Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

# CERTIFICATION PRACTICES AND POLICIES STATEMENT ON CENTRALISED ELECTRONIC SIGNATURE CERTIFICATES FOR PUBLIC EMPLOYEES

| | NAME | DATE |
|---|---|---|
| Prepared by: | FNMT-RCM | 21/03/2021 |
| Reviewed by: | FNMT-RCM | 26/04/2021 |
| Approved by: | FNMT-RCM | 28/04/2021 |

| Version | Date | Description |
|---|---|---|
| 1.0 | 13/06/2018 | Certification Practices and Policies Statement on centralised electronic signature certificates for public employees |
| 1.1 | 21/09/2018 | Certificates will have a validity period of 2 years |
| 1.2 | 28/04/2021 | General review. Section 4.9.12: reference to DGPC |

**Reference:** DPC/DPCFCEP_0102/SGPSC/2021

**Document classified as:** *Public*

## Content

## Index of tables

# 1. INTRODUCTION

1. Article 81 of Law 66/1997 (30 December) on Tax, Administrative and Social Measures authorised the Spanish Mint to provide security services in communications through electronic, computer and telematic techniques and means. Paragraph one states the following:

   *"without prejudice to the powers attributed by the Law to administrative bodies with respect to the registration of applications, documents and communications, the Spanish Mint (FNMT) is authorised to provide the technical and administrative services necessary to guarantee the security, validity and effectiveness of the issuance and receipt of communications and documents through electronic, computer and telematic means in relations that take place*:

   *a) Between central government bodies or between those bodies and public entities related or attached to the central government, as well as between the latter entities.*

   *b) Between individuals or legal entities and the Central Government or public entities related or attached to the latter."*

2. Paragraph two stipulates the following:

   *"Furthermore, the FNMT is authorised to provide, if applicable, Regional Governments, local entities and public-law companies related or attached to them, with the services referred to in the preceding paragraph, in relations that take place between them through electronic, computer and telematic means, with the central government or with individuals and legal entities, provided the pertinent arrangements or agreements have previously been concluded."*

3. Law 11/2007 (22 June) on citizens' electronic access to public services established the right of citizens to enter into electronic relationships with Public Administrations. The legal framework resulting from the approval of Law 39/2015 (1 October) on the Common Administrative Procedure for Public Administrations and Law 40/2015 (1 October) on the Public Sector systematises all regulations on the administrative procedure, clarifying and including the content of Law 30/1992 (26 November) on Public Administrations and the Common Administrative Procedure and of the said Law 11/2007 (22 June). Moreover, Law 18/2011 (5 July) on the use of information and communication technologies in the Justice Administration regulates the identification and electronic signature systems used by the Justice Administration.

4. Electronic signature systems permitted under the current legal framework include *Electronic signature certificates for government employees*.

5. The FNMT-RCM has been issuing this type of Certificates as a means of identification and electronic signing since the said Law first came into force. However, many commercial applications used on a daily basis have evolved to the extent that they no longer allow cryptographic functionalities necessary for electronic signatures, generating the need for additional supplements and a high level of technical know-how on the part of system users.

6. Regulation (EU) No. 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 lays down a general legal framework for the use of *Electronic signatures*. The Regulation allows the creation of remote *Electronic signatures* in an electronic signature creation environment managed by a *Trust Service Provider* in the *Signatory*'s name.

## 1.1. PURPOSE

7. The purpose of this document is to provide public information on the conditions and features of the remote electronic signature service, or centralised electronic signature service, for *Government employees* provided by the FNMT-RCM as a *Trust Service Provider*. Specifically, this refers to the obligations the FNMT-RCM must fulfil in connection with:

- the management of *Signature creation and verification data* and *Certificates*, conditions applicable to the request, issuance, use and expiration of *Certificates* and related *Signature creation data*, and, if applicable, the existence of procedures for coordination with the relevant Public Registries that allow the immediate and confidential exchange of information on the validity of the powers stated in the *Certificates*, which must mandatorily be entered in such registers;
- the provision of a consultancy service on the validity status of the *Certificates.*

8. This document also includes, directly or by reference to the *FNMT-RCM Trust Services Practices and Electronic Certification General Statement*, to which this Statement relates, details of the liability regime applicable to the users of and/or persons that place their trust in the services referred to in the previous paragraph, security controls applied to procedures and facilities, which may be disclosed without harming their effectiveness, and secrecy and confidentiality rules, as well as matters related to the ownership of goods and assets, personal data protection and other informative aspects that should be made available to the general public.

## 1.2. DOCUMENT NAME AND IDENTIFICATION

9. The FNMT-RCM's *Certification Practices Statement* as a *Trust Service Provider* is formed by the common section of the *FNMT-RCM Trust Services Practices and Electronic Certification General Statement* (GCPS), since some action levels are the same for all the Entity's trust services, and by the specific sections of this document containing *Certification Policies and Specific Certification Practices*. Nonetheless, the *Issuance Law* for each type of *Certificate* or group of *Certificates* may stipulate special features applicable to the bodies, entities and personnel that use the FNMT-RCM's trust services.

10. Accordingly, the *FNMT-RCM Certification Practices Statement* is structured as follows:

a. Firstly, the ***Trust Services Practices and Electronic Certification General Statement***, which must be regarded as the main body of the *Certification Practices Statement*, describing the liability regime applicable to the members of the *Electronic Community*, security controls applied to the FNMT-RCM's procedures and facilities, which may be disclosed without harming their effectiveness, and secrecy and confidentiality rules, as well as matters related to the ownership of goods and assets, personal data protection and other informative aspects that should be made available to the general public, regardless of their role in the Electronic Community.

b. Moreover, for each trust service or set or group of *Certificates*, identified and distinguished from the rest by type and specific or distinctive regime, there is a specific ***Certification Policy*** describing the parties' obligations, restrictions on the use of the *Certificates* and responsibilities, and ***Specific Certification Practices*** that develop the terms defined in the relevant policy and contain additional or specific provisions with respect to the general provisions contained in the *Trust Services Practices and Electronic Certification General Statement.*

These *Certification Policies and Specific Certification Practices* specify the provisions of the main body of the *Trust Services Practices and Electronic Certification General Statement* and, therefore, form part of the General Statement; together, they form the FNMT-RCM's *Certification Practices Statement*. However, these policies and practices only apply to the set of *Certificates* characterised and identified in the relevant *Specific Certification Policies and Practices* and may also include special provisions brought in through the *Issuance Law* of the relevant *Certificate* or group of *Certificates*, if there are specific features or functionalities.

c. This document therefore represents the *Certification Policies and Specific Certification Practices* for *Centralised Signature Certificates.*

11. This document is entitled "*Certification Practices and Policies Statement on centralised electronic signature certificates for public employees*" and will be referred to henceforth in this document, with the scope described herein, as the "*Specific Practices and Policies Statement*" or by its acronym "*SPPS*".

12. These *Certification Policies and Specific Certification Practices* form part of the *Certification Practices Statement* and will prevail over the provisions of the main body of the *Trust Services Practices and Electronic Certification General Statement (GCPS)*.

13. In the event of a conflict between this document and the content of the *Trust Services Practices and Electronic Certification General Statement*, the provisions of this document will prevail.

14. This *Certification Policy* is identified as follows:

**Name**: Certification Policy on centralised electronic signature *Certificates* for public employees

**Reference / OID**[1]:

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

- 1.3.6.1.4.1.5734.3.3.10.1.

Policy type:

- QCP-n. OID: 0.4.0.194112.1.0

**Version**: 1.2

**Approval date**: 28/04/2021

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

**Related Certification Practices Statement**: FNMT-RCM Trust Services Practices and Electronic Certification General Statement

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

15. The centralised electronic signature *Certificate* for public employees is a certificate type designed to make signatures at a distance or in a server, i.e. the *Public and private keys* are not generated directly in the *Signatory's* Internet browser or in a different device held by the *Signatory*, and the *Certificate* is not downloaded; they are generated and stored in a Qualified Electronic Signature Creation Device (QSCD) owned by the FNMT-RCM. Additionally, the electronic signature is completed in a centralised manner, guaranteeing at all times exclusive control over the signature process by the *Government employees* to whom the *Certificate* has been issued.

16. The FNMT-RCM will interpret, register, maintain and publish the procedures relating to this section and may also receive communications from interested parties on these matters through the contact information stated in point 1.5.2 Contact details in this document.

## 1.3. PARTIES

17. The following parties are involved in the management and use of the *Trust services* described in this *Specific Practices and Policies Statement (SPPS)*:

    1. Certification Authority
    2. Registration Authority
    3. *Signatories*
    4. *Certificate* subscribers
    5. Trusting parties
    6. Other participants

### 1.3.1. Certification Authority

18. The FNMT-RCM is the *Certification Authority* that issues the electronic *Certificates* which are the subject matter of this *SPPS*. Certification Authorities are as follows:

    a) Root Certification Authority. This authority exclusively issues *Certificates* for Subordinate Certification Authorities. This CA's root certificate is identified by the following information:

**Table 1 – FNMT root CA 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 4096 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: issues the end-entity *Certificates* that are the subject matter of this *SPPS*. This Authority's certificate is identified by the following information:

**Table 2 – Subordinate CA Certificate**

| | |
|---|---|
| Subject | CN = AC Administración Pública, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES |
| Issuer | OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES |
| Serial number (hex) | 02 |
| Validity | Not before: 21 May 2010. Not after: 21 May 2022 |
| Public key length | RSA 2048 bits |

| | |
|---|---|
| Signature algorithm | RSA – SHA256 |
| Key identifier | 14 11 E2 B5 2B B9 8C 98 AD 68 D3 31 54 40 E4 58 5F 03 1B 7D |

### 1.3.2. Registration Authority

19. The *Registration Authority* carries out tasks to identify applicants, *Government employees*, verify the documentation attesting to the circumstances stated, and validate and approve requests to issue, revoke and, if applicable, renew the said *Certificates*.

20. Registration entities for the FNMT-RCM may be Registration Offices designated by the *Certificate Subscriber* body or entity with which the latter entity signs a legal instrument for this purpose.

### 1.3.3. Signatories

21. *Signatories* are the individuals, *Government employees* that exclusively use the *Signature creation data* associated with the said *Certificate*.

### 1.3.4. Certificate subscribers

22. Centralised electronic signature *Certificate Subscribers* for public employees are the Administration, bodies and public entities represented through the competent bodies.

### 1.3.5. Trusting parties

23. Trusting parties are individuals or legal entities, other than the *Signatory/Subscriber*, that receive and/or use certificates issued by the FNMT-RCM and, as such, are subject to the provisions of this SPPS when they effectively decide to place their trust in the *Certificates*.

### 1.3.6. Other participants

24. Not stipulated.

## 1.4. USE OF CERTIFICATES

### 1.4.1. Permitted uses of certificates

25. *Certificates* issued under this *Certification Policy* are issued to public officials, employees, statutory personnel and authorised personnel working for Public Administrations, government bodies or public-law entities. These *Certificates* are valid as electronic signature systems

pursuant to Law 40/2015 (1 October) on the Public Sector and Law 18/2011 (5 July) on the use of information and communication technologies in the Justice Administration.

26. The *Issuance Law* for these *Certificates* may determine, in the absence of specific legislation, the terms and conditions of use and the regime for these *Certificates* that will allow the attribution to the Administrations, bodies and entities of the acts and resolutions made by their personnel; all without any legal modification or change with respect to the activities of these Public Administrations through traditional means.

27. The said *Certificates* are *Qualified Certificates* pursuant to Regulation (EU) No. 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 (eIDAS Regulation) and in accordance with the requirements of the European standards ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

### 1.4.2. Restrictions on the use of certificates

28. The powers and functions of the *Subscriber* Public Administration (acting through their personnel as the *Signatories* of the *Certificates*) constitute restrictions on the use of this type of *Certificates*, on the basis of the relevant post, position and, if applicable, authorisation conditions. The FNMT-RCM and the Administration, bodies and public entities may reach agreements on other additional limits, through the relevant relationship document or, if appropriate, in the *Issuance Law* governing these *Certificates*.

29. The FNMT-RCM will have no control over the activities and uses of the *Certificates* and the *Private key* by *Government employees* on behalf of the government, so the FNMT-RCM will be exonerated from liability for such uses, as well as from any consequences and effects that might arise as regards any actions or, if applicable, claims against its assets by third parties.

30. As regards the activities of *Registration Office* personnel, the FNMT-RCM will be subject to the obligations and responsibilities stipulated in electronic signature legislation, without affecting the special provisions contained in Article 11 of RD 1317/2001 (30 November), which develops Article 81 of Law 66/1997 (30 December) on Tax, Administrative and Social Measures in relation to the provision of security services by the Spanish Mint in communications with Public Administrations through electronic, computer and telematic means. In order to be able to diligently use the *Government employees' Electronic signature Certificates*, the user must previously form part of the *Electronic Community* and the acting Administration must become a *Subscriber*.

31. In any event, should a third party wish to trust the *Electronic signature* completed using one of these *Certificates* without accessing the *Status information service* for *Certificates* issued under this *Certification policy*, there will be no coverage from these *Certification Policies and Specific Certification Practices*, and there will be no entitlement whatsoever to bring claims or legal actions against the FNMT-RCM for damages, harm or disputes deriving from the use of or trust in a *Certificate*.

32. Moreover, even within the scope of the *Electronic Community*, this type of *Certificates* may

not be used to:

- Sign or stamp a different *Certificate*, unless specific prior authorisation is obtained.
- Private uses, barring relations with Administrations where permitted.
- Sign or stamp software or components.
- Generate time stamps for *Electronic dating* procedures.
- Provide services for no consideration or for valuable consideration, unless specific prior authorisation is obtained, such as, for illustrative purposes:
    - Provision of OCSP services.
    - Generation of *Revocation Lists*.
    - Provision of notification services.

## 1.5. POLICY ADMINISTRATION

### 1.5.1. Entity responsible

33. The Spanish Mint, holding tax code Q2826004-J, is the Certification Authority that issues the certificates to which this *Certification Practices and Policies Statement* applies.

### 1.5.2. Contact details

34. The FNMT-RCM's contact address as a *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
Tel.: 902 181 696

35. 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. Parties responsible for adapting the CPS

36. The FNMT-RCM's management's powers include the capacity to specify, revise and approve review and maintenance procedures both for the Specific Certification Practices and the relevant Certification Policy.

### 1.5.4. CPS approval procedure

37. The FNMT-RCM, through its *Trust Service Provider* Management Committee, oversees compliance with the *Certification Policies and Practices Statements*, approves them and reviews them annually.

## 1.6. DEFINITIONS AND ACRONYMS

### 1.6.1. Definitions

38. For the purposes of this *SPPS*, when the terms begin with an upper-case letter and are in italics, they will have the meanings stated in general in the GCPS and, in particular, those set out below:

- *Electronic Signature Certificate:* in this SPPS document, it refers always to the electronic *Certificate* issued by the FNMT-RCM to *Government employees* for remote or server signatures. This means that the *Public and private keys* are generated and stored in a secure environmental owned by the FNMT-RCM, guaranteeing at all times exclusive control over the use of the keys by the *Signatory* (*Government employee*).
- *Certification Practices Statement (CPS):* a statement made available to the general public in an easily accessible manner, electronically and free of charge, by the FNMT-RCM. It is classed as a security document detailing, under the eIDAS framework, the obligations that *Trust Service Providers* undertake to fulfil in connection with the management of *Signature creation and verification data* and electronic *Certificates*, terms and conditions applicable to the request, issuance, use and expiration of *Certificates*, technical and organisational security measures, profiles and mechanisms for information on the validity of *Certificates.*
- *Specific Practices and Policies Statement (SPPS):* a specific *CPS* applicable to a certain set of *Certificates* issued by the FNMT-RCM under the specific terms and conditions contained in this Statement, subject to the specific policies defined therein.
- *Signatory*: *Government employee* that makes use of his or her *Signature creation data.*
- *Supervisory body:* body designated by a Member State as responsible for supervisory functions in trust services, pursuant to Article 17 of the eIDAS Regulation. In Spain, this is currently the Ministry of Energy, Tourism and Digital Agenda.
- *Government employees*: public officials, personnel, statutory personnel, authorised personnel or employees of the Public Administration or Justice Administration, body, public body or public-law entity.
- *Person responsible for Registration Operations*: individual appointed by the representative of the Public Administration, public body or public-law entity who is responsible for the tasks assigned to the *Registration Office*, having the

obligations and responsibilities assigned in these *Specific Certification Policies and Practices*.

- *Electronic site*: electronic address, available to citizens through telecommunications networks, owned by a Public Administration or by one or more public bodies or public-law entities when exercising their powers.
- *Subscriber*: the Public Administration, body, public body or public-law entity.

### 1.6.2. Acronyms

39. For the purposes of this *SPPS*, the following acronyms are applicable, the meaning of which is in line with the European standard ETSI EN 319 411 “Policy and security requirements for Trust Service Providers issuing certificates”:

**CA**: Certification Authority

**RA**: Registration Authority

**ARL**: Certification Authority Revocation List

**CN**: Common Name

**CRL**: *Certificate* Revocation List

**DN**: Distinguished Name

**CPS**: Certification Practices Statement

**GCPS**: Trust Services Practices and Electronic Certification General Statement

**eIDAS**: Regulation (EU) No. 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. A security device that generates and protects cryptographic keys.

**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

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

**UTC**: Coordinated Universal Time

# 2. PUBLICATION AND REPOSITORIES

## 2.1. REPOSITORY

39. The FNMT-RCM, as a *Trust Service Provider*, has a repository of public information available 24x7, every day of the year, at the address:

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

## 2.2. PUBLICATION OF CERTIFICATION INFORMATION

40. Information on the issuance of the electronic *Certificates* referred to in this *SPPS* is published at the following address:

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

## 2.3. PUBLICATION FREQUENCY

41. Any amendment to the *Trust Services Practices and Electronic Certification General Statement* or to the *Specific Certification Policies and Practices* will be immediately published in the URL where they may be accessed.

42. The frequency of publication of CRLs is defined in paragraph “4.10.3 Additional features. Publication frequency”.

## 2.4. REPOSITORY ACCESS CONTROL

43. All the above-mentioned repositories are freely accessible for information consultation and, if applicable, download purposes. Moreover, the FNMT-RCM has put in place controls to prevent unauthorised persons from adding, altering or deleting information included in its repositories and to protect the authenticity and integrity of the information.

# 3. IDENTIFICATION AND AUTHENTICATION

## 3.1. NAMES

44. *Certificate* encoding follows 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 *Certification Policies* and *Specific Certification Practices,* except where expressly stated in the relevant field, use UTF8String encoding.

### 3.1.1. Name types

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

46. The Common Name field defines the *Government employees* to whom the *Certificate* has been issued.

*Pseudonyms*

47. The *Centralised Signature Certificates* issued by the FNMT-RCM under these *Certification Policies* and *Specific Certification Practices* making use of pseudonyms will clearly state this feature, pursuant to the eIDAS Regulation and applicable domestic legislation.

48. In the identity accreditation procedure, as a step prior to the issuance of a *Centralised Signature Certificate* with a pseudonym, the FNMT-RCM, through the *Registration Office,* will check the *Signatory'*s true identity and will keep the supporting documents.

### 3.1.2. Name uniqueness

49. The distinguished name (*DN*) assigned to the *Certificate* inside the *Trust Service Provider'*s domain will be unique.

### 3.1.3. Registered trademark recognition and authentication

50. The FNMT–RCM makes no commitment whatsoever regarding the use of distinctive signs, whether registered or otherwise, in the issuance of the *Certificates* under this *Certification Policy. Certificates* including distinctive signs may only be requested when the *Holder* owns the right of use or is authorised to use the sign. The FNMT–RCM is not obligated to previously verify the ownership or registration of the distinctive signs before issuing the *Certificates,* even if they are entered in public registers.

## 3.2. INITIAL VALIDATION OF IDENTITY

### 3.2.1. Methods to prove possession of the private key

51. The *Applicant*, *a Government employee,* generates his or her *Public and private keys* in the FNMT-RCM's system after having been registered in the system and once such generation has been validated by the *Registration Office*, following the accreditation of the *Applicant*'s identity and obtainment of his or her consent to the issuance of the *Centralised Signature Certificate*.

52. After the *Applicant* has been informed that his or her *Certificate* is to be issued, the system generates the *Key* pair, such that the *Private key* is stored in a protected manner, guaranteeing its use under the exclusive control of the *Government employee*.

### 3.2.2. Authentication of the organisation's identity

53. The activities performed to verify the identity of the *Government employee*, the *Certificate Applicant*, will be carried out by authorised personnel in the *Registration Offices* implemented by the body or entity of the Public Administration in question. This guarantees the identity of

the Administration, the *Certificate Subscriber*, which, in each case, is the body or entity in which the employee provides his or her services. The *Registration Offices* will not therefore be authorities delegated by or attached to the FNMT-RCM.

### 3.2.3. Authentication of the individual applicant's identity

54. The FNMT-RCM, based on the list of user personnel sent by the Administration, body or public entity, will consider, under the responsibility of the bodies and/or entities, which will act through the *Registration Offices*, that such personnel validly hold their posts, that their personal ID number, position or authorisation is authentic and, therefore, that they are authorised to obtain and use the *Certificate*. The FNMT-RCM will not be responsible, in this type of *Certificate*, for verifying the post or position held by the said personnel, or that these requirements are fulfilled throughout the life of the *Certificate*, as the FNMT-RCM does not have a legal public official, administrative or employment relationship with the personnel, beyond the document stating the terms and conditions of use or, if applicable, the issuance contract, which has a strict documentary effect for the performance of the functions pertaining to the post.

55. These verification activities will be carried out by the people responsible in the *Registration Offices* implemented by the body or entity of the Public Administration in question, which, in each case, is the body or entity in which the employee provides his or her services. The *Registration Offices* will not therefore be authorities delegated by or attached to the FNMT-RCM.

56. Validation directly by physical presence of the Applicant Applicants for Certificates must physically appear to formalize the procedure of confirmation of personal identity, with any of the means of identification admitted by law in accordance with the national legislation in force, appearing at the *Registration Office* designated for such purposes by the *Subscriber* body or public entity in which the employee provides his or her services. The said *Registration Office* is created by the *Subscriber* Administration, which provides the FNMT- RCM with a list of people authorised to carry out the Registration activities, in accordance with procedures stipulated for such purposes, and communicates any changes to the Office's structure.

*Indirect verification using means which provides equivalent assurance to physical presence in accordance with national law*

57. Personal appearance will not be necessary when the *Registration Office* of the Administration's competent body is aware of the identity or other permanent circumstances of the *Certificate* applicants (identity, validity of post and other conditions to be included in the *Certificate*) by virtue of a pre-existing relationship between the *Applicants* and the Administration in which they work, if it is guaranteed that the *Applicants* (*Government employees)* have been identified by physical presence (in accordance with the process defined at the previous paragraph), and the period of time elapsed since such physical appearance is less than five years.

### 3.2.4. Unverified subscriber information

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

## 3.3. IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS

59. The terms and conditions for the authentication of a renewal request are developed in the *Certificate* renewal process section of this document.

## 3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

60. The terms and conditions for the authentication of a revocation request are developed in the *Certificate* revocation process section of this document.

# 4. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFE CYCLE

## 4.1. APPLICATION FOR CERTIFICATES

### 4.1.1. Who may apply for a certificate

61. In this type of *Certificates*, the *Applicant* may only be a *Government employee*.

### 4.1.2. Registration process and responsibilities

62. The *Applicant*, a *Government employee,* through the *Certificate* application web software developed for this purpose, must accept the terms and conditions of use of the *Certificate* and input his or her particulars: national ID number, first surname, tax code of the body in question and the e-mail address to which an application code will be sent.

63. The FNMT-RCM may agree, with the Administrations, bodies and public entities that request it, to create delegated *Registration Offices* in order to centralise registration procedures for other related or attached Administrations that lack sufficient resources to do so under applicable cost-cutting laws.

64. Paragraph 9.8 “Responsibilities” of this document lays down the responsibilities of the parties to this process.

## 4.2. CERTIFICATE APPLICATION PROCEDURE

### 4.2.1. Performance of identification and authentication functions

65. In the event that the *Applicant* appears in person at the *Registration Office*, he or she will furnish the requested data and provide evidence of his or her personal identity and of *Government employee* status. In the case of a *Centralised Signature Certificate* with a

pseudonym, the FNMT-RCM, through the *Registration Office,* will check the *Signatory'*s true identity and will keep the supporting documents. In any event, the FNMT-RCM will accept the function carried out and report prepared by the *Registration Office* designated by the Administration.

66. The *Applicant* will sign the terms and conditions of use of the *Certificate* and will be provided with identification credentials to be used in the *Certificate* request software application (username and a part of the application access password).

67. The FNMT-RCM may identify the *Applicant*, alternatively to his or her appearance at the *Registration Office*, through the use of a *Qualified electronic certificate* issued to the *Government employee,* thus guaranteeing the authenticity of all the fields to be included in the *Centralised electronic certificate* to be issued, provided more than five years have not elapsed since the *Signatory* was identified.

### 4.2.2. Approval or rejection of certification application

68. Once the *Registration Office* has confirmed the *Applicant*'s identity and the validity of his or her post or position, and the terms and conditions of use document or, if applicable, the application contract has been signed by the *Applicant* and the *Registration Office*, the office will validate, sign and send the data, together with the application code obtained in the application phase. The *Applicant* is then registered in the FNMT-RCM's system, although the *Keys* have yet to be generated.

69. This information transfer to the FNMT-RCM will take place by means of secure communications created for this purpose between the *Registration Office* and the FNMT-RCM.

70. The FNMT-RCM will only gather from the *Applicants* the information, received from the *Registration Office*, that is necessary to issue the *Certificates* and to verify their identity; the information required by electronic signature legislation will be stored for a fifteen (15)-year period and treated with due diligence, pursuant to prevailing domestic personal data protection legislation.

71. The personal data and related processing will be subject to specific legislation.

### 4.2.3. Application processing time

72. The application is automatically processed by the system, so there is no stipulated period of time for this process.

## 4.3. CERTIFICATE ISSUANCE

### 4.3.1. CA's issuance actions

73. As indicated previously, the *Applicant*, *a Government employee,* has been registered in a highly secure manner in the system, as a prior step to the generation of the *Public and private keys*.

74. The FNMT-RCM sends a notification to the *Applicant*'s e-mail address containing the other part of the password forming his or her identification credentials, thus completing the information provided by the *Registration Office*.

75. Subsequently, the *Applicant* will identify himself in the system using the credentials received plus a second authentication factor that will be sent to his e-mail address[2]; once his identity has been verified, he will specifically request the issuance of his *Centralised signature certificate.* In this way, the infrastructure securely links the identification data provided by the *Applicant*, as described in the section "4.1.2 Registration process" of this document, with the process of generating its *Certificate.*

76. At this time, the system will generate the *Public and Private Keys* in a protected HSM and will issue the requested *Centralised signature certificate* to the *Government employee*. Additionally, the system requires the *Applicant* to create a personal ID number (PIN) that will be requested in operations using the *Private key*. This PIN is not known (nor stored) at any time by FNMT-RCM's system.

77. The issuance of *Certificates* entails generating electronic documents that confirm the employee's identity*,* relationship, post or position with the Public Administration, as well as correspondence with the associated *Public key*. The issuance of FNMT-RCM *Certificates* may only be carried out by the FNMT-RCM, as a *Trust Service Provider*, there being no other entity or body with the capacity to do so. The FNMT-RCM *Certification Authority* only accepts *Certificate* generation applications from authorised sources. All the data contained in each application are protected against alterations by means of electronic signature or stamp mechanisms using *Certificates* issued to the said authorised sources.

### 4.3.2. Issuance notification

78. Once the *Keys* and *Certificate* have been generated, the system notifies the *Government employee* accordingly.

## 4.4. CERTIFICATE ACCEPTANCE

### 4.4.1. Acceptance process

79. In the *Certificate* application process, the *Government employee* accepts the terms and conditions of use and expresses his or her desire to obtain the *Certificate*, as necessary generation requirements.

### 4.4.2. Certificate publication by the CA

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

[2] The FNMT-RCM may employ other means of communication to transfer this second authentication factor, subject to authorisation from the *Applicant*, such as a mobile telephone, the number having previously been evidenced.

### 4.4.3. Notification of issuance to other entities

81. No issuance notifications are sent to other entities.

## 4.5. KEY PAIR AND USE OF CERTIFICATE

### 4.5.1. Private key and use of certificate

82. The *Centralised Signature Certificate* is the electronic certificate issued by the FNMT- RCM that links the *Signatory* with *Signature verification data* and confirms, jointly:

- the identity of the *Signatory* (*Government employee)* including, if applicable, his or her personal ID number, post, position and/or authorisation status; and
- the identity of the *Certificate Subscriber*, for which the *Signatory* exercises his powers, works or carries out his activities.

83. This *Certificate* is issued by the FNMT-RCM on behalf of the relevant Administration, which receives the necessary technical, administrative and security services from FNMT-RCM, as a *Trust Service Provider*.

84. The *Centralised Signature Certificate* is issued by the FNMT-RCM based on identification and registration activities carried out by the network of *Registration Offices* designated by the *Certificate Subscriber* body or entity. The "*Issuance Laws*" may stipulate, within the remit of the Public Administrations, common *Registration Offices* with uniform effects for any Administration, body and or public entity.

85. The *Issuance Law* will replace, based on the different functionalities within the scope of the *Certificates*, elements or fields normally included in the *Certificate* itself, depending on the specific remit of the Public Administration in question.

### 4.5.2. Use of the certificate and public key by trusting third parties

86. Third parties that place their trust in the *Electronic signatures* completed using the *Private keys* associated with *Centralised Signature Certificates* will abide by the obligations and responsibilities defined in this *SPPS*.

## 4.6. CERTIFICATE RENEWAL

87. *Certificate* renewal consists of issuing a new *Certificate* without changing any information on the *Signatory* or *Public key,* or any other information appearing in the *Certificate*. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* maintaining the *Public key*.

## 4.7. RENEWAL WITH REGENERATION OF CERTIFICATE KEYS

88. The "key regeneration" process consists of issuing a new *Certificate* with a different *Public key*, serial number and validity period, maintaining the subject field content from the old

certificate.

89. Under these Certification Policies, the FNMT-RCM does not contemplate this process of key regeneration. If the *Signatory* wish to continue using a *Centralised Signature Certificate* under these *Certification Policies and Specific Certification Practices* once his *Certificate* has expired, a new *Certificate* must be requested and his identity must be confirmed following the procedure described in point "4.1 Application for certificates" in this document.

## 4.8. CERTIFICATE AMENDMENT

90. No amendments may be made to *Certificates* issued. Consequently, a new Certificate must be issued in order for changes to be made.

## 4.9. CERTIFICATE REVOCATION

91. The effects of the revocation of the *Centralised Signature Certificate*, i.e. its expiration, will automatically entail the expiration of the associated *Signature creation data*. These effects will arise as from the date on which the FNMT-RCM has certain knowledge of any of the determining events, which will be stated in its *Certificate status information and consultation service*.

### 4.9.1. Revocation circumstances

92. The application for the revocation of *Centralised Signature Certificates* may be made during the validity period stated in the *Certificate.*

93. Admissible causes for the revocation of a *Centralised Signature Certificate* are as follows:

a) Revocation application issued by the *Signatory* (*Government employee*) or by the *Subscriber* (*Administration* where the *Signatory* works) through duly authorised personnel. In any event, this application must be the result of:

- The use by a third party of the *Signature creation data* pertaining to the *Signature verification data* contained in the *Certificate* and linked to the *Signatory*'s personal identity.
- Infringement or jeopardising of the secrecy of the *Signature creation data* or of the information necessary to access them.
- Termination of the *Government employee*'s relationship with the Administration.
- Non-acceptance of the new terms and conditions that may result from the issuance of new *Certification Practices and Policies Statements*, for a one-month period following their publication.

b) Cancellation of the *Signatory*'s credentials.

c) Court or administrative ruling ordering revocation.

d) *Signatory*'s death or full or partial disability ex post facto.

e) Inaccuracies in the data furnished by the *Applicant* to obtain the *Certificate*, or alteration of the data provided to obtain the *Certificate*, or change in the circumstances verified for the issuance of the *Certificate*, such that it no longer reflects reality.

f) Infringement of a substantial obligation laid down in this *Certification Practices and Policies Statement* by the *Certificate Signatory* or *Applicant* if, in the latter case, it affected the *Certificate* issuance procedure.

g) Infringement or jeopardising of the secrecy of the *Signatory*'s *Signature creation data*.

h) Infringement of a substantial obligation laid down in this *Certification Practices and Policies Statement* by a *Registration Office*, if it affected the *Certificate* issuance procedure.

i) Termination of the agreement between the *Signatory* or the *Subscriber* and the FNMT-RCM.

j) Infringement or jeopardising of the secrecy of the *Trust Service Provider's Signature creation data*.

k) Discontinuance of the *Trust Service Provider'*s activity, unless management of the electronic certificates issued is transferred to a different *Trust Service Provider*.

94. In no circumstances does the FNMT-RCM acquire any obligation to verify the matters mentioned in letters d) to g) of this point, which must be communicated to this entity in a duly attested manner by submitting the documents and information necessary to verify it.

95. The FNMT-RCM will only be liable for the consequences of the failure to revoke a *Certificate* in the following cases:

- Revocation should have been completed due to a duly attested application from the *Signatory* or *Subscriber* by means of the systems made available by the FNMT-RCM for this purpose.
- The FNMT-RCM has been notified of the revocation application or cause through a court or administrative ruling.
- Causes d) to g) above are duly evidenced to the FNMT-RCM following the identification of the *Applicant* authorised to carry out the revocation.

96. Activities that constitute an offence or misdemeanour of which the FNMT-RCM is unaware, affecting the data and/or *Certificate*, and inaccuracies in the data or a lack of diligence in the communication of the data to the FNMT-RCM will exonerate the FNMT-RCM from liability.

97. The revocation of the *Centralised Signature Certificate*, i.e. its expiration, will have effect as from the date on which the FNMT-RCM has certain knowledge of any of the determining events and they are included in its *Certificate status information and consultation service*.

98. Revocation of the *Centralised Signature Certificate* entails, in addition to its expiration and the impossibility of continuing to use the associated *Signature creation data*, the end of the relationship and use regime for that *Certificate* and its *Private key* with the FNMT-RCM.

### 4.9.2. Who may apply for revocation

99. The revocation of a *Centralised Signature Certificate* may only be requested by the *Subscriber* through the *Registration Office* authorised for this purpose or by the *Signatory*, either through the said *Registration Office* or by means of the telephone number created for this purpose (subject to identification of the *Applicant*), which may be found in the FNMT-RCM's website and will be operational 24x7.

100. Nonetheless, the FNMT-RCM may revoke *Centralised Signature Certificates* ex officio in the circumstances stated in the *Certification Practices and Policies Statement*.

### 4.9.3. Revocation application procedure

101. The application for the revocation of *Centralised Signature Certificates* may be made during the validity period stated in the *Certificate.*

102. There follows a description of the procedure to be followed by the *Registration Office* to request the revocation of a *Certificate*.

103. The requester of the revocation of the Certificate will introduce, in the application developed for this purpose, the identifying data of the Signatory: DNI number, surname, NIF of the Administration to which he belongs and his e-mail address to which the revocation will be confirmed.of his/her Certificate. In this way, the infrastructure securely links the identification data provided by the *Registration Office*, with the process of revocation of the *Certificate*

104. In any event, the FNMT-RCM will receive information from the Administration, body or entity that is relevant to the revocation of a *Certificate*, in a paper or electronic format, through the *Registration Office*.

105. The *Registration Office* will send the registered information to the FNMT-RCM for the revocation of the *Certificate*. The personal data and related processing will be subject to specific legislation.

106. The FNMT-RCM will consider that the requester of the revocation of a *Certificate* of this type has the relevant authorisation if the application is made through its *Registration Office*. The FNMT-RCM will not perform any assessment of the suitability or otherwise of the requested revocation when it is applied for through the said *Registration Office*.

107. The *Signatory*, a *Government employee,* may also apply for revocation using the telephone number designated for this purpose (once the *Applicant* has been identified), which may be found in the FNMT-RCM's website and will be operational 24x7.

108. As soon as revocation is complete, the *Signatory* will receive notification of the *Certificate*'s revocation through e-mail address[3] stated in the application.

109. Once the FNMT-RCM has revoked the *Certificate*, the relevant *Certificate Revocation List* will be published in the secure *Directory,* containing the serial number of the revoked

[3] The FNMT-RCM may employ other means of communication to notify this matter, subject to authorisation from the *Applicant*, such as a mobile telephone, the number having previously been evidenced.

*Certificate* and the data, time and cause of revocation. Once a *Certificate* has been revoked, its validity expires definitively and this may not be reversed.

### 4.9.4. Grace period for revocation application

110. There is no grace period associated with this process, since revocation is immediate upon verified receipt of the revocation application.

### 4.9.5. Time period for revocation application processing

111. The FNMT-RCM immediately revokes the *Certificate* once the *Applicant'*s identity is verified or, if applicable, the veracity of the application made by means of a court or administrative ruling is verified. In any event, the *Certificate* will be effectively revoked in less than 24 hours as from receipt of the revocation application.

### 4.9.6. Trusting parties' obligation to verify revocations

112. Third parties that place their trust in and accept the use of *Certificates* issued by the FNMT-RCM are obligated to verify:

- the *Advanced electronic signature* or the *Advanced electronic stamp* of the *Trust Service Provider* that issues the *Certificate;*
- that the *Certificate* is still valid and active;
- the status of *Certificates* included in the *Certification chain.*

### 4.9.7. CRL generation frequency

113. *Revocation lists* (*CRLs*) for *Centralised Signature Certificates* are issued at least every 12 hours, or whenever there is a revocation; they have a 24-hour validity period. *CRLs* of *Authority certificates* are issued every six months, or whenever there is a revocation of an *Authority certificate*; they have a 6-month validity period.

### 4.9.8. Maximum CRL latency period

114. *Revocation lists* are published at the time they are generated, so the latency period between CRL generation and publication is zero.

### 4.9.9. Availability of the online certificate status verification system

115. Information on the status of certificates will be available online 24 hours a day, seven days a week. In the event of system failure, the business continuity plan will be implemented to resolve the incident as soon as possible.

### 4.9.10. Online revocation verification requirements

116. The *Centralised Signature Certificate'*s revocation status may be verified online by means of the *Certificate status information service* provided through the OCSP, as described in paragraph 4.10 of this document. Persons wishing to use this service must:

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

### 4.9.11. Other available revocation notification methods

117. Not defined.

### 4.9.12. Special revocation requirements for committed keys

118. See the relevant section of the General Statement (DGPC).

### 4.9.13. Suspension circumstances

119. The suspension of *Certificates* is not envisaged.

## 4.10. CERTIFICATE STATUS INFORMATION SERVICES

### 4.10.1. Operational features

120. The information on the validation of electronic *Certificates* referred to in this *SPPS* is accessible through:

   a. Certificate Revocation Lists:

      i. ROOT CA. Accesses:

         1. ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

         2. http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

      ii. Subordinate Public Administration CA. Accesses:

         1. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,CN=AC%20Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

         2. http://www.cert.fnmt.es/crlsacap/ CRL<xxx*>.crl

   b. Certificate status verification service (OCSP):

i. ROOT CA. Access:

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

ii. Subordinate CA Administración Pública *Certificate*

http://ocspap.cert.fnmt.es/ocspap/OcspResponder

### 4.10.2. Service availability

121. The FNMT-RCM guarantees access to this service 24x7 by *Users* and parties that place their trust in the *Certificates*, securely, quickly and free of charge.

## 4.11. END OF SUBSCRIPTION

122. For the purposes of these *Specific Certification Policies and Practices,* the subscription will end when the *Centralised Signature Certificate* ceases to be valid. If the *Certificate* is not renewed, the relationship between the *Signatory* and FNMT-RCM will be deemed to have expired.

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

*a)* Termination of the *Certificate'*s validity period.

b) Discontinuance of FNMT-RCM's activities as a *Trust Service Provider* unless, once evidence that the *Subscribers* do not object has been obtained, the *Certificates* issued by the FNMT-RCM are transferred to a different *Trust Service Provider*.

In these two cases [a) and b)], the loss of the *Certificate*'s effectiveness will occur as soon as the circumstances arise.

c) Revocation of the *Certificate* for any of the causes set out in this document.

124. For the purposes stated above, an application for the issuance of a *Centralised Signature Certificate* by the FNMT-RCM where the same *Signatory* and the same *Subscriber* have a *Certificate* in force under the same *Issuance Law* will entail the revocation of the first *Certificate* obtained.

## 4.12. KEY CUSTODY AND RECOVERY

### 4.12.1. Key custody and recovery practices and policies

125. The FNMT-RCM will not recover the *Private keys* associated with the *Centralised Signature Certificate*s. Should the PIN protecting access to the *Private key* be lost by the *Signatory,* the *Certificate* must be revoked and a new *Certificate* must be requested.

### 4.12.2. Session key protection and recovery practices and policies

126. Not stipulated.

# 5. PHYSICAL SECURITY, PROCEDURE AND PERSONNEL CONTROLS

126. See the relevant section of the *General Statement* (*DGPC*).

# 6. TECHNICAL SECURITY CONTROLS

127. See the relevant section of the *General Statement* (*DGPC*).

## 6.1. KEY GENERATION AND INSTALLATION

### 6.1.1. Key pair generation

128. As regards the *Key* information required by the FNMT-RCM to carry out its *Trust Service Provider* activities, see the relevant section of the *DGPC*.

129. *Private keys* associated with *Centralised Signature Certificates* are generated and custodied by the FNMT-RCM's signature activation module, so that access to the *Keys* takes place through means that guarantee, to a high level of trust, the *Signatory*'s exclusive control.

### 6.1.2. Sending of private key to the subscriber

130. The *Private keys* associated with *Centralised Signature Certificates* are generated in a signature creation device controlled exclusively by the *Signatory*, where they will be custodied for use. Consequently, the *Private Key* is not handed over to the *Signatory*.

131. However, in the event that the FNMT-RCM or any of the registration offices is aware of unauthorized access to the *Signatory's Private Key*, the *Centralized Signature Certificate* associated with said *Private Key* will be revoked.

### 6.1.3. Sending of public key to the certificate issuer

132. The *Public key* generated together with the *Private key* using the key generation and custody device is handed over to the Certification Authority by sending a certification application in a PKCS#10 format.

### 6.1.4. Distribution of the CA's public key to the trusting parties

133. The FNMT-RCM distributes *Public keys* of both the root CA and the Subordinate CA that issues the *Centralised Signature Certificates,* through various means, such as publication in its electronic site (www.sede.fnmt.gob.es) or in paragraph 1.3.1 of this document.

### 6.1.5. Key sizes and algorithms used

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

135. The *Key* size, depending on each case, is:

- FNMT root CA *Keys:* 4096 bits.

- *Keys* of the FNMT Subordinate CA that issues the *Centralised Signature Certificates:* 2048 bits.
- *Keys* of the *Centralised Signature Certificates:* 2048 bits.

### 6.1.6. Public key generation parameters and quality verification

136. The *Public keys* of the *Centralised Signature Certificates* are encoded under RFC5280 and PKCS#1.

### 6.1.7. Permitted uses of keys (KeyUsage field X.509v3)

137. The FNMT *Certificates* include the Key Usage extension and, as applicable, the Extended Key Usage extension, indicating authorised uses of the *Keys*.

138. The authorised *Key* uses of the FNMT root CA *Certificate* are the signing/stamping of FNMT Subordinate CA Certificates and ARLs. The authorised uses of the *Certificate* of the FNMT Subordinate CA that issues the *Centralised Signature Certificates* are exclusively the signing/stamping of end-user *Certificates* (*Centralised Signature Certificates*) and CRLs.

139. The *Centralised Signature Certificate* issued to users, as *Signatories*, is exclusively authorised for use in electronic signatures.

## 6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE CONTROLS

### 6.2.1. Cryptographic module standards

140. The *Trust Service Provider*'s *Signature creation data* are protected by a cryptographic device that fulfils FIPS PUB 140-2 Level-3 security standards. Operations for the signing of *Certificates, Revocation lists* and data structures relating to the validity of *Electronic certificates and Time stamps* are carried out inside the cryptographic device, which brings *Confidentiality* to the *Trust Service Provider*'s *Signature creation data*.

141. If the *Signature creation data* had to be outside the cryptographic device in any circumstances, the FNMT-RCM would apply the appropriate technical and organisational measures to guarantee their *Confidentiality.*

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

142. The FNMT-RCM guarantees that all operations involving the *Private keys* of its Certification Authorities require the approval of at least two people.

### 6.2.3. Private key custody

143. Copy, backup or recovery operations relating to the *Private keys* of the FNMT-RCM's Certification Authorities are controlled exclusively by authorised personnel employing, at minimum, dual control in a secure environment.

144. *Private keys* relating to the *Centralised Signature Certificates* issued to end users

*(Signatories*) are custodied in the FNMT-RCM's systems such that only the *Signatory* can access his or her *Private key*. Access is guaranteed through the use of his identification credentials and signature PIN (only known by the *Signatory*), plus a second authentication factor in the form of a single-use password.

### 6.2.4. Private key backup

145. A copy is kept of the necessary files and components so that, in the event of a contingency, the cryptographic device's security environment may be restored, in security envelopes duly custodied inside a fire-resistant cabinet, which may only be accessed by authorised personnel.

### 6.2.5. Private key filing

146. The FNMT-RCM may make a backup of the *Signature creation data* associated with the *Centralised Signature Certificates,* guaranteeing that the security level of the copied data is at least equal to that of the original data and that the number of data duplicated does not exceed the minimum necessary to assure service continuity. The *Signature creation data* are not duplicated for any other purpose.

### 6.2.6. Transfer of private key to or from the cryptographic module

147. The Certification Authorities' *Private keys* are generated as described in point "6.1 Key generation and installation". Consequently, the *Keys* cannot be transferred, although there is a recovery procedure as a contingency measure, as described in point "6.2.4 Private key backup".

### 6.2.7. Storage of private key in the cryptographic module

148. The FNMT-RCM has the necessary means to assure that the cryptographic hardware used to protect its *Keys* as a *Trust Service Provider:*

- Has not been manipulated during transportation, by means of an inspection of the material supplied which includes controls to detect authenticity and possible manipulation.
- Functions correctly, through continuous monitoring processes, periodic preventive maintenance and a software and firmware upgrade service.
- Remains in a physically secure environment from receipt to destruction, if applicable.

### 6.2.8. Private key activation method

149. The Certification Authorities' *Private keys* are generated and custodied by a cryptographic device that meets FIPS PUB 140-2 Level 3 security requirements.

150. Mechanisms to activate and use the Certification Authorities' *Private keys* are based on the segmentation of management and operation roles that the FNMT-RCM has implemented, including multi-person access based on cryptographic cards and related PINs in a simultaneous use M of N (2 of 5) system.

151. The activation mechanisms and use of the *Private keys* for end-entity *Centralised Signature Certificates* are based on the *Signatory*'s use of his or her identification credentials and signature PIN (known only to the *Signatory*), plus a second authentication factor in the form of a single-use password.

### 6.2.9. Private key deactivation method

152. A person in an administrator's role may deactivate the Certification Authorities' *Key* by stopping the system. Reactivation will follow the steps described in point "6.2.8 Private key activation method".

153. *Private keys* for end-entity *Centralised Signature Certificates* will be deactivated until the *Signatory* is authenticated in the centralised signature system.

### 6.2.10. Private key destruction method

154. The FNMT-RCM will destroy or store the *Trust Service Provider*'s *Keys* in an appropriate manner once the validity period has elapsed so as to avoid misuse.

155. *Private keys* for end-entity *Centralised Signature Certificates* will be destroyed once their use period or the *Signatories'* relationship with the FNMT-RCM has ended. Moreover, if the *Signatory* inputs his or her signature PIN incorrectly a certain number of times, both his *Key* and the signature *Certificate* will be destroyed. Destruction will be preceded by the revocation of the *Centralised Signature Certificate* relating to that *Private key*.

### 6.2.11. Cryptographic module classification

156. The cryptographic modules fulfil the security requirements necessary to guarantee *Key* protection, as indicated in point "6.2.1 Cryptographic module standards" of this document.

## 6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

### 6.3.1. Public key filing

157. *Centralised Signature Certificates* and thus their associated *Public keys* are kept by the FNMT-RCM during the period of time stipulated in prevailing legislation, as stated in this document.

### 6.3.2. Certificate operating periods and key pair usage periods

158. *Certificate* and associated *Key* operating periods are as follows:

- FNMT root CA *Certificate* and its *Key* pair: to 1 January 2030.
- *Certificate* of the FNMT subordinate CA that issues the *Centralised Signature Certificates* and its *Key* pair: to 21 May 2022.
- *Centralised Signature Certificates* and their *Key* pair: no longer than two years.

## 6.4. ACTIVATION DATA

### 6.4.1. Activation data generation and installation

159. The activation data, both the FNMT root CA *Keys* and the *Keys* of the subordinate CA that issues the *Centralised Signature Certificates,* are generated during the *Certification Authorities*' *Key* creation ceremony.

160. The activation data for *Centralised Signature Certificate Keys* are generated by the signature activation module in the same manipulation-proof environment as the *Trust Service Provider*'s signature creation device, guaranteeing that they may only be generated under the *Signatory*'s exclusive control.

### 6.4.2. Activation data protection

161. The activation data for the Certification Authorities' *Private keys* are protected using the method described in paragraph "6.2.8 Private key activation method" of this document, including multi-person access based on cryptographic cards and related PINs in a simultaneous use M of N (2 of 5) system.

162. The PIN protecting access to the *Private key* for the *Centralised Signature Certificate* is confidential, personal and non-transferable. Consequently, the *Signatory*, who also needs a second authentication factor to activate his *Private key*, is responsible for protecting his activation data.

### 6.4.3. Other aspects of activation data

163. Not stipulated.

## 6.5. IT SECURITY CONTROLS

164. See the relevant section of the *General Statement* (*DGPC*).

## 6.6. TECHNICAL LIFE CYCLE CONTROLS

165. See the relevant section of the *General Statement* (*DGPC*).

## 6.7. NETWORK SECURITY CONTROLS

166. See the relevant section of the *General Statement* (*DGPC*).

## 6.8. TIME SOURCE

167. See the relevant section of the *General Statement* (*DGPC*).

# 7. CERTIFICATE PROFILES, CRLs AND OCSP

## 7.1. CERTIFICATE PROFILE

167. *Centralised Signature Certificates* comply with the European standard ETSI EN 319 412-2 “Certificate profile for certificates issued to natural persons”.

### 7.1.1. Version number

168. *Centralised Signature Certificates* follow the X.509 version 3 standard.

### 7.1.2. Certificate extensions

169. The document describing the *Centralised Signature Certificate* profile, including all its extensions, is published at http://www.cert.fnmt.es/dpcs/.

### 7.1.3. Algorithm object identifiers

170. The object identifier (OID) relating to the cryptographic algorithm used (SHA- 256 with RSA Encryption) is 1.2.840.113549.1.1.11.

### 7.1.4. Name formats

171. *Centralised Signature Certificate* encoding follows the RFC 5280 recommendation “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. All the fields defined in the *Certificate* profile, except where expressly stated in the relevant field, use UTF8String encoding.

### 7.1.5. Name restrictions

172. The distinguished name (*DN*) assigned to the *Certificate Subscriber* in the *Trust Service Provider*’s domain will be unique and will be composed as defined in the *Certificate* profile.

### 7.1.6. Certificate policy object identifier

173. The object identifier (OID) of the *Centralised Signature Certificate* policy is defined in paragraph “1.2 Document name and identification” of this document.

### 7.1.7. Use of the policy constraints extension

174. The “Policy Constraints” extension of the CA's root *Certificate* is not used.

### 7.1.8. Syntax and semantics of the policy qualifiers

175. The extension “Certificate Policies” includes two “Policy Qualifiers” fields:

- CPS Pointer: contains the URL in which the *Certification Policies* and *Trust Services Practices* applicable to this service are published.
- User notice: contains a text that may drop down on the *Certificate* user's Screen during verification.

### 7.1.9. Semantic treatment of the certificate policy extension

176. The "Certificate Policy" extension includes the policy OID field, which identifies the policy associated with the *Certificate* by the FNMT–RCM, as well as the two fields referred to in the previous paragraph.

## 7.2. CRL PROFILE

### 7.2.1. Version number

177. The CRL profile follows the X.509 version 2 standard.

### 7.2.2. CRL and extensions

178. 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 | UTC issuance time. |
| Date of next upgrade | Issuance date + 24 hours |
| Authority key identifier | Issuer key hash |
| Distribution point | URLs of distribution point & CRL scope |

| | |
|---|---|
| Certificates revoked | List of certificates revoked, containing at least the serial number and revocation date for each entry |

## 7.3. OCSP PROFILE

### 7.3.1. Version number

179. The *Certificates* used by the *Certificate validity status information and consultation service*, via OCSP, comply with the X.509 version 3 standard.

### 7.3.2. OCSP extensions

180. The *Certificate validity status information and consultation service*'s OCSP responses include, where requested, the global extension “nonce”, which is used to link a request to a response so as to prevent repetition attacks.

181. The “Extended Revoked Definition” extension is also included in cases in which the consultation relates to a *Certificate* that the CA classes as not issued. The service therefore responds to consultations on certificates not issued by the CA as if they were revoked *Certificates*.

# 8. COMPLIANCE AUDITS

182. The FNMT-RCM will have a specific system in place to register events for all operations, such as: issuance, validation and revocation of *Certificates*, issuance of *Revocation lists*, information on the status of *Certificates* and issuance of *Electronic time stamps*.

183. In order to minimise the impact on systems during production, audits are scheduled for off-peak times.

## 8.1. AUDIT FREQUENCY

184. Audit plans will be drawn up periodically, encompassing the following action at least:

- Risk analysis as stipulated in the Information Security Management System: annual review and full analysis every three (3) years.
- Review of the Information Security Management System under the UNE- ISO/IEC 27001 standard “Information Security Management Systems. 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 certification.
- Data protection: one internal audit every two (2) years by the Information Systems Department.

- The *Certification Authority* that issues the *Centralised Signature Certificates* undergoes periodic audits under the European standard ETSI EN 319 401 "General Policy Requirements for Trust Service Providers". Annual audit by a reputable external company.
- One audit every two (2) years of the information system used by the FNMT-RCM to provide *Trust Services*, as stipulated in the National Security Scheme (Royal Decree 3/2010 of 8 January on the National Security Scheme for E-Government).

## 8.2. AUDITOR QUALIFICATIONS

185. See the relevant section of the *General Statement* (*DGPC*).

## 8.3. AUDITOR'S RELATIONSHIP WITH THE COMPANY AUDITED

186. See the relevant section of the *General Statement* (*DGPC*).

## 8.4. ASPECTS AUDITED

187. See the relevant section of the *General Statement* (*DGPC*).

## 8.5. DECISION-MAKING ON WEAKNESSES DETECTED

188. See the relevant section of the *General Statement* (*DGPC*).

## 8.6. NOTIFICATION OF FINDINGS

189. See the relevant section of the *General Statement* (*DGPC*).

# 9. OTHER LEGAL AND BUSINESS MATTERS

## 9.1. CHARGES

190. The FNMT-RCM will apply to the Public Administrations the fees approved by the relevant Under-Secretary's Office for the provision of *Trust Services* or, failing this, the fees stated in the specific management agreement.

### 9.1.1. Certificate issuance or renewal fees

191. Fees applicable to the issuance or renewal of *Certificates* will be determined as stipulated in paragraph "9.1 Fees" of this document.

### 9.1.2. Certificate access fees

192. Not stipulated.

### 9.1.3. Status or revocation information access fees

193. The FNMT-RCM provides *Certificate* status information services free of charge by means of CRLs or the OCSP.

### 9.1.4. Fees for other services

194. Fees applicable to other services will be determined as stipulated in paragraph “9.1 Fees” of this document.

### 9.1.5. Refund policy

195. Not stipulated.

## 9.2. FINANCIAL LIABILITY

196. See the relevant section of the *General Statement* (*DGPC*).

## 9.3. INFORMATION CONFIDENTIALITY

197. See the relevant section of the *General Statement* (*DGPC*).

## 9.4. PERSONAL DATA PROTECTION

198. See the relevant section of the *General Statement* (*DGPC*).

## 9.5. INTELLECTUAL PROPERTY RIGHTS

199. See the relevant section of the *General Statement* (*DGPC*).

## 9.6. OBLIGATIONS AND GUARANTEES

### 9.6.1. CA's obligations

200. The FNMT-RCM’s obligations and responsibilities, as a *Trust service provider*, with respect to the person associated with the *Certificate*, who acts as the *Signatory*, and to the other members of the *Electronic Community*, will be determined mainly by the document on the terms and conditions of use or *Certificate* issuance agreement and, secondarily, by this *Certification Practices and Policies Statement*.

201. The FNMT-RCM meets the technical specification requirements of the ETSI EN 319 412 standard for the issuance of qualified *Certificates* and undertakes to continue to fulfil that standard or any standards that may replace it.

202. The FNMT-RCM does not make the *Centralised Signature Certificate* available to the Signatories for their recovery.

203. See the relevant section of the *General Statement* (*DGPC*).

### 9.6.2. RA's obligations

204. See the relevant section of the *General Statement* (*DGPC*).

### 9.6.3. Signatories' obligations

205. The natural person associated with the *Certificate*, who acts as the *Signatory,* must comply with the security standards related to the custody and use of the PIN, as confidential, personal and non-transferable information that guarantees access to his or her *Private keys*. Accordingly, the *Signatory* must observe the following cautions relating to the PIN:

- Protect its confidentiality, avoiding disclosure to other persons.
- Memorise it and not write it down in any physical or electronic document.
- Change it as soon as he suspects that it may be known to another person.
- Notify the FNMT-RCM of any possible loss of control over his *Private key* in order to revoke the *Centralised Signature Certificate* and associated *Keys*.
- Refrain from choosing a PIN that may be easily deduced from his or her personal data or is predictable (date of birth, telephone number, series of consecutive numbers, repetitions of the same character, etc.).
- Follow the FNMT-RCM's security policy regarding PIN composition, frequency of changes, etc.

### 9.6.4. Trusting parties' obligations

206. See the relevant section of the *General Statement* (*DGPC*).

### 9.6.5. Other participants' obligations

207. Not stipulated.

## 9.7. WAIVER OF GUARANTEES

208. Not stipulated.

## 9.8. RESPONSIBILITIES

### 9.8.1. Trust Service Provider's responsibility

209. See the relevant section of the *General Statement* (*DGPC*).

### 9.8.2. Applicant's responsibility

210. See the relevant section of the *General Statement* (*DGPC*).

### 9.8.3. Signatory's responsibility

211. The person associated with the *Certificate* who acts as the *Signatory* is obligated to:

- Adequately custody the *Signature creation data* access PIN, using the means necessary to prevent its use by other people.
- Not use the *Certificate* when any of the data included in the *Certificate* are inaccurate or incorrect, or there are security reasons making this advisable.
- Inform the FNMT-RCM of the loss or suspected loss of the *Signature creation data* access PIN so as to initiate the revocation procedure, if appropriate.

212. The *Signatory* will be responsible for informing the FNMT-RCM of any change affecting his or her status or information reflected in the *Certificate* so it may be revoked and a new *Certificate* may be issued.

213. In any case, the *Signatory* will not use the *Signature Creation Data* associated with its *Centralised Signature Certificate* in cases in which it has expired its period of validity, or the *Signature Creation / Seal Data* of the Provider may be threatened and / or committed and so it has been communicated by the Provider or, in his case, the *Signatory* knew, suspected or had news of these circumstances. If the *Signatory* contravenes this obligation, it will be responsible for the consequences of the acts, documents or transactions signed in these conditions, as well as the costs, damages and losses that may arise, for the FNMT-RCM or for third parties, in case of using the *Certificate* beyond its period of validity.

214. Additionally, the *Signatory* will be answerable to the members of the *Electronic community* and other *User entities* or, if applicable, third parties for the undue use of the *Certificate*, or the falseness of the declarations contained in it, or acts or omissions that cause harm to the FNMT-RCM or to third parties.

215. The *Signatory* will be responsible for the use of his or her *Certificate* in the event that the *Trust service provider* has discontinued its activities as an issuer of *Certificates* and the subrogation envisaged in the law has not taken place. In any event, the *Signatory* must not use the *Signature creation data* associated to his or her *Certificate* when it expires, where the *Provider*'s *Signature creation data / Stamp* may be jeopardised and/or compromised and the *Provider* has notified this or, if applicable, the *Signatory* has become aware of these circumstances.

### 9.8.4. Responsibility of the User entity and trusting third parties

216. See the relevant section of the *General Statement* (*DGPC*).

### 9.9. INDEMNITIES

217. See the relevant section of the *General Statement* (*DGPC*).

## 9.10. VALIDITY PERIOD OF THIS DOCUMENT

### 9.10.1. Period

218. This *Certification Practices and Policies Statement* will come into force when it is published.

### 9.10.2. Termination

219. This *Certification Practices and Policies Statement* will be terminated when a new version of the document is published. The new version will entirely supersede the previous document. The FNMT- RCM undertakes to subject the said Statement to an annual review process.

### 9.10.3. Effects of termination

220. For valid *Certificates* issued under a previous *Certification Practices and Policies Statement*, the new version will prevail over the previous version in all matters that do not conflict.

## 9.11. INDIVIDUAL NOTIFICATIONS AND COMMUNICATION WITH PARTICIPANTS

221. See the relevant section of the *General Statement* (*DGPC*).

## 9.12. AMENDMENTS TO THIS DOCUMENT

### 9.12.1. Amendment procedure

222. Amendments to this *Certification Practices and Policies Statement* will be approved by Ceres Department management and will be reflected in the relevant minutes of the *Provider*'s Management Committee meetings, pursuant to the internal procedure approved in the document "Review and maintenance procedure for certification policies and trust service practices statement".

### 9.12.2. Notification period and mechanism

223. The *Trust Service Provider*'s Management Committee will review this *Certification Practices and Policies Statement* annually and, in any event, whenever any amendment is necessary.

224. Any amendment to this *Certification Practices and Policies Statement* will be immediately published in the URL where it may be accessed.

225. Should the amendments not entail significant changes to the parties' obligations and responsibilities or the modification of the service provision policies, the FNMT-RCM will not previously inform users and will simply post a new version of the statement in question on its website.

### 9.12.3. Circumstances in which an OID must be changed

226. Significant amendments to the terms and conditions of the services, obligations and

responsibilities, or restrictions on use may give rise to a change to the service policy and identification (OID), as well as a new link to the new service policy statement. In this case, the FNMT-RCM may establish a mechanism for providing information on the proposed changes and, if applicable, gathering opinions from the affected parties.

## 9.13. CLAIMS AND DISPUTE RESOLUTION

227. See the relevant section of the *General Statement* (*DGPC*).

## 9.14. GOVERNING LAWS

228. See the relevant section of the *General Statement* (*DGPC*).

## 9.15. COMPLIANCE WITH APPLICABLE LEGISLATION

229. The FNMT-RCM declares that it complies with applicable legislation.

## 9.16. SUNDRY STIPULATIONS

230. See the relevant section of the *General Statement* (*DGPC*).

## 9.17. OTHER STIPULATIONS

231. Not envisaged.