Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Certification Policies and Practices for Public Sector Electronic Signature and Electronic Seal Certificates

	NAME	DATE
Prepared by:	FNMT-RCM /	15/10/2021
Revised by:	FNMT-RCM /	22/10/2021
Approved by:	FNMT-RCM /	26/10/2021

Version	Date	Description
1.0	20/01/2020	Certification Policy and Practice Statement for Public Sector Electronic Signature and Electronic Seal Certificates
1.1	29/06/2020	Incorporation of the *Justice Administration Pseudonym Centralised Signature Certificate*
1.2	28/04/2021	Annual review. Section 4.9.12: reference to DGPC
1.3	26/10/2021	Incorporation of the *Public Employee Certificate in QSCD*

Reference: DPC/DPCSP_0103/SGPSC/2021

Document classified as: *Public*

Table of contents

Tables

1. INTRODUCTION

1. The Spanish mint Fábrica Nacional de Moneda y Timbre was authorised under Article 81 of Tax, Administrative and Social Measures Act 66/1997, 30 December, to provide communications security services using electronic, information technology and telematics means and methods. Pursuant to paragraph One:

"notwithstanding the powers allocated in the Act to administrative bodies in regard to the registration of applications, letters and communications, the Spanish mint Fábrica Nacional de Moneda y Timbre (FNMT) is authorised to provide such technical and administrative services as may be necessary to guarantee the security, validity and effectiveness of communications and documents submitted and received using electronic, information technology and telematics means and methods in relations between:

a) General State Administration bodies amongst themselves or between these bodies and public agencies related to or dependent on General State Administration, and between the latter agencies amongst themselves.

b) Natural and legal persons and the General State Administration and public agencies related to or dependent on the latter".

2. On the other hand, Pursuant to paragraph Two:

"FNMT is also authorised, where appropriate, to provide Autonomous Communities, local entities and their related and dependent public-law entities with the services referred to in the preceding paragraph, in relations using electronic, information technology and telematics means and methods amongst themselves, with the General State Administration or with natural and legal persons, provided however that the relevant arrangements or agreements have first been entered into."

3. Citizens' Electronic Access to Public Services Act 11/2007, 22 June, established citizens' right to engage in electronic exchanges with the various Public Administrations (Public Authorities). The legal framework resulting from the approval of Public Administration Common Administrative Procedure Act 39/2015, 1 October, and of Public Sector Legal Regime Act 40/2015, 1 October, systematises all administrative procedure laws, clarifying and consolidating the contents of Public Administration Legal Regime and Common Administrative Procedure Act 30/1992, 26 November, and of the aforementioned Act 11/2007, 22 June. In addition, Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July, makes provision for electronic signature and identification systems to be used within the sphere of Justice Administration.

4. FNMT-RCM has been issuing this type of *Certificates* for electronic identification and signature purposes since the aforementioned Act 11/2007 first came into force.

5. At a time when the use of electronic means should be the norm, appropriate electronic identification, signature and seal systems are required for signature purposes, electronic data interchange in closed communication environments and *Automated administrative action*, where electronic interconnection between Public Administrations is required.

6. The above-mentioned electronic identification, signature and seal systems permitted by the current legal framework include the *Electronic Certificates* referred to herein.

7. 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/EC (eIDAS Regulation), lays down a general legal framework for the use of *Electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and website authentication Certificate services.*

1.1. OVERVIEW

8. The purpose of this document is to provide public information as to the terms and features of the trust services and, in particular, the electronic *Certificate* issuance services provided by FNMT-RCM as a *Trust Service provider*, setting out in particular the obligations and procedures FNMT-RCM undertakes to fulfil in connection with the issuance of *Electronic Signature Certificates* and *Electronic Seal Certificates*, and the obligations FNMT-RCM agrees to fulfil in connection with:

- management of *Signature creation and verification data* and of the *Certificates*, the terms applicable to the application for, issuance, use and termination of the *Certificates* and their *Signature Creation Data*, and, where appropriate, the existence of procedures for coordination with the relevant Public Registers to allow immediate and confidential data interchange as to the validity of the powers specified in the *Certificates* and which must mandatorily be entered in those registers
- provision of the *Certificate* status checking service.

9. This document further sets out, directly or with reference to the FNMT-RCM *Trust Services Practices and Electronic Certification General Statement* to which this Statement is subject, details as to the scope of liability applicable to participants using and/or relying on the services referred to in the preceding paragraph, security controls applied to its procedures and facilities to the extent they may be disclosed without detracting from their effectiveness, and secrecy and confidentiality standards, as well as matters relating to the ownership of its property and assets, protection of personal data, and such other information as may be deemed of interest to be made available to the public.

10. The *Certificates* issued by FNMT-RCM under these *Specific Certification Policies and Certification Practices* are *Qualified Certificates*, as defined in the aforementioned eIDAS Regulation, and Public Sector Legal Regime Act 40/2015, 1 October, and Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July.

1.2. DOCUMENT NAME AND IDENTIFICATION

11. The structure of FNMT-RCM's *Certification Practice Statement* as *Trust Service Provider* comprises on the one hand the common part of FNMT-RCM's *Trust Services Practices and Electronic Certification General Statement* (*GCPS*), for there are actions commons to all of the Entity's trust services, and, on the other hand, the specific sections of this *Specific Certification Policies and Certification Practices* document. However, the *Issuance Law* for

each type of *Certificate* or group of *Certificates* may provide for special features applicable to the bodies, agencies, entities and employees using FNMT-RCM's trust services.

12. Accordingly, FNMT-RCM's *Certification Practice Statement* is structured as follows:

- On the one hand, the ***Trust Services Practices and Electronic Certification General Statement***, which must be regarded as the main body of the *Certification Practice Statement*, describing the scope of liability applicable to members of the *Electronic Community*, security controls applied to FNMT-RCM's procedures and facilities, to the extent they may be disclosed without detracting from their effectiveness, and secrecy and confidentiality standards, as well as matters relating to the ownership of its property and assets, protection of personal data and such other general information issues as should be made available to the public, whatever their role in the Electronic Community may be.

- And on the other hand, for every trust service or set or group of *Certificates*, identified and distinguished from the rest based on typology and specific or distinctive regime, there is a specific ***Certification Policy*** describing participants' obligations, restrictions on the use of the *Certificates* and responsibilities, and there are ***Specific Certification Practices*** implementing the terms defined in the relevant policy and making provision for additional or specific practices with respect to the general practices established in the *Trust Services Practices and Electronic Certification General Statement*.

  These *Specific Certification Policies and Certification Practices* actually elaborate on the contents of the main body and are therefore an integral part of the *Trust Services Practices and Electronic Certification General Statement*, and together they make up the FNMT-RCM *Certification Practice Statement*. However, they apply only to the set of *Certificates* characterised and identified in the relevant *Specific Certification Policies and Practices* and may also cover special provisions introduced by the *Issuance Law* governing the relevant *Certificate* or group of *Certificates*, where specific features or functionalities exist.

- This document therefore sets out the *Specific Certification Policies and Certification Practices* for the following *Certificates within the Administrative sphere:*

  - *Electronic Signature Certificate*
    - *Public Employee Certificate*
    - *Public Employee Certificate in QSCD*
    - *Pseudonym Certificate*
    - *Justice Administration Pseudonym Certificate*
    - *Public Employee Centralised Signature Certificate*
    - *Justice Administration Pseudonym Centralised Signature Certificate*
  - *Electronic Seal Certificate:*
    - *Administration Electronic Seal Certificate*

13. The name of this document is *"Certification Policies and Practices for Public Sector Electronic Signature and Electronic Seal Certificates*", and the document will hereinafter be

referred to, within the scope herein defined, as the "*Specific Policy and Practice Statement*" or abbreviated as "*SPPS*".

14. These *Specific Certification Policies and Certification Practices* are part of the *Certification Practice Statement* and will prevail over the standard provisions of the *Trust Services Practices and Electronic Certification General Statement (GCPS).*

15. The provisions hereof will prevail in the event of conflict between this document and the provisions of the *Trust Services Practices and Electronic Certification General Statement (GCPS).*

16. Additionally, for the *Centralized Signature Certificates*, the provisions of the Policy and Practices of the server signing service will apply, establishing the set of specific rules and procedures followed by the FNMT-RCM for the provision of its server signing service.

17. The following *Certification Policies* are included in this document identified as follows:

Name: *Electronic Seal Certificate* Certification Policy

Reference / OID: 1.3.6.1.4.1.5734.3.17.1

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

Name: *Public Employee Certificate* Certification Policy

Reference / OID[1]: 1.3.6.1.4.1.5734.3.17.2

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

Name: *Justice Administration Pseudonym Certificate* Certification Policy

Reference / OID: 1.3.6.1.4.1.5734.3.17.3

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

Name: *Pseudonym Certificate* Certification Policy

Reference / OID: 1.3.6.1.4.1.5734.3.17.4

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

Name: *Public Employee Centralised Signature Certificate* Certification Policy

Reference / OID: 1.3.6.1.4.1.5734.3.17.5

Type of associated policy: QCP-n.-qscd OID: 0.4.0.194112.1.2

Name: *Justice Administration Pseudonym Centralised Signature Certificate* Certification Policy

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

Reference / OID: 1.3.6.1.4.1.5734.3.17.6

Type of associated policy: QCP-n.-qscd OID: 0.4.0.194112.1.2

Name: *Public Employee Certificate in QSCD* Certification Policy

Reference / OID: 1.3.6.1.4.1.5734.3.17.7

Type of associated policy: QCP-n.-qscd OID: 0.4.0.194112.1.2

Version: 1.3

Approval date: 26/10/2021

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

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

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

18. A *Public Employee Certificate* is an *Electronic Signature Certificate* issued by FNMT-RCM linking the *Signatory* to *Signature verification data* and jointly confirming:

- the *Signatory's* identity (*Public Servant*), including, as appropriate, the *Signatory's* personal identification number, office, job and/or authorised capacity, and
- the *Certificate Subscriber's* identity, where the *Signatory* uses its powers, provides its services, or carries out its activity.

19. A *Public Employee Certificate in QSCD* is the *Public Employee Certificate* whose keys, public and private, have been generated in a qualified signature creation device (*QSCD*)

20. A *Pseudonym Certificate* is the *Public Employee Certificate* linking a Public Administration pseudonym allocated to the relevant *Public Servant*.

21. The *Public Servant Centralised Signature Certificate* and the *Justice Administration Pseudonym Centralised Signature Certificate* are *Electronic Signature Certificate* designed for remote or server-based signatures, i.e., *Public and private keys* are not directly generated in the *Signatory's* Internet browser or other device and the *Certificate* is not downloaded, but is generated and stored in an FNMT-RCM qualified signature creation device. In addition, the electronic signature is centrally provided, and it is guaranteed at all times that the signature process is exclusively controlled by the *Signatory* to whom the *Certificate* has been issued.

22. "*Electronic Seal Certificates*" issued by FNMT-RCM under this certification policy have the necessary safeguards to be used as an identification and seal system for *Automated administrative / judicial action* by Administrations, agencies or public-law entities (and, where appropriate, their respective organisational units) to which those *Certificates* are issued.

23. FNMT-RCM will interpret, register, maintain and publish the procedures referred to in this section and may also receive communications from interested parties in this connection using the contact information provided in section 1.5.2 Contact details hereof.

1.3. PKI PARTICIPANTS

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

1. Certification Authority
2. Registration Authority
3. *Signatories*
4. *Certificate Subscribers*
5. Relying Parties
6. Other participants

1.3.1. Certification Authority

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

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

Table 1 – Root FNMT CA Certificate

Root FNMT CA Certificate	
Subject	OU = FNMT-RCM ROOT CA, O = FNMT-RCM, C = ES
Issuer	OU = FNMT-RCM ROOT CA, 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 bytes
Signature algorithm	RSA – SHA256
Key identifier	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

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

Table 2 – Subordinate CA Certificate

Subordinate CA Certificate	
Subject	CN = AC Sector Público, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES
Issuer	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	34 81 60 C5 1F 5E DB CB 5D DF 89 CA B4 57 33 92
Validity	Not before: 28 November 2019 Not after: 28 November 2029
Public key length	RSA 4096 bytes
Signature algorithm	RSA – SHA256
Key identifier	E7:04:EE:70:91:11:92:44:F9:0E:92:8F:56:43:1E:07:1D:BF:04:9C

1.3.2. Registration Authority

26. The Registration Authority deals with identifying the applicant, the *Public Servant*, 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.

27. Registration Offices designated by the *Certificate Subscriber* body, agency or entity with which the *Subscriber* signs the relevant legal instrument for that purpose may act as FNMT-RCM registration entities.

1.3.3. Signatories

28. *Signatories* are natural persons, *Public Servants*, who maintain the *Signature Creation Data* associated with that *Certificate* for their own use only.

1.3.4. Certificate Subscribers

29. *Electronic Signature Certificate and Seal Certificate Subscribers* are the Administration, public agencies and entities represented through the various competent bodies.

1.3.5. Relying Parties

30. Relying parties are natural or legal persons other than the *Signatory* / *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*.

1.3.6. Other participants

31. No stipulation.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

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

33. The *Electronic Signature Certificates* issued under this *Certification Policy* are issued to *Public Servants*. These *Certificates* are valid as electronic signature systems under Public Sector Legal Regime Act 40/2015, 1 October, and under Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July.

34. *Pseudonym Certificates* will be issued to Administrations so requiring in order to be used in actions implemented by electronic means affecting classified information, public safety and security, national defence or other actions where anonymity is justified by law.

35. The scope of application of *Certificates* issued under the *Justice Administration Pseudonym Certificate* and *Justice Administration Pseudonym Centralised Signature Certificate* Policies exclusively comprises the Justice Administration.

36. *Electronic Seal Certificates* issued under this *Certification Policy* are issued to *Electronic Community* member agencies, as defined in the FNMT-RCM *GCPS Definitions* section, in order to guarantee the origin and integrity of content by creating the *Electronic Seal*.

37. The *Electronic Seal Certificates* issued under this *Certification Policy* are valid systems for identifying and creating an *Electronic Seal* for a Public Administration, body, agency or public-law entity, in accordance with Public Sector Legal Regime Act 40/2015, 1 October, and Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July, for the purposes of identifying and authenticating authority for an *Automated administrative action* and an *Automated judicial action*.

38. The *Issuance Law* governing these *Certificates* may, in the absence of specific legislation, determine the terms of use and rules applicable to these *Certificates*, thereby allowing

Administrations, agencies and entities to be attributed the different actions and decisions of their employees or of the *Electronic Seal* creators, all of which shall take place without any legal modification or change with respect to the actions carried out by these Public Administrations through traditional means.

1.4.2. Prohibited certificate uses

39. The restrictions on the use of *Electronic Signature Certificates* are set by reference to the various powers and functions of the Public Administration *Subscriber* (acting through a public servant as the *Certificate Signatory*), having regard to office, employment and, where appropriate, authorisation terms. FNMT-RCM and the Administrations, public agencies and entities may establish other additional restrictions by way of arrangements or agreements, in the relevant relationship document, or, if appropriate, in the *Issuance Law* governing those *Certificates*.

40. The restrictions on the use of the *Electronic Seal Certificates* are set by reference to the creation of electronic seals for a Public Administration, agency or public-law entity, under Act 40/2015 and Act 18/2011, 5 July, to identify and authenticate the exercise of power and for an *Automated administrative / judicial action* of a Public Administration’s organisational unit, public agency or entity.

41. FNMT-RCM shall have no control over actions taken with and use of *Electronic Signature Certificates* and the *Private key* by *Public Servants* on the Administration’s behalf, so FNMT-RCM will be saved harmless from the effects of any such uses, and from the consequences and implications, if any, of potential third-party claims or, where appropriate, actions for recovery.

42. As for activities carried out by *Registration Office* employees, FNMT-RCM shall have the obligations and responsibilities established in electronic signature laws, notwithstanding the specific provisions of article 11 of Royal Decree 1317/2001, 30 November, implementing article 81 of Tax, Administrative and Social Measures Act 66/1997, 30 December, in regard to the provision of security services by the Spanish mint Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, in communications with Public Administrations through electronic, information technology and telematics means. In order to be properly used, *Public Servant Electronic Signature Certificates* will require prior membership of the *Electronic Community* and that the Public Administration involved acquires *Subscriber* capacity.

43. FNMT-RCM and the Administration, agencies and entities may establish other additional restrictions by way of arrangements or agreements, or in the relevant relationship document, or, if appropriate, in the *Issuance Law* governing those *Certificates*.

44. In order to be properly used within the aforementioned limits, *Electronic Seal Certificates* will require prior membership of the *Electronic Community* and *User Entity* capacity to be acquired.

45. In any case, if a third party wishes to rely on the *Electronic signature* or *Electronic Seal Certificates* 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*.

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

- To sign or seal any other *Certificate*, except where previously authorised on a case-by-case basis.
- For personal or private uses, barring relations with Administrations where permitted.
- 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.
- Any use exceeding the purpose of this type of *Certificates* without the prior consent of FNMT-RCM.

1.5. POLICY ADMINISTRATION

1.5.1. Organisation administering the document

47. 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

48. 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
Email: ceres@fnmt.es
Telephone: 902 181 696

49. 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

50. 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

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

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

52. 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:

- *Automated administrative / judicial action*: Administrative / judicial action issued by a suitably programmed information system without an individual having to be involved in each particular case. This includes the issuance of procedural actions or actions resolving proceedings, and actions merely involving communication.
- *Public Employee Certificate:* This is the *Electronic Signature Certificate* with the details identifying the Public Servant and the Public Administration where the Public Servant is employed.
- *Public Employee Certificate in QSCD:* is the *Public Employee Certificate* whose keys, public and private, have been generated in a qualified signature creation device (*QSCD*)
- *Centralised Signature Certificate: Electronic Signature Certificate* designed for remote or server-based signatures. This means that *Public and private keys* are generated and stored in a secure environment belonging to FNMT-RCM, and it is guaranteed at all times that use of those *Keys* is exclusively controlled by the *Signatory*. Under this *SPPS* the following *Certificates* are issued as *Centralised Signature Certificates:*
    - ▪ *Public Employee Centralised Signature Certificate*
    - ▪ *Justice Administration Pseudonym Centralised Signature Certificate*
- *Justice Administration Pseudonym Centralised Signature Certificate:* Is the *Centralised Signature Certificate* whose *Signatory* will always belong to the Administration of Justice, and that links the *validation data* of a natural person and confirms the pseudonym granted by the Administration of Justice as a means of identification and signature under Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July 5.
- *Public Employee Centralised Signature Certificate:* Is the *Centralised Signature Certificate* issued to Personnel at the service of the Administration, which links the

validation data of said personnel, and confirms both their identity and that of the public Administration in which they provide service.

- *Electronic Signature Certificate:* For the purposes of this SPPS, this is a qualified *Certificate* issued to *Public Servants* containing their validation data and confirming both their identity and that of their Public Administration where they are employed. The following are *Electronic Signature Certificates*:
  - *Public Employee Certificate*
  - *Public Employee Certificate in QSCD*
  - *Public Employee Centralised Signature Certificate*
  - *Pseudonym Certificate*
  - *Justice Administration Pseudonym Certificate*
  - *Justice Administration Pseudonym Centralised Signature Certificate*
- *Pseudonym Certificate:* This is an *Electronic Signature Certificate* containing a natural person's *validation data* and confirming the pseudonym given by the administration.
- *Justice Administration Pseudonym Certificate:* This is an *Electronic Signature Certificate* containing a natural person's validation data and confirming the pseudonym given by the Justice Administration for identification and signature purposes under Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July.
- *Electronic Seal Certificate*: An electronic statement linking seal validation data to a legal person and confirming that person's name.
- *Specific Policy and Practice Statement (SPPS):* A specific *CPS* which applies to the issuance of a given set of *Certificates* issued by FNMT-RCM under the specific terms contained in that Statement and to which the specific Policies defined therein apply.
- *Signatory*: a *Public Servant* using his or her *Signature Creation Data*.
- *Supervisory body:* a body designated by a Member State responsible for supervisory tasks in the provision of trust services, in accordance with article 17 of the eIDAS Regulation.
- *Public Servants*: Civil servants, workers, statutory service personnel, authorised personnel or Public or employees serving in the Public or Justice Administration, public body, agency or public-law entity.
- *Policy and Practices of the server signing service:* Document that establishes the set of specific rules and procedures followed by the FNMT-RCM for the provision of its server signing service.
- *QSCD (Qualified signature creation device):* electronic signature creation device that meets the requirements listed in Annex II of Regulation (EU) 910/2014,
- *Registration Operations Officer*: A natural person appointed by the representative of the Public Administration, public agency or public-law entity whose duty it is to oversee the tasks assigned to the *Registration Office*, and who has the obligations

and responsibilities provided for in these *Specific Policies and Certification Practices*.

- *Subscriber*: The Public Administration, public body, agency or public-law entity.

1.6.2. References

53. 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

54. 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

55. 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

56. 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.

57. The CRL publication frequency is defined in section “4.9.7 Additional features. Time and frequency of publication”.

2.4. ACCESS CONTROLS ON REPOSITORIES

58. 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

59. *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

60. 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.

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

3.1.2. Need for names to be meaningful

62. 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).

63. The Common Name field of *Electronic Signature Certificates* defines the *Public Servant* to whom the *Certificate* has been issued.

64. The Common Name field of Electronic Seals contains 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

65. *Electronic Signature Certificates* issued by FNMT-RCM under these Specific Certification Policies and Certification Practices using pseudonyms shall clearly specify this feature, in accordance with the eIDAS Regulation and the applicable national laws.

66. The use of pseudonyms as a method for identifying the *Subscriber* is not established for *Electronic Seal Certificates* and the CN attribute contains the name of the automatic process application or system for which the *Certificate* is issued.

3.1.4. Rules for interpreting various name forms

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

3.1.5. Uniqueness of names

68. 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

69. 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 possession of private key

70. FNMT-RCM neither generates nor stores the *Private Keys* associated with *Public Employee Certificates*, *Pseudonym Certificates* or *Justice Administration Pseudonym Certificates* issued

under these *Specific Certification Policies and Certification Practices*, the generation of which is exclusively controlled by the *Signatory* and, if appropriate, with the involvement of the relevant *Registration Office*, and custody of which is the responsibility of the *Public Servant*.

71. For the issuance of the *Public Employee Certificates on QSCD*, it will be required and verified that the *Applicant, Personnel at the service of the Administration*, generates the public and private Keys in a qualified signature creation device.

72. The issuance of *Centralised Signature Certificates* shall require that the *Applicant.*, a *Public Servant,* generate the *Public and private keys* in FNMT-RCM's system, after being registered therein and once that generation is validated by the *Registration Office*, after the aforementioned *Applicant's* identity has been checked and the *Applicant's* consent has been obtained.

73. In the case of *Centralised Signature Certificates*, after the *Applicant* is informed that the *Applicant's Certificate* is to be issued, the system generates the *Key* pair, and the *Private key* will therefore be stored and protected, guaranteeing that its use will be exclusively controlled by the *Public Servant*.

74. FNMT-RCM neither generates nor stores the *Key* pair associated with the *Electronic Seal Certificates* issued under this Certification Policy, and does everything that is necessary during the Seal *Application* procedure in order to make sure that the *Registration Operations Officer* and/or the *Subscriber's* representative is in possession of the Private Key associated with the Public Key to be certified.

3.2.2. Authentication of organisation identity

75. Before entering into any institutional relationship with *Subscribers*, FNMT-RCM uses the website addresses and means referred to in these *Specific Certification Practices* and otherwise the *GCPS* to inform about the terms of service and representations, warranties and responsibilities of the parties involved in the issuance and use of the *Certificates* issued thereby in its capacity as *Trust Service Provider*.

76. The identity checks of *Public Servants*, *Applicants* for both *Electronic Signature* and *Electronic Seal Certificates*, will be carried out by authorised employees of the *Registration Offices* set up by the relevant Public Administration body, agency or entity, thereby guaranteeing the identity of the Administration *Certificate Subscriber*, which is in each case the agency or entity where the servant is employed.

77. For *Electronic Seal Certificates*, FNMT-RCM will consider and have authority to decide as to any application for an *Electronic Seal Certificate* by the relevant *Registration Operations Officer*, acting as the *Subscriber's* representative.

78. Therefore, and in this connection, *Registration Offices* shall not be deemed to be authorities with powers delegated by or reporting to FNMT-RCM.

3.2.3. Authentication of individual applicant identity

79. For the record, FNMT-RCM will consider, based on the list of dependent user employees submitted by the Administration, public agency or entity, for which the relevant body, agency and/or entity will be responsible, acting through the *Registration Offices*, that these are incumbent employees, that their Personal Identification number, employment or authorisation is authentic and in force and, therefore, that they have authority to obtain and use *Electronic Signature Certificates*. FNMT-RCM shall not be responsible, insofar as this type of *Certificate* is concerned, for checking the servant's position or employment or that these requirements continue to be met throughout the life of the *Certificate*, because FNMT-RCM has no legal civil service, administrative or employment relationship whatsoever with those employees, beyond the document containing the terms of use or, as the case may be, the issuance agreement, the effect of which is strictly instrumental for the discharge of employment-related duties.

80. The above-mentioned checks shall be carried out by officers at the *Registration Offices* set up by the relevant Public Administration body, agency or entity, which shall in each case be the agency or entity where the servant is employed. Therefore, and in this connection, *Registration Offices* shall not be deemed to be authorities with powers delegated by or reporting to FNMT-RCM.

3.2.3.1 Direct check by physical presence

81. *Applicants* for *Electronic Signature Certificates* shall be physically present in order for their personal identity to be formally confirmed, through any of the identification means legally admitted under the national laws in force, and will go to the *Registration Office* designated for that purpose by the *Subscriber* body, public agency or entity where the servant is employed. That *Registration Office* is created by the *Subscriber* Public Administration, which provides FNMT-RCM with a list of persons authorised to perform these Registration activities, in accordance with the procedures established for such purpose, and notifies any change to the Office structure.

82. The *Applicant* for *Electronic Seal Certificates* is the *Registration Operations Officer* and/or the *Subscriber's* representative or the person with delegated powers of the organisational unit that needs to be identified or carry out the *Automated administrative / judicial action* with this type of *Certificates*, and is employed by a Public Administration, public agency or public-law entity in which that organisational unit is located.

3.2.3.2 Verification using electronic identification means

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

- A *Public Employee Certificate* issued by the FNMT-RCM, or by a *Trust Service Provider* with which an agreement is reached for this purpose, in the request for in the application of a:

  - *Public Employee Certificate*
  - *Justice Administration Pseudonym Certificate*
  - *Public Employee Centralised Signature Certificate*
  - *Justice Administration Pseudonym Centralised Signature Certificate*

- A *Justice Administration Pseudonym Certificate* issued by the FNMT-RCM in the application of a:
  - *Justice Administration Pseudonym Certificate*
  - *Justice Administration Pseudonym Centralised Signature Certificate*

- A *Pseudonym Certificate* issued by the FNMT-RCM in the application of a:
  - *Pseudonym Certificate*

- A *Certificate for natural person* issued by the FNMT-RCM in the application of a*:*
  -
  - *Justice Administration Pseudonym Centralised Signature Certificate*

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

3.2.3.3 Indirect check by reliable means equivalent to physical presence under national Law

85. There will be no need for physical presence where the *Registration Office* of the competent Administration body is acquainted with the identity or other permanent circumstances of the applicants for the *Certificates* (identity, validity of the position and other terms to be included in the *Certificate*) based on a previously existing relationship between those *Applicants* and the Administration where they serve, provided that it is guaranteed that those *Applicants* (*Public Servants*) were identified by physical presence (as described in the preceding paragraph), and less than five years have elapsed since their physical presence.

3.2.4. Non-verified Subscriber information

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

3.2.5. Validation of authority

87. The Registration Authority verifies that the *Applicant* for an *Electronic Signature Certificate* issued under this SPPS has been previously authorised by the Subscriber to submit that application.

88. In addition, in the case of *Electronic Seal Certificates*, the FNMT-RCM Registration Authority verifies that the applicant for a Seal has sufficient authority through the applicant's appointment as *Registration Operations Officer* and the electronic signature used for the application form, as described in section 3.2.3 of this SPPS, and accepts the use of a qualified *Certificate* by the representative of a sole or joint director of the legal person *Subscriber* or a

qualified *Certificate* by *Public Servants*, where authority to issue the same has been established.

3.2.6. Criteria for interoperation

89. There are no interactivity relationships with Certification Authorities external to FNMT-RCM.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

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

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

3.3.1. Identification and authentication for routine re-key

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

3.3.2. Identification and authentication for re-key after revocation

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

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

94. 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.

95. 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

96. Only *Public Servants*, previously authorised by the *Subscriber*, may apply for this type of *Certificates*.

4.1.2. Registration process and responsibilities

97. *Applicants*, *Public Servants*, through *Certificate* application web-based software developed for that purpose, will accept the terms of use of the *Certificate* and provide their identification particulars, including, but not limited to, Tax Identification Number (NIF), first surname, Tax Identification Number of the agency where they are employed, and their email address to which an application code shall be sent. In the case of *Electronic Seal Certificates*, the *Registration Operations Officer*, the *Subscriber's* representative, shall be in charge of signing and sending the *Certificate* issuance agreement to FNMT-RCM.

98. After receiving this information, FNMT-RCM will check that the information on the signed application is valid, and the size of keys generated.

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

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing identification and authentication functions

100. For *Electronic Signature Certificates*, *Applicants* will supply the requested information and evidence of their personal identity and *Public Servant* status. For *Pseudonym Certificates* to be issued, FNMT-RCM shall, through the *Registration Office,* check the *Signatory's* true identity and retain the supporting documentation. FNMT-RCM shall in any event accept the function performed and report prepared by the Administration's designated *Registration Office*.

101. In the case of *Centralised Signature Certificates*, *Applicants* shall, during the process to establish their identity, sign the terms of use of the *Certificate*, and will be provided with identification credentials (user and first part of the password). Applicants will subsequently receive an email with the second part of the password.

102. In the case of *Electronic Seal Certificates*, identification and documentation will at all times be validated from FNMT-RCM's Office. Upon receiving the agreement sent and signed by the *Registration Operations Officer*, FNMT-RCM shall promptly:

- Check that the *Certificate Subscriber* exists and that its details are correct.
- Check that the person signing the agreement is the *Registration Operations Officer* and therefore has the *Subscriber's* permission to proceed to apply for the *Electronic Seal Certificate*.

103. For *Electronic Signature Certificates* to be issued, FNMT-RCM may identify *Applicants*, other than by their physical presence at the *Registration Office*, using a *qualified Electronic Signature Certificate* issued to *Public Servants,* thereby guaranteeing the authenticity of all fields to be included in the *Certificate* to be issued, provided that not more than five years have elapsed since the *Signatory* was identified.

104. FNMT-RCM may agree with Administrations, public agencies and entities so requesting to create delegated Registration Offices in order to centralise the performance of registration

procedures for other related or dependent Administrations that do not have sufficient means to do so, in conformity with cost rationalisation laws.

4.2.2. Approval or rejection of certificate applications

105. In the case of *Electronic Signature Certificates,* once the *Registration Office* has confirmed the *Applicant's* identity and incumbency or employment, the *Office* will validate the information and send it signed, along with the application code obtained at the application stage.

106. In the case of *Centralised Signature Certificates*, once the information is confirmed, the *Applicant* shall be registered in FNMT-RCM's system to be provided with complete identity credentials. Keys will be generated once the *Signatory* configures the signature password which shall protect the keys and request generation of signature identity. These actions will be carried out accessing the *Certificate* application software (Identity Management Portal) with a high level of security.

107. Information will be submitted to FNMT-RCM via secure communications established for such purpose between the *Registration Office* and FNMT-RCM.

108. 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.

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

4.2.3. Time to process applications

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

111. The time to process applications for *Electronic Seal Certificates* the minimum required after FNMT-RCM's *Registration Office* receives all documentation necessary to perform the checks required before the *Certificate* is issued. FNMT-RCM shall provide the *Applicant* with a mechanism to download the *Certificate.*

4.3. CERTIFICATE ISSUANCE

4.3.1. CA actions during issuance

112. Once FNMT-RCM receives the *Applicant's* personal information, information describing the *Applicant's* relationship with the Public Administration, and the application code obtained at the application stage, the *Certificate* will be issued.

113. The issuance of *Certificates* results in the generation of electronic documents confirming the information to be included in the *Certificate*, and that it matches the associated *Public Key*. FNMT-RCM *Certificates* may only be issued by FNMT-RCM in its capacity as *Trust Service*

Provider, and no other entity or organisation has authority to issue the same. The FNMT-RCM *Certification Authority* only accepts *Certificate* generation applications from authorised sources. The information contained in each application is fully protected against alterations through *Electronic Signature* or *Electronic Seal* mechanisms prepared using *Certificates* issued to those authorised sources.

114. 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 as provided for in the agreements or arrangements and, as the case may be, those provided for in the relevant *Issuance Law*.

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

- To check that the *Certificate Applicant* or the *Registration Operations Officer* 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.

116. 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.

   The attribute *CN* contains the *Public Servant's* identification data. Where *Pseudonym Certificates* are issued for *Public Servants*, the attribute *CN* includes that pseudonym. And in the case of *Electronic Seals*, the attribute *CN* contains the name of the automatic process application or system for which the *Certificate* is issued.

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

117. 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/.

118. Within the process of issuing the *Public Employee Certificates in QSCD*, it will be verified that the device used to generate keys is a qualified signature creation device (*QSCD*) in accordance with the eIDAS Regulation.

119. In processing issuance of *Centralised Signature Certificates*, the system requires *Applicants* to identify themselves using the credentials received plus a second authentication factor which

shall be sent to their email address[2] and, once their identity has been verified, they must expressly request the issuance of their *Centralised Signature Certificate*. The infrastructure thereby securely links the identification details provided by Applicants, as described in section "4.1.2 Registration process" hereof, with the process to generate their *Certificate*.

120. The system will then generate the *Public and private keys* in a protected HSM and issue the requested *Centralised Signature Certificate* to the *Public Servants*. In addition, the system requires *Applicants* to establish their signature password which they will have be asked to provide when carrying out transactions using their *Private key*. This password is not known (or stored) at any time by FNMT-RCM's system.

4.3.2. Notification of issuance

121. Upon the *Electronic Certificate and Electronic Seal Signature* being issued, FNMT-RCM will inform *Public Servants* that the *Certificate* is available for download.

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1. Conduct constituting certificate acceptance

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

4.4.2. Publication of the certificate by the CA

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

4.4.3. Notification of issuance to other entities

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

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Private key and certificate usage

125. FNMT-RCM neither generates nor stores the Private Keys associated with *Certificates* issued under this Certification Policy, with the exception of *Centralised Signature Certificates*.

[2] FNMT-RCM may use other communication methods to submit this second authentication factor, subject to the *Applicant's* prior consent, namely for instance the use of mobile telephones with a previously accredited number.

Custody of and responsibility for controlling the *Certificate* keys lies with *Public Servants* and, for *Centralised Signature Certificates*, with FNMT-RCM.

126. These *Certificates* are valid electronic signature systems as provided for in Public Sector Legal Regime Act 40/2015, 1 October, and in Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July.

127. The *Electronic Seal Certificates* issued under this Certification Policy are valid systems for identifying and creating an *Electronic Seal* for a Public Administration, body, agency or public-law entity, in accordance with Public Sector Legal Regime Act 40/2015, 1 October, and Justice Administration Information and Communication Technologies Use Act 18/2011, 5 July, for the purposes of identifying and authenticating authority for an *Automated administrative action* and an *Automated judicial action*.

4.5.2. Relying party public key and certificate usage

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

4.6. CERTIFICATE RENEWAL

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

4.6.1. Circumstances for certificate renewal

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

4.6.2. Who may request renewal

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

4.6.3. Processing certificate renewal requests

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

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

134. 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

135. 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 other entities

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

4.7. CERTIFICATE RE-KEY

137. 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

138. *Certificates* shall be re-keyed in the following events:

- Where the current keys will expire soon, upon request by the renewal requestor.
- Due to key compromise or any other circumstance set out in section "*4.9 Certificate revocation and suspension"* of this *SPPS.*

4.7.2. Who may request re-key

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

4.7.3. Processing certificate re-keying requests

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

4.7.4. Notification of certificate re-key

141. 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

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

4.7.6. Publication of the re-keyed certificate

143. 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

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

4.8. CERTIFICATE MODIFICATION

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

4.8.1. Circumstance for certificate modification

146. The modification is not stipulated.

4.8.2. Who may request certificate modification

147. The modification is not stipulated.

4.8.3. Processing certificate modification requests

148. The modification is not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

149. The modification is not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

150. The modification is not stipulated.

4.8.6. Publication of the modified certificate by the CA

151. The modification is not stipulated.

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

152. The modification is not stipulated.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

153. *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.

154. 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*.

155. 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

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

157. The following are 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) Cancellation of the *Signatory's* identification credentials in the case of *Centralised Signature Certificates.*

158. FNMT-RCM shall in no case accept any obligation whatsoever to check the particulars referred to in c) to e) above, which this entity must be duly notified of by delivering the documents and information required for the same to be checked.

159. FNMT-RCM will only be responsible for the consequences of the failure to revoke a *Certificate* in the following events:

- Where it should have been revoked following termination of the agreement entered into with the *Subscriber*
- Where revocation was requested through the *Subscriber's* relevant *Registration Office* observing the procedure established for this type of *Certificates*
- Where it received notice of the revocation request or the underlying cause by means of a court or administrative decision.
- Where it is duly provided with proof of the grounds referred to in c) to e) above, after the revocation *Requestor* is identified.

160. FNMT-RCM shall be held harmless in the event of actions in the nature of criminal offences or misdemeanours which FNMT-RCM is unaware of in connection with the data or the *Certificate*, data inaccuracies or untimely communication thereof to FNMT-RCM.

161. In addition to their termination and the inability to carry on using the *Signature creation data* or associated private keys, the revocation of a *Certificate* terminates the relationship and terms of use of that *Certificate* and its *Private key* with FNMT-RCM.

4.9.1.2 Reasons for revoking a subordinate CA certificate

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

4.9.2. Who can request revocation

163. Revocation of a *Certificate* may only be requested by:

- the *Certification Authority* and the *Registration Authority*
- the *Subscriber* through its representative or authorised person, at the Registration Office with authority for that purpose

- as the case may be, the *Signatory,* calling the telephone number provided for that purpose (subject to identification of the Requestor) and posted at FNMT-RCM's website, which shall be operational 24x7, or through that Registration Office.

164. 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

165. An *Electronic Signature and Electronic Seal Certificates* revocation request may be made during the validity period specified in the *Certificate*.

166. 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.

167. During telephone revocation, the requestor 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.

168. Additionally, a request for revocation of any *Certificate* may be made through the *Registration Office.* Personal information and processing of such information shall be subject to specific laws. The revocation process at the Registration Office is as follows:

- For *Electronic Signature Certificates*, the requestor shall go to the *Registration Office,* where the requestor's identity shall be established, along with the requestor's capacity to revoke that *Certificate,* and the ground for revocation shall be specified. The Office will send the information to FNMT-RCM electronically using registration software, and will process revocation of the *Certificate*.

- For *Electronic Seal Certificates*, the requestor shall submit to the *Registration Office* the duly completed and signed form created for that purpose. Once the *Registration Office* receives the documentation, it shall check and validate the information, and the requestor's authority to request revocation, and revocation of the *Certificate* shall be processed if everything is in order.

169. The only *Registration Office* able to validate revocations of *Electronic Seal Certificates* is FNMT-RCM's Office.

170. As soon as revocation is effective, the following will be notified using the email address provided:

- The *Signatory* and the requestor in the case of an *Electronic Signature Certificate*

- The *Subscriber's* representative who requested revocation in the case of an *Electronic Seal Certificate.*

171. 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.

4.9.4. Revocation request grace period

172. 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

173. FNMT-RCM processes *Certificate* revocation immediately upon checking the *Requestor'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.

4.9.6. Revocation checking requirement for relying parties

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

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

4.9.7. CRL issuance frequency

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

4.9.8. Maximum latency for CRLs

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

4.9.9. On-line revocation/status checking availability

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

4.9.10. On-line revocation checking requirements

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

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

4.9.11. Other forms of revocation advertisements available

179. Not defined.

4.9.12. Special requirements related to key compromise

180. See the relevant section in the *GCPS*.

4.9.13. Circumstances for suspension

181. *Certificate* suspension is not supported.

4.9.14. Who can request suspension

182. *Certificate* suspension is not supported.

4.9.15. Procedure for suspension request

183. *Certificate* suspension is not supported.

4.9.16. Limits on suspension period

184. *Certificate* suspension is not supported.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational characteristics

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

4.10.2. Service availability

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

4.10.3. Optional features

187. Not stipulated.

4.11. END OF SUBSCRIPTION

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

189. It is noted in the above connection that where an application for FNMT-RCM to issue an *Electronic Signature Certificate* and the same *Signatory* and same *Subscriber* have another *Certificate* in force under the same *Issuance Law*, the first *Certificate* obtained will be revoked. This shall not occur in the case of *Electronic Seal Certificates.*

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policy and practices

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

191. In the case of *Centralised Signature Certificates*, where the password protecting access to that *Key* by the *Signatory* is lost, that *Certificate* must be revoked and a request must be made for a new one to be issued.

4.12.2. Session key encapsulation and recovery policy and practices

192. No stipulation.

5. PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

193. See the relevant section in the *GCPS*.

5.1. PHYSICAL SECURITY CONTROLS

194. See the relevant section in the *GCPS*.

5.1.1. Site location and construction

195. See the relevant section in the *GCPS*.

5.1.2. Physical access

196. See the relevant section in the *GCPS*.

5.1.3. Power and air conditioning

197. See the relevant section in the *GCPS*.

5.1.4. Water exposures

198. See the relevant section in the *GCPS.*

5.1.5. Fire prevention and protection

199. See the relevant section in the *GCPS.*

5.1.6. Media storage

200. See the relevant section in the *GCPS.*

5.1.7. Waste disposal

201. See the relevant section in the *GCPS.*

5.1.8. Off-site backup

202. See the relevant section in the *GCPS.*

5.2. PROCEDURAL CONTROLS

203. See the relevant section in the *GCPS.*

5.2.1. Trusted roles

204. See the relevant section in the *GCPS.*

5.2.2. Number of persons required per task

205. See the relevant section in the *GCPS.*

5.2.3. Identification and authentication for each role

206. See the relevant section in the *GCPS.*

5.2.4. Roles requiring separation of duties

207. See the relevant section in the *GCPS.*

5.3. PERSONNEL CONTROLS

208. See the relevant section in the *GCPS.*

5.3.1. Qualifications, experience, and clearance requirements

209. See the relevant section in the *GCPS*.

5.3.2. Background check procedures

210. See the relevant section in the *GCPS*.

5.3.3. Training requirements

211. See the relevant section in the *GCPS*.

5.3.4. Retraining frequency and requirements

212. See the relevant section in the *GCPS*.

5.3.5. Job rotation frequency and sequence

213. See the relevant section in the *GCPS*.

5.3.6. Sanctions for unauthorized actions

214. See the relevant section in the *GCPS*.

5.3.7. Independent contractor requirements

215. See the relevant section in the *GCPS*.

5.3.8. Documentation supplied to personnel

216. See the relevant section in the *GCPS*.

5.4. AUDIT-LOGGING PROCEDURES

217. See the relevant section in the *GCPS*.

5.4.1. Types of events recorded

218. See the relevant section in the *GCPS*.

5.4.2. Frequency of processing log

219. See the relevant section in the *GCPS*.

5.4.3. Retention period for audit log

220. See the relevant section in the *GCPS*.

5.4.4. Protection of audit log

221. See the relevant section in the *GCPS*.

5.4.5. Audit log backup procedures

222. See the relevant section in the *GCPS*.

5.4.6. Audit collection system (internal vs. external)

223. See the relevant section in the *GCPS*.

5.4.7. Notification to event-causing subject

224. See the relevant section in the *GCPS*.

5.4.8. Vulnerability assessments

225. See the relevant section in the *GCPS*.

5.5. RECORDS ARCHIVAL

226. See the relevant section in the *GCPS*.

5.5.1. Types of records archived

227. See the relevant section in the *GCPS*.

5.5.2. Retention period for archive

228. See the relevant section in the *GCPS*.

5.5.3. Protection of archive

229. See the relevant section in the *GCPS*.

5.5.4. Archive backup procedures

230. See the relevant section in the *GCPS*.

5.5.5. Requirements for time-stamping of records

231. See the relevant section in the *GCPS*.

5.5.6. Audit collection system (internal vs. external)

232. See the relevant section in the *GCPS*.

5.5.7. Procedures to obtain and verify archive information

233. See the relevant section in the *GCPS*.

5.6. CA KEY CHANGEOVER

234. See the relevant section in the *GCPS*.

5.7. COMPROMISE AND DISASTER RECOVERY

235. See the relevant section in the *GCPS*.

5.7.1. Incident and compromise handling procedures

236. See the relevant section in the *GCPS*.

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

237. See the relevant section in the *GCPS*.

5.7.3. Entity private key compromise procedures

238. See the relevant section in the *GCPS*.

5.7.4. Business continuity capabilities after a disaster

239. See the relevant section in the *GCPS*.

5.8. TRUST SERVICE PROVIDER TERMINATION

240. See the relevant section in the *GCPS*.

6. TECHNICAL SECURITY CONTROLS

241. 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

242. 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

243. No stipulation.

6.1.1.3 Subscriber key pair generation

244. As for *Subscriber Key* generation, other than for *Public Employee Centralised Signature Certificates*, 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:

- *Public Servants* in the case of *Electronic Signature Certificates*.
- The *Registration Operations Officer* or the person authorised thereby in the case of *Electronic Seal Certificates.*

245. *Private Keys* associated with the *Public Employee Certificates in QSCD* are generated and kept in a *Qualified signature creation device* that meets the requirements listed in Annex II of the eIDAS Regulation.

246. *Private keys* associated with *Centralised Signature Certificates* are generated and held securely by FNMT-RCM's signature activation module, so that those *Keys* are accessed by means reliably guaranteeing exclusive control by the *Signatory*.

6.1.2. Private key delivery to the subscriber

247. There is no Private key delivery in the issuance of *Certificates* under these *Certification Policies and Practices*.

248. The *Private keys* associated with *Centralised Signature Certificates* are generated in a signature creation device exclusively controlled by the *Signatory*, where they will be held securely for use. The *Private key* is not therefore delivered to the *Signatory* in this case.

249. 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

250. 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

251. See the relevant section in the *GCPS*.

6.1.5. Key sizes and algorithms used

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

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

- Root FNMT CA keys: 4096 bytes.
- Subordinate Public Sector CA Keys*:* 4096 bytes.
- *Electronic Signature and Electronic Seal Certificate* Keys*:* 2048 bytes.

6.1.6. Public key parameters generation and quality checking

254. See the relevant section in the *GCPS*.

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

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

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

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

258. The key usage purposes of *Public Employee Certificates*, *Public Employee Certificates in QSCD*, *Pseudonym Certificates*, *Justice Administration Pseudonym Certificates* and *Electronic Seal Certificates* are exclusively for encryption, authentication and signature purposes.

259. The usage purpose of *Public Employee Centralised Signature Certificates* is exclusively use of signature.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic module standards and controls

260. See the relevant section in the *GCPS*.

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

261. See the relevant section in the *GCPS*.

6.2.3. Private key escrow

262. 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.

263. *Private Keys* associated with the *Public Employee Certificates in QSCD* are generated and kept in a *Qualified signature creation device* that meets the requirements listed in Annex II of the eIDAS Regulation.

264. The *Private keys* of *Public Employee Centralised Signature Certificates* issued to end users (*Signatories*) are held safely in FNMT-RCM's systems so that only *Signatories* may access their *Private key*. Access is guaranteed through the use of *Signatories'* identification credentials and their signature password (only known to *Signatories*), plus a second authentication factor consisting of a single-use password.

6.2.4. Private key backup

265. See the relevant section in the *GCPS*.

6.2.5. Private key archival

266. See the relevant section in the *GCPS*.

6.2.6. Private key transfer into or from a cryptographic module

267. See the relevant section in the *GCPS*.

6.2.7. Private key storage on cryptographic module

268. See the relevant section in the *GCPS*.

6.2.8. Activating private keys

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

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

271. End-entity *Centralised Signature Certificate Private key* activation and use is based on use by *Signatories* of their identification credentials and signature password (known only to them), plus a second authentication factor in the form of a single-use password.

6.2.9. Deactivating private keys

272. See the relevant section in the *GCPS*.

6.2.10. Destroying private keys

273. 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.

274. End-entity *Public Employee Centralised Signature Certificate Private keys* will be destroyed once their period of use is over or when the *Signatories'* relationship with FNMT-RCM terminates. In any case, private key destruction shall be preceded by revocation of the *Public Employee Centralised Signature Certificate*.

6.2.11. Cryptographic module capabilities

275. See the relevant section in the *GCPS*.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

276. See the relevant section in the *GCPS*.

6.3.2. Certificate operational periods and key pair usage periods

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

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

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

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

279. Key activation data for *Public Employee Centralised Signature Certificates* is generated by the signature activation module in the same manipulation-proof environment as the *Trust Service Provider's* signature creation device, guaranteeing that such generation can only be carried out under the future *Signatory's* exclusive control.

6.4.2. Activation data protection

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

281. The password protecting access to the *Centralised Signature Certificate Private key* is confidential, personal and non-transferable. *Signatories*, who also need a second authentication factor to activate their *Private key*, are therefore responsible for protecting their activation data.

6.4.3. Other aspects of activation data

282. No stipulations.

6.5. COMPUTER SECURITY CONTROLS

283. See the relevant section in the *GCPS*.

6.5.1. Specific computer security technical requirements

284. See the relevant section in the *GCPS*.

6.5.2. Computer security rating

285. See the relevant section in the *GCPS*.

6.6. LIFE CYCLE TECHNICAL CONTROLS

286. See the relevant section in the *GCPS*.

6.6.1. System development controls

287. See the relevant section in the *GCPS*.

6.6.2. Security management controls

288. See the relevant section in the *GCPS*.

6.6.3. Life cycle security controls

289. See the relevant section in the *GCPS*.

6.7. NETWORK SECURITY CONTROLS

290. See the relevant section in the *GCPS*.

6.8. TIME-STAMPING

291. See the relevant section in the *GCPS*.

6.9. OTHER ADDITIONAL CONTROLS

292. See the relevant section in the *GCPS*.

6.9.1. Control of the ability to provide services.

293. See the relevant section in the *GCPS*.

6.9.2. Control of systems development and computer applications

294. See the relevant section in the *GCPS*.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

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

296. *Electronic Seal Certificates* are issued as “qualified” *Certificates* in accordance with European standards ETSI IN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates” and ETSI IN 319 412-3 “Certificate profile for certificates issued to legal persons”.

7.1.1. Version number

297. *Electronic Signature and Electronic Seal Certificates* conform to standard X.509 version 3.

7.1.2. Certificate extensions

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

7.1.3. Algorithm object identifiers

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

7.1.4. Name forms

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

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

7.1.5. Name constraints

302. 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

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

7.1.7. Usage of policy constraints extension

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

7.1.8. Policy qualifiers syntax and semantics

305. 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

306. 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

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

7.2.2. CRL and CRL entry extensions

308. The CRL profile has the following structure:

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	Distribution point URLs and CRL scope
ExpiredCertsOnCRL	CA NotBefore value
Revoked Certificates	Certificate revocation list, containing at least serial number and revocation date for each entry

Table 3 – CRL profile

7.3. OCSP PROFILE

7.3.1. Version number

309. See the relevant section in the *GCPS*.

7.3.2. OCSP extensions

310. See the relevant section in the *GCPS*.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

311. 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".

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

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

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

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

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

8.2. QUALIFICATIONS OF ASSESSOR

315. See the relevant section in the *GCPS*.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

316. See the relevant section in the *GCPS*.

8.4. TOPICS COVERED BY ASSESSMENT

317. See the relevant section in the *GCPS*.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

318. See the relevant section in the *GCPS*.

8.6. COMMUNICATION OF RESULTS

319. See the relevant section in the *GCPS*.

8.7. AUTOEVALUATION

320. See the relevant section in the *GCPS*.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

321. See the relevant section in the *GCPS*.

9.1.1. Certificate issuance or renewal fees

322. See the relevant section in the *GCPS*.

9.1.2. Certificate access fees

323. No stipulation.

9.1.3. Revocation or status information access fees

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

9.1.4. Fees for other services

325. See the relevant section in the *GCPS*..

9.1.5. Refund policy

326. 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

327. See the relevant section in the *GCPS*.

9.2.1. Insurance coverage

328. See the relevant section in the *GCPS*.

9.2.2. Other assets

329. See the relevant section in the *GCPS*.

9.2.3. Insurance or warranty coverage for end-entities

330. See the relevant section in the *GCPS*.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

331. See the relevant section in the *GCPS*.

9.3.1. Scope of confidential information

332. See the relevant section in the *GCPS*.

9.3.2. Information not within the scope of confidential information

333. See the relevant section in the *GCPS*.

9.3.3. Responsibility to protect confidential information

334. See the relevant section in the *GCPS*.

9.4. PRIVACY OF PERSONAL INFORMATION

335. See the relevant section in the *GCPS*.

9.4.1. Privacy plan

336. See the relevant section in the *GCPS*.

9.4.2. Information treated as private

337. See the relevant section in the *GCPS*.

9.4.3. Information not deemed private

338. See the relevant section in the *GCPS*.

9.4.4. Responsibility to protect private information

339. See the relevant section in the *GCPS*.

9.4.5. Notice and consent to use private information

340. See the relevant section in the *GCPS*.

9.4.6. Disclosure pursuant to judicial or administrative process

341. See the relevant section in the *GCPS*.

9.4.7. Other information disclosure circumstances

342. See the relevant section in the *GCPS*.

9.5. INTELLECTUAL PROPERTY RIGHTS

343. See the relevant section in the *GCPS*.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA representations and warranties

344. FNMT-RCM’s representations and warranties as *Trust Service Provider* to the person associated with the *Certificate*, who acts as *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*.

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

346. The rights and obligations of Administrations, agencies, public entities and FNMT-RCM shall be governed by the relevant agreement or arrangement regulating the provision of the trust services. These agreements or arrangements may establish the *Issuance Law* governing these *Certificates* with the content and for the purpose referred to in this Statement.

347. See the relevant section in the *GCPS*.

9.6.2. RA representations and warranties

348. In addition to the participants' representations and warranties set out herein and in the *GCPS*, *Registration Offices* and/or the *Registration Operations Officer* have the following obligations:

- To thoroughly check the information as to identity and appointment to office, job, employment or any other information reflecting or defining the Public Servant's relationship as *Certificate Signatory* with the Administration, agency or entity where the Public Servant is employed (*Certificate Subscriber*).
- The *Trust Service Provider*, through the *Registration Operations Officer*, will make sure that the procedures approved by FNMT-RCM to identify Certificate Applicants are fulfilled and will inform *Certificate* users how to use them properly, in accordance with the terms of use, the Certification Policies and Practices and the applicable laws.
- Not to register or process applications by employees serving in an entity other than the entity for which they are acting, or with respect to which the Registration Office has no power or authority to act as such, without prejudice to centralised Registration Offices being created or agreements being entered into between administrations for registrations to be made.
- Not to register or process applications for Certificates issued under these policies and where the Applicant has not been authorised by the *Registration Operations Officer*.
- Not to process Pseudonym Certificates, other than for use in actions implemented by electronic means affecting classified information, public safety and security, national defence or other actions where anonymity is justified by law.
- To request revocation of the *Certificate* forthwith upon learning of any of the trigger events specified in section 4.9.1 of this SPPS.

349. See the relevant section in the *GCPS*.

9.6.3. Subscriber and signatory representations and warranties

350. In addition to the participants' representations and warranties set out in the *GCPS*, the *Public Servant*, as the *Certificate Signatory*, and/or as the case may be the *Certificate Subscriber*, have the following obligations:

- Not to use the *Certificate* where any of the information as to office, job, employment or any other information is inaccurate or incorrect or does not reflect or define the relationship with the body, agency or entity where the Public Servant is employed, or where security reasons so advise.
- To properly use the *Certificate* based on the powers and authorities conferred by the *Public Servant's* office, job or employment.
- To notify the *Registration Operations Officer* of any of the trigger events specified in section 4.9.1 of this SPPS, in order to start processing revocation of the *Certificate*.

351. The natural person associated with the *Public Employee Certificate in QSCD and Centralised Signature Certificate* acting as *Signatory* shall also comply with the security rules regarding custody and use of the signature password, as confidential, personal and non-transferable information that guarantees access to the *Signatory's Private keys*. That *Signatory* must therefore observe the following precautions in relation to the signature password,:

- To hold it in confidence, and not to disclose it to third parties.
- To memorise it and not to write it down on any physical or electronic document.
- To change it forthwith upon suspecting that a third party may know it.
- To notify FNMT-RCM of any possible loss of control over the Private key, in order for the *Public Employee Centralised Signature Certificate* and associated Keys to be revoked.
- Not to choose a password that may be easily inferred from the *Signatory's* personal information or a predictable password (date of birth, telephone, consecutive number series, same character repetitions, etc.).
- To observe FNMT-RCM's security policy with respect to password composition, regular password change, etc.
- Digital signatures are only created by a QSCD device.

352. The *Signatory* will be responsible for informing FNMT-RCM of any change to the status or information recorded in the *Certificate*, in order for the *Certificate* to be revoked and re-issued.

353. In any case, the *Signatory* shall not use the *Signature Creation Data* or private keys associated with the *Signatory's Certificate* where its validity period has expired or the Provider's *Signature / Seal Creation Data* may be under threat and/or compromised and the *Signatory* has been so advised by the Provider or, as the case may be, is aware, suspects or has learned of any such circumstances. The *Signatory's* breach of this requirement shall make the *Signatory* liable for the consequences of acts, documents or transactions signed in any such circumstances, and for any costs, damages and losses arising for FNMT-RCM or third parties if the *Certificate* is used beyond its validity period.

354. In addition, the *Signatory* shall be liable to the members of the *Electronic Community* and other *User entities* or, as the case may be, third parties for *Certificate* misuse, or for any misrepresentations therein contained, or acts or omissions resulting in damages and losses for FNMT-RCM or third parties.

9.6.4. Relying party representations and warranties

355. See the relevant section in the *GCPS*.

9.6.5. Representations and warranties of other participants

356. No stipulation.

9.7. DISCLAIMER OF WARRANTIES

357. No stipulation.

9.8. LIMITATIONS OF LIABILITY

358. In addition to the liabilities set out in the *GCPS*, the *Trust Service provider*:

- Shall not be liable for the use of the *Certificates* issued under this policy where the *Certificate Subscriber's* representatives or *Public Servants* do things for which they have no authority or acting ultra vires.
- In the case of *Electronic Seal Certificates*, FNMT-RCM shall not be responsible for checking membership of the organisational unit to be specified in the *Certificate* of the *Certificate Subscriber* administration body or the *Applicant's* membership of the organisational unit as its chief officer, for it is the *Registration Office* that will have that duty and responsibility to check. FNMT-RCM shall consider that the relevant *Registration Operations Officer* is the representative of the body, agency or entity of the administration *Certificate Subscriber*, unless otherwise advised.
- The Public Administration *Certificate Subscriber's* and its relations with FNMT-RCM shall be conducted at all times through the *Registration Office* and the officer responsible therefor.

359. See the relevant section in the *GCPS*.

9.9. INDEMNITIES

360. See the relevant section in the *GCPS*.

9.9.1. CA indemnity

361. See the relevant section in the *GCPS*.

9.9.2. Subscribers indemnity

362. See the relevant section in the *GCPS*.

9.9.3. Relying parties indemnity

363. See the relevant section in the *GCPS*.

9.10. TERM AND TERMINATION

9.10.1. Term

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

9.10.2. Termination

365. 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

366. 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

367. See the relevant section in the *GCPS*.

9.12. AMENDMENTS

9.12.1. Procedure for amendment

368. See the relevant section in the *GCPS*.

9.12.2. Notification mechanism and period

369. See the relevant section in the *GCPS*.

9.12.3. Circumstances under which OID must be changed

370. See the relevant section in the *GCPS*.

9.13. DISPUTE RESOLUTION PROVISIONS

371. See the relevant section in the *GCPS*.

9.14. GOVERNING LAW

372. See the relevant section in the *GCPS*.

9.15. COMPLIANCE WITH APPLICABLE LAW

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

9.16. MISCELLANEOUS PROVISIONS

374. See the relevant section in the *GCPS*.

9.16.1. Entire agreement

375. See the relevant section in the *GCPS*.

9.16.2. Assignment

376. See the relevant section in the *GCPS*.

9.16.3. Severability

377. See the relevant section in the *GCPS*.

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

378. See the relevant section in the *GCPS*.

9.16.5. Force Majeure

379. See the relevant section in the *GCPS*.

9.17. OTHER PROVISIONS

380. See the relevant section in the *GCPS*.