax and semantics

259. 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

260. 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

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

7.2.2. CRL and CRL entry extensions

262. The CRL profiles have the following structures:

Table 5 – CRLs Profiles

Fields and extensions	Value
Version	V2

Fields and extensions	Value
Signature Algorithm	Sha256WithRSAEncryption or Sha256WithECDSAEncryption
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

263. See the relevant section in the GCPS

7.3.2. OCSP extensions

264. See the relevant section in the GCPS

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

265. 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".

266. 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".

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

- Audit of the Information Security Management System in accordance with UNE-ISO / IEC 27001 "Information Security Management Systems. Requirements".
- Audit of the Privacy Information Management System in accordance with UNE-ISO/ IEC 27701 "Privacy Information Management Systems Requirements".
- Audit as ruled in the National Security Scheme (Royal Decree 311/2022, of May 3 , which regulates the National Security Scheme in the field of Electronic Administration).
- Audit of the Quality Management System according to ISO 9001.
- Audit of the Social Responsibility Management System in correspondence with IQNet SR10.
- Audit of the Business Continuity Plan according to ISO 22301.
- Audit in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/, and Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (RGPD / LOPD-GDD).

268. Risk analysis is also carried out, in accordance with the dictates of the Information Security Management System.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

269. The corresponding audit plans will be prepared periodically.

270. The Certification Authority issuing the *Electronic 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 319 412-3 "Certificate profile for certificates issued to legal persons". The audit is carried out on a yearly basis by an external accredited firm.

271. An independent auditor shall annually assess the CA's compliance with the requirements and practices established in this CPS.

272. The frequency of the rest of the additional audits will be in accordance with the provisions of the corresponding current regulations.

8.2. QUALIFICATIONS OF ASSESSOR

273. See the relevant section in the GCPS

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTINTY

274. See the relevant section in the GCPS

8.4. TOPICS COVERED BY ASSESSMENT

275. See the relevant section in the GCPS

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

276. See the relevant section in the GCPS

8.6. COMMUNICATION OF RESULTS

277. See the relevant section in the GCPS

8.7. AUTOEVALUATION

278. See the relevant section in the GCPS

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

279. 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 .

280. See the relevant section in the GCPS

9.1.1. Certificate issuance or renewal fees

281. See the relevant section in the GCPS

9.1.2. Certificate access fees

282. No stipulation.

9.1.3. Revocation or status information access fees

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

9.1.4. Fees for other services

284. See the relevant section in the GCPS

9.1.5. Refund policy

285. 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

286. See the relevant section in the GCPS

9.2.1. Insurance coverage

287. See the relevant section in the GCPS

9.2.2. Other assets

288. See the relevant section in the GCPS

9.2.3. Insurance or warranty coverage for end-entities

289. See the relevant section in the GCPS

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

290. See the relevant section in the GCPS

9.3.1. Scope of confidential information

291. See the relevant section in the GCPS

9.3.2. Information not within the scope of confidential information

292. See the relevant section in the GCPS

9.3.3. Responsibility to protect confidential information

293. See the relevant section in the GCPS

9.4. PRIVACY OF PERSONAL INFORMATION

294. See the relevant section in the GCPS

9.4.1. Privacy plan

295. See the relevant section in the GCPS

9.4.2. Information treated as private

296. See the relevant section in the GCPS

9.4.3. Information not deemed private

297. See the relevant section in the GCPS

9.4.4. Responsibility to protect private information

298. See the relevant section in the GCPS

9.4.5. Notice and consent to use private information

299. See the relevant section in the GCPS

9.4.6. Disclosure pursuant to judicial or administrative process

300. See the relevant section in the GCPS

9.4.7. Other information disclosure circumstances

301. See the relevant section in the GCPS

9.5. INTELLECTUAL PROPERTY RIGHTS

302. See the relevant section in the GCPS

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA representations and warranties

303. 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*.

304. 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*.

305. FNMT-RCM meets the technical requirements for qualified *Certificate* issuance specified in standard ETSI EN 319 411-2 and agrees to continue complying with that standard or any replacement standards.

306. See the relevant section in the GCPS

9.6.2. RA representations and warranties

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

- 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*.
- 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.
- 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.
- Inform the FNMT-RCM of any aspect that affects the *Certificates* issued by said Entity (eg: requests for issuance, renewal ...).
- Notify the FNMT-RCM promptly of the applications for the issuing of *Certificates*.
- In regard to the expiration of the validity of the *Certificates :*
    - Duly verify the causes for the revocation that could affect the validity of the *Certificates*.
    - Notify the FNMT-RCM promptly of the applications for the revocation of the *Certificates*.
- In regard to the Protection of personal information, the provisions in the corresponding section of the *GCPS* shall apply.
- In regard to the Protection of personal information, the provisions in the corresponding section of the *GCPS* shall apply.

308. 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.

309. See the relevant section in the GCPS

9.6.3. Subscriber representations and warranties

310. 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.

311. 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 to use the *Certificate* outside of the limitations specified in these *Specific Certification Practices and Policy*.
- Not to use the *Certificate* in the event that the *Trust Service Provider* that issued the certificate in question has ceased its activity as Certificate Issuer, in particular in any cases where the Supplier's Creation Data may be compromised, and this fact has been expressly communicated.
- Provide truthful information in any applications for *Certificates* and keep it updated, with all contracts being signed by an individual with sufficient capacity for such purpose.
- Not to request for the *Subject* of the certificate any distinctive signs, denominations or industrial or intellectual property rights of which it does not own, license, or have demonstrable authorisation for its use.
- Acting diligently with respect to the custody and preservation of the *Signature/Seal Creation data* or any other sensitive information such as *Keys, Certificate* activation codes, access words, personal identification numbers, etc., as well as the *Certificates* themselves, which includes, in any case, the commitment to maintain all mentioned data confidential.
- To be aware of and comply with the conditions of use of the *Certificates* provided for under the conditions of use and in the *Certification Practices Statement,* and, in particular, all applicable limitations of use of the Certificates
- Become aware of and comply all modifications that may arise in the *Certification Procedure Statement.*
- To request the revocation of the corresponding *Certificate,* according to the procedure described in this document, duly notifying the FNMT-RCM of the circumstances for revocation or suspected loss of *Confidentiality*, unauthorised disclosure, modification or use of the associated *Private keys,*
- Review the information contained in the *Certificate* and notify the FNMT-RCM of any error or inaccuracy.
- Verify the *Electronic signature* or *Advanced electronic seal* provided by the *Trust Service Provider* issuing any *Certificates* prior to trusting them.
- Diligently report any modification of the data provided in the application for the *Certificate* to the FNMT-RCM, requesting, when pertinent, the revocation of the same.
- To return or destroy the *Certificate* where it is so demanded by FNMT-RCM, and not to use it with the purpose of signing or identifying oneself electronically when the Certificate runs out or is revoked.

312. In any event, it shall remain the responsibility of the *Subscriber* to use appropriately use diligently guard the *Certificate,* according to the specific purpose and function for which it was issued, and to inform the FNMT-RCM regarding any potential variation of status or information with respect to that which is contained in the *Certificate,* so that it may be revoked and re-issued.

313. Likewise, Subscriber shall be answerable, in all cases, to the FNMT-RCM, the User Entities and, when applicable, to third parties, with regard to any improper use of the *Certificate* or for any inaccuracy or errors in the declarations contained in it, or for acts or omissions causing harm to the FNMT-RCM or third parties.

314. It will be the responsibility and, therefore, obligation of the *Subscriber* not to use the *Certificate* in the event that the *Trust Service Provider* has ceased in the activity as *Certification Entity* that made the issuance of the Certificate in question, and in the case that the subrogation detailed under the law is not performed. In any event, the *Subscriber* must not use the *Certificate* where the *Provider's Signature creation data* may be jeopardised and/or compromised and the Provider has notified this or, if applicable, has become aware of these circumstances.

315. The relationships of the FNMT-RCM and the *Subscriber* will be determined mainly, for the purposes of the use regime of the *Certificates*, through the document related to the conditions of use or, where appropriate, the contract for the issuance of the *Certificate* and in accordance with all contracts, agreements or relationship documents entered into between the FNMT-RCM and the corresponding Public Entity.

9.6.4. Relying party representations and warranties

316. See the relevant section in the GCPS

9.6.5. Representations and warranties of other participants

317. No stipulation.

9.7. DISCLAIMER OF WARRANTIES

318. No stipulation.

9.8. LIMITATIONS OF LIABILITY

319. 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.

320. See the relevant section in the GCPS

9.9. INDEMNITIES

321. See the relevant section in the GCPS

9.9.1. CA indemnity

322. No stipulation.

9.9.2. Subscribers indemnity

323. No stipulation.

9.9.3. Relying parties indemnity

324. No stipulation.

9.10. TERM AND TERMINATION

9.10.1. Term

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

9.10.2. Termination

326. 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

327. 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

328. See the relevant section in the GCPS

9.12. AMENDMENTS

9.12.1. Procedure for amendment

329. See the relevant section in the GCPS

9.12.2. Notification mechanism and period

330. See the relevant section in the GCPS

9.12.3. Circumstances under which OID must be changed

331. See the relevant section in the GCPS

9.13. DISPUTE RESOLUTION PROVISIONS

332. See the relevant section in the GCPS

9.14. GOVERNING LAW

333. See the relevant section in the GCPS

9.15. COMPLIANCE WITH APPLICABLE LAW

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

9.16. MISCELLANEOUS PROVISIONS

335. See the relevant section in the GCPS

9.16.1. Entire agreement

336. See the relevant section in the GCPS

9.16.2. Assignment

337. See the relevant section in the GCPS

9.16.3. Severability

338. See the relevant section in the GCPS

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

339. See the relevant section in the GCPS

9.16.5. Force Majeure

340. See the relevant section in the GCPS

9.17. OTHER PROVISIONS

341. None stipulated.