Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERTIFICATION POLICIES AND PRACTICES FOR PUBLIC SECTOR ELECTRONIC SEAL CERTIFICATES

	NAME	DATE
Prepared by:	FNMT-RCM	19/01/2026
Revised by:	FNMT-RCM	19/01/2026
Approved by:	FNMT-RCM	19/01/2026

Version	Date	Description
1.0	19/01/2026	Document Creation

Reference: DPC/DPSELSP_0100/SGPSC/2026

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 *Electronic Seal Certificates within the Administrative sphere.*

13. The name of this document is *"Certification Policies and Practices for Public Sector 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. The following *Certification Policies* are included in this document identified as follows:

Name: *Electronic Seal Certificate* Certification Policy

Reference / OID[1]:: 1.3.6.1.4.1.5734.3.17.1

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

Name: *G2 Electronic Seal Certificate* Certification Policy

Reference / OID: 1.3.6.1.4.1.5734.3.22.2.0

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

Version: 1.0

Approval date: 19/01/2026

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/

17. "*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.

18. 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

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

1. Certification Authority
2. Registration Authority
3. *Certificate Subscribers*

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

4. Relying Parties
5. Other participants

1.3.1. Certification Authority

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

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

Table 1 – Root FNMT CA Certificate

Root FNMT CA Certificate	
Subject	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Issuer	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	5D 93 8D 30 67 36 C8 06 1D 1A C7 54 84 69 07
Validity	Not before: 29 October 2008. Not after: 1 January 2030
Public key length	RSA 4096 bits
Signature algorithm	RSA – SHA256
Key identifier	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

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

Table 2 – AC SECTOR PUBLICO Subordinate CA Certificate

Subordinate CA Certificate	
Subject	CN=AC Sector Público,ORG_ID=VATES-Q2826004J,OU=Ceres,O=FNMT-RCM,C=ES

Subordinate CA Certificate	
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 bits
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

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

Table 3 – Root FNMT CA Certificate

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

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

Table 4 – AC ENTIDADES G2 Subordinate CA Certificate

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

1.3.2. Registration Authority

21. 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.

22. The validation and approval of requests for issuance for Entity Seals shall only be carried out from the *Registration Authority* of the FNMT-RCM itself.

1.3.3. Certificate Subscribers

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

1.3.4. Relying Parties

24. 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*.

1.3.5. Other participants

25. No stipulation.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

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

27. *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*.

28. 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*. 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

29. 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.

30. FNMT-RCM shall have no control over actions taken with and use of *Authentication, Code Signing and Electronic Signature Certificates* and their *Private keys* 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.

31. 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.

32. 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*.

33. 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.

34. In any case, if a third party wishes to rely on the *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*.

35. 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

36. 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

37. 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: +34 91 740 69 82

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

1.5.3. Person determining CPS suitability for the policy

39. 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

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

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

41. 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.

- *Electronic Seal Certificate*: An electronic statement that links the seal's validation data to a legal entity and confirms the name of that entity. It is used for automating signature and authentication processes between IT components
- *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.
- *Supervisory body:* a body designated by a Member State responsible for supervisory tasks in the provision of trust services, in accordance with 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.
- *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*.
- *Signer:* the individual who creates an electronic signature on behalf of his or her own or on behalf of the Legal entity or of the Institution with no legal entity that they represent
- *Subscriber*: The Public Administration, public body, agency or public-law entity.

1.6.2. References

42. 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

43. 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

44. 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

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

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

2.4. ACCESS CONTROLS ON REPOSITORIES

47. 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

48. *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

49. 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.

50. In processing proof of identity prior to issuing *Electronic Seal 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

51. 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).

52. 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

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

3.1.4. Rules for interpreting various name forms

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

3.1.5. Uniqueness of names

55. 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

56. 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

57. 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

58. 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*.

59. The identity checks of *Public Servants, Applicants* for *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.

60. 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.

61. 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

62. 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 Seal 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.

63. 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.

64. 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.

65. The RA of the FNMT-RCM verifies that the *Subscriber Representative* matches with the individual requesting a *Certificate*, by means of the electronic signature of the application form using a verified *Certificate* of electronic signature, thus guaranteeing the authenticity of their identity.

3.2.4. Non-verified Subscriber information

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

3.2.5. Validation of authority

67. 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

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

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

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

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

3.3.1. Identification and authentication for routine re-key

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

3.3.2. Identification and authentication for re-key after revocation

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

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

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

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

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who can submit a Certificate application

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

4.1.2. Registration process and responsibilities

76. *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. The *Registration Operations Officer*, the *Subscriber's* representative, shall be in charge of signing and sending the *Certificate* issuance agreement to FNMT-RCM.

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

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

79. Section 9.6 “Respresentation and warranties” hereof defines the parties’ responsibilities in this process

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing identification and authentication functions

80. Applicants will supply the requested information and evidence of their personal identity. 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*.

4.2.2. Approval or rejection of certificate applications

81. The *Registration Authority* that acts in the process of issuing Certificates shall always be that of the FNMT-RCM itself, and, therefore, the validation of domains will never be delegated to any other *RA*.

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

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

84. 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.

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

4.2.3. Time to process applications

86. 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

87. 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.

88. 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.

89. 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*.

90. 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.

91. 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 name of the automatic process application or system for which the *Certificate* is issued.

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

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

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

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

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

4.3.2. Notification of issuance

93. Upon the *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

94. 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.

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

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

4.4.2. Publication of the certificate by the CA

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

4.4.3. Notification of issuance to other entities

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

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Private key and certificate usage

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

100. 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

101. 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

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

4.6.1. Circumstances for certificate renewal

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

4.6.2. Who may request renewal

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

4.6.3. Processing certificate renewal requests

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

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

107. 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

108. 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

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

4.7. CERTIFICATE RE-KEY

110. 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

111. *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

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

4.7.3. Processing certificate re-keying requests

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

4.7.4. Notification of certificate re-key

114. 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

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

4.7.6. Publication of the re-keyed certificate

116. 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

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

4.8. CERTIFICATE MODIFICATION

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

4.8.1. Circumstance for certificate modification

119. The modification is not stipulated.

4.8.2. Who may request certificate modification

120. The modification is not stipulated.

4.8.3. Processing certificate modification requests

121. The modification is not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

122. The modification is not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

123. The modification is not stipulated.

4.8.6. Publication of the modified certificate by the CA

124. The modification is not stipulated.

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

125. The modification is not stipulated.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

126. *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.

127. 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*.

128. 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

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

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

131. Under no circumstances does the FNMT-RCM assume any obligation to verify the circumstances mentioned in letters c) to i) of this section; the FNMT-RCM must be notified by certified communication by delivery of the documents and information required to verify this.

132. 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 i) above, after the revocation *Requestor* is identified.

133. 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.

134. 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

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

4.9.2. Who can request revocation

136. 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.

137. 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

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

139. 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.

140. 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.

141. 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 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.

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

143. As soon as revocation is effective, the *Subscriber’s* representative who requested revocation will be notified using the email address provided.

144. 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.

145. In order to report suspected Private Key Compromise, *Certificate* misuse, or other types of fraud, inappropriate conduct or any other matter related to Certificates, a certificate problem request (CPR) can be sent to the email address incidentes.ceres@fnmt.es as indicated in section 1.5.2.

4.9.4. Revocation request grace period

146. 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

147. 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

148. 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

149. *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

150. *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

151. 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

152. The revocation status of *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

153. Not defined.

4.9.12. Special requirements related to key compromise

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

4.9.13. Circumstances for suspension

155. *Certificate* suspension is not supported.

4.9.14. Who can request suspension

156. *Certificate* suspension is not supported.

4.9.15. Procedure for suspension request

157. *Certificate* suspension is not supported.

4.9.16. Limits on suspension period

158. *Certificate* suspension is not supported.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational characteristics

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

4.10.2. Service availability

160. 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

161. Not stipulated.

4.11. End of subscription

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

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

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

4.12.2. Session key encapsulation and recovery policy and practices

164. No stipulation.

5. Physical security, procedural and personnel controls

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

5.1. Physical security controls

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

5.1.1. Site location and construction

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

5.1.2. Physical access

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

5.1.3. Power and air conditioning

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

5.1.4. Water exposures

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

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

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

5.1.7. Waste disposal

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

5.1.8. Off-site backup

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

5.2. Procedural Controls

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

5.2.1. Trusted roles

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

5.2.2. Number of persons required per task

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

5.2.3. Identification and authentication for each role

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

5.2.4. Roles requiring separation of duties

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

5.3. Personnel Controls

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

5.3.1. Qualifications, experience, and clearance requirements

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

5.3.2. Background check procedures

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

5.3.3. Training requirements

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

5.3.4. Retraining frequency and requirements

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

5.3.5. Job rotation frequency and sequence

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

5.3.6. Sanctions for unauthorized actions

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

5.3.7. Independent contractor requirements

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

5.3.8. Documentation supplied to personnel

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

5.4. AUDIT-LOGGING PROCEDURES

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

5.4.1. Types of events recorded

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

5.4.2. Frequency of processing log

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

5.4.3. Retention period for audit log

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

5.4.4. Protection of audit log

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

5.4.5. Audit log backup procedures

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

5.4.6. Audit collection system (internal vs. external)

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

5.4.7. Notification to event-causing subject

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

5.4.8. Vulnerability assessments

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

5.5. RECORDS ARCHIVAL

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

5.5.1. Types of records archived

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

5.5.2. Retention period for archive

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

5.5.3. Protection of archive

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

5.5.4. Archive backup procedures

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

5.5.5. Requirements for time-stamping of records

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

5.5.6. Audit collection system (internal vs. external)

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

5.5.7. Procedures to obtain and verify archive information

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

5.6. CA KEY CHANGEOVER

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

5.7. COMPROMISE AND DISASTER RECOVERY

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

5.7.1. Incident and compromise handling procedures

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

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

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

5.7.3. Entity private key compromise procedures

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

5.7.4. Business continuity capabilities after a disaster

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

5.8. TRUST SERVICE PROVIDER TERMINATION

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

6. TECHNICAL SECURITY CONTROLS

213. 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

214. 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

215. No stipulation.

6.1.1.3 Subscriber key pair generation

216. 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 the *Registration Operations Officer* or the person authorised thereby.

6.1.2. Private key delivery to the subscriber

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

218. 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

219. 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

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

6.1.5. Key sizes and algorithms used

221. The algorithms used in this CPS are:

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

222. Regarding Keys sizes:

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

6.1.6. Public key parameters generation and quality checking

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

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

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

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

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

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

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

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic module standards and controls

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

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

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

6.2.3. Private key escrow

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

6.2.4. Private key backup

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

6.2.5. Private key archival

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

6.2.6. Private key transfer into or from a cryptographic module

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

6.2.7. Private key storage on cryptographic module

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

6.2.8. Activating private keys

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

237. The Certification Authority's *Private keys* are activated and used based on management and operation role segmentation implemented by FNMT-RCM, including multi-person access based on cryptographic cards and related simultaneous use pattern.

6.2.9. Deactivating private keys

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

6.2.10. Destroying private keys

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

6.2.11. Cryptographic module capabilities

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

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

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

6.3.2. Certificate operational periods and key pair usage periods

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

- RSA hierarchy
    - *Root FNMT CA Certificate and Key pair:* until 1 January 2030.
    - *Certificate of the Subordinate CA issuing Electronic Signature and Electronic Seal Certificates and Key pair:* until 28 November 2029.
    - *Electronic Seal Certificates and Key pair:* until 31 December 2028.
- Elliptic curve hierarchy
    - Root FNMT CA *Certificate* and Key pair: until 4 October 2049.
    - El *Certificate* of the Subordinate CA issuing *Electronic Seal Certificates* and Key pair: until 07 October 2039.
    - *Electronic Seal Certificates and Key pair:* not in excess of 3 years.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

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

6.4.2. Activation data protection

244. The *Certification Authority's Private key* activation data is protected, as described in section "6.2.8 Activating private keys" above, with multi-person access based on cryptographic cards and related simultaneous use pattern.

6.4.3. Other aspects of activation data

245. No stipulations.

6.5. COMPUTER SECURITY CONTROLS

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

6.5.1. Specific computer security technical requirements

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

6.5.2. Computer security rating

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

6.6. LIFE CYCLE TECHNICAL CONTROLS

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

6.6.1. System development controls

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

6.6.2. Security management controls

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

6.6.3. Life cycle security controls

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

6.7. NETWORK SECURITY CONTROLS

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

6.8. TIME-STAMPING

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

6.9. OTHER ADDITIONAL CONTROLS

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

6.9.1. Control of the ability to provide services.

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

6.9.2. Control of systems development and computer applications

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

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

258. *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

259. *Electronic Seal Certificates* conform to standard X.509 version 3.

7.1.2. Certificate extensions

260. The document describing the profile of *Electronic Authentication Certificates, 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

261. The corresponding object identifiers (OID) for the cryptographic algorithm used are:

- RSA hierarchy:

  - SHA-256 with RSA Encryption with its corresponding OID: 1.2.840.113549.1.1.11.

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

7.1.4. Name forms

262. *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.

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

7.1.5. Name constraints

264. 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

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

7.1.7. Usage of policy constraints extension

266. The "Policy Constraints" extension is not used in any root CA *Certificate* (neither in AC RAIZ FNMT-RCM nor in AC RAIZ FNMT-RCM G2).

7.1.8. Policy qualifiers syntax and semantics

267. 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

268. 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

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

7.2.2. CRL and CRL entry extensions

270. The CRLs profiles have the following structures:

Table 5 – CRL profiles

Fields and extensions	Value
Version	V2
Signature algorithm	Sha256WithRSAEncryption o SHA-256 with ECDSA
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

7.3. OCSP PROFILE

7.3.1. Version number

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

7.3.2. OCSP extensions

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

273. *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”.

274. 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”.

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

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

276. Risk analysis is also carried out, in accordance with the dictates of the Information Security Management SystemProviders issuing certificates".

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

277. The corresponding audit plans will be prepared periodically.

278. The *Certification Authority* issuing the *Electronic Signature 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" The audit is carried out on a yearly basis by an external accredited firm.

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

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

8.2. QUALIFICATIONS OF ASSESSOR

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4. TOPICS COVERED BY ASSESSMENT

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

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6. COMMUNICATION OF RESULTS

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

8.7. AUTOEVALUATION

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

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

9.1.1. Certificate issuance or renewal fees

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

9.1.2. Certificate access fees

289. No stipulation.

9.1.3. Revocation or status information access fees

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

9.1.4. Fees for other services

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

9.1.5. Refund policy

292. 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

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

9.2.1. Insurance coverage

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

9.2.2. Other assets

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

9.2.3. Insurance or warranty coverage for end-entities

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

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1. Scope of confidential information

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

9.3.2. Information not within the scope of confidential information

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

9.3.3. Responsibility to protect confidential information

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

9.4. PRIVACY OF PERSONAL INFORMATION

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

9.4.1. Privacy plan

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

9.4.2. Information treated as private

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

9.4.3. Information not deemed private

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

9.4.4. Responsibility to protect private information

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

9.4.5. Notice and consent to use private information

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

9.4.6. Disclosure pursuant to judicial or administrative process

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

9.4.7. Other information disclosure circumstances

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

9.5. Intellectual property rights

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

9.6. Representations and warranties

9.6.1. CA representations and warranties

310. 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*.

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

312. 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.

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

9.6.2. RA representations and warranties

314. The activities related to the RA will be carried out exclusively by the FNMT-RCM, through its Registry Area.

315. In addition to the obligations and responsibilities of the parties listed in this document and in the General Declaration of Trust Services and Electronic Certification Practices, the RA, through the Registry Area of the FNMT-RCM, has the following obligations::

- In general terms, to follow all procedures established by the FNMT-RCM in the Certification Policy and Practices Statement in terms of the performance of its functions of management, issuance and revocation of Certificates, and to not take any steps to alter this operating framework.

- In particular, to verify the identity, and any personal data that may be relevant for the specified purpose, of Applicants for Certificates, Subscribers and their Representatives, using any of the methods permitted under the Law, and in accordance, in general terms, with the provisions contained in the DGPC, and, in particular, in this DPPP. The identification will be carried out through qualified electronic signature certificates accepted in the FNMT-RCM processes.

- Preserve all information and documentation relating to Certificates, maintaining all application, renewal or revocation data for fifteen (15) years.

- Handle the receipt and management of applications and the issuance contracts (pdf form) sent to Certificate Subscribers.
- Diligently check the causes for revocation that could affect the validity of Certificates

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

9.6.3. Subscriber and signatory representations and warranties

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

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

- Review the information contained in the *Certificate* and notify the FNMT-RCM of any error or inaccuracy.
- Verify the *Electronic signature* or *Advanced electronic seal* provided by the *Trust Service Provider* issuing any *Certificates* prior to trusting them.
- Diligently report any modification of the data provided in the application for the *Certificate* to the FNMT-RCM, requesting, when pertinent, the revocation of the same.
- To return or destroy the *Certificate* where it is so demanded by FNMT-RCM, and not to use it with the purpose of signing or identifying oneself electronically when the Certificate runs out or is revoked.

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

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

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

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

9.6.4. Relying party representations and warranties

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

9.6.5. Representations and warranties of other participants

324. No stipulation.

9.7. DISCLAIMER OF WARRANTIES

325. No stipulation.

9.8. LIMITATIONS OF LIABILITY

326. 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.

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

9.9. INDEMNITIES

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

9.9.1. CA indemnity

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

9.9.2. Subscribers indemnity

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

9.9.3. Relying parties indemnity

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

9.10. TERM AND TERMINATION

9.10.1. Term

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

9.10.2. Termination

333. 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

334. 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

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

9.12. AMENDMENTS

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

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

9.12.3. Circumstances under which OID must be changed

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

9.13. DISPUTE RESOLUTION PROVISIONS

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

9.14. GOVERNING LAW

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

9.15. Compliance with applicable law

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

9.16. Miscellaneous provisions

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

9.16.1. Entire agreement

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

9.16.2. Assignment

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

9.16.3. Severability

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

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

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

9.16.5. Force Majeure

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

9.17. Other provisions

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