Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SPECIFIC CERTIFICATION POLICIES AND PRACTICES APPLICABLE TO ELECTRONIC CERTIFICATION AND SIGNATURE SERVICES FOR PUBLIC ORGANIZATIONS AND ADMINISTRATIONS, THEIR PUBLIC BODIES AND PUBLIC LAW ENTITIES

	NAME	DATE
Prepared by:	FNMT-RCM	21/04/2021
Revised by:	FNMT-RCM	26/04/2021
Approved by:	FNMT-RCM	28/04/2021

BACKGROUND TO THE DOCUMENT		
Version	Date	Description
1.0	06/11/2008	Creation of the document
1.1	05/05/2009	Expansion of certificate validity to four years.
1.2	01/08/2010	Deletion of the organization aspects section as it is included in the DGPC Obligation to show entity to which signatory provides services (Certificate Subscriber) in the certificate for Public Administration Personnel in the extension subjectAltName Modification of certificate profiles. Inclusion of new profiles in accordance with new certification policies.
1.3	03/07/2011	Deletion of sections related to information on management of policies pertaining to this document as they are already included in the DGPC. Modification in certificate profiles to change AIA field value in certificates for end entities.

BACKGROUND TO THE DOCUMENT		
Version	**Date**	**Description**
1.4	19/12/2011	Addition of definitions of people related to certificate management. Addition of definitions on delegate Registry Offices and requesting Registry Offices for implementation of user registration activities by delegation. Modification in certificate profile table: the serial number of AP certificates is assigned randomly.
1.5	31/10/2012	Removal of AC references known as "APE AC". This type of certificate-related information can be found in earlier versions of this document. Deleted 2,4,7 and 9 profile certificate tables. Correction of errors in certificates profiles: the CRL's distribution point of end-entity certificates is http://www.cert.fnmt.es/crlsacap/CRLxxx.crl End-entity certificates will have a validity period of 3 years. Modification of certificates auto-revocation policies. When an equal Subscriber requests the issuance of a new certificate, the certificates of site and seal are not revoked. Remarks about considering the Cryptography Card a secure device for signature creation. Rectification of mistakes on reference to paragraphs ETSI 101 456 about the exclusions to this rule. Removed the sections of "Forms models" as these are available through each document generation application.
1.6	29/5/2013	Replacement of the term holder by signatory or subscriber. Removal of last paragraph of the description type of civil servant certificate, which interpreted the application of the law on electronic signature in the certificate for Public Administration Personnel. Clarification of the private use of public employee certificate.
1.7	03/07/2013	Clarification of paragraph 51 about private use of the Certificate permitted to public employees

BACKGROUND TO THE DOCUMENT		
Version	**Date**	**Description**
1.8	02/04/2014	Alignment with the LTE general liability regime PSC regarding the Registration Offices and for the consent of "signatory" in case of termination of activities of the PSC. Some links to the Risk Application have been updated.
2.0	16/06/2014	Alignment with the LTE general liability regime PSC regarding the Registration Offices and for the consent of "signatory" in case of termination of activities of the PSC. Some links to the Risk Application have been updated. Revision according to WebTrust.
2.1	17/11/2014	Issuance of certificate with SHA-256. Reduction of the maximum period of certificates suspension to 30 days. Elimination of QcLimitValue field profiles certificates. Revocation of certificates for Public Administration Personnel via phone 24x7
2.2	10/07/2015	Revision according to ETSI 101 456
2.3	27/01/2016	Revocation 24x7 of certificates for identification of electronic venues of the Public Administration and certificates for automated administrative actions.
2.4	24/06/2016	Modification of certificate profiles in accordance with CAB/Forum requirements.
2.5	03/01/2017	Alignment with the eIDAS Regulation of the Certificate for Public Administration Personnel.
3.0	03/01/2017	Alignment with the eIDAS Regulation of the venue and seal Certificates.
3.1	09/10/2017	Inclusion of the Certificate with pseudonym for Public Administration Personnel PPAA and requirements of CAB/Forum.
3.2	21/09/2018	Inclusion of requirements of CAB/Forum. Public Administration Personnel and Seal Certificates will have a validity period of 2 years.
3.3	05/03/2019	Removal of certificate suspension practices.

BACKGROUND TO THE DOCUMENT		
Version	**Date**	**Description**
3.4	30/05/2019	Update domain validation methods according to CA / Browser Forum Baseline Requeriments.
3.5	07/10/2019	Electronic Venue Certificate is removed because new specific DPC is created
3.6	14/04/2020	Modifications in accordance with RFC3647 and reduction of the validity period of the final entity certificates.
3.7		Annual review. Section 4.9.12: reference to DGPC

Reference: DPC/PCPAA0307/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. 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.

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

1) ***Electronic Signature Certificate*** *for* ***Public Administration Personnel.***

2) ***Electronic Seal Certificate*** for Public Administrations, public bodies or public-law entities as a system of identification and for A*utomated administrative activities* and *Automated legal activities*, allowing documents issued by the Administration or any digital asset to be authenticated.

6. In addition, 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

7. This document is an integral part of the FNMT-RCM's *General Trust Service and Electronic Certification Practices Statement* (TSPS) and its purpose is to provide public information on the conditions and characteristics of trust services and, particular, services for the issuance of electronic *Certificates* by the FNMT-RCM as a *Trust Service Provider*, covering, in particular the duties and procedures it undertakes to fulfil with relation to the issue of *Electronic Signature Certificates* for *Public Administration Personnel*, as well as *Electronic Seal Certificates* issued to Public Administrations, public bodies and public-law entities. It also includes 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.

8. Of particular note in order to interpret these Specific Certification Policies and Practices, is the section "Definitions" in the *General Trust Service and Electronic Certification Practices Statement* and, as the case may be, the Issuance Law corresponding to each body and/or agency or *User entity* of the FNMT-RCM certification services.

9. 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

10. 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.

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

    1) 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.

    2) 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.

12. This document therefore sets out the *Specific Certification Policies and Certification Practices* for the following *Certificates:*

    1) *Electronic Signature Certificate for Public Administration Personnel*:

       i. *Certificate* in cryptographic card

       ii. *Certificate* in software

       iii. *Certificate* with a pseudonym for use in the Justice Administration

       iv. *Certificate* with a pseudonym for use in the Public Administration

    2) *Electronic Seal Certificate* for Public Administrations, public bodies or public-law entities

13. The name of this document is *"Specific Certification Policies and Practices applicable to electronic certification and signature services for public organizations and administrations,*

their public bodies and public law entities", 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. Therefore, in the event of any contradiction between this document and that stipulated in the *General Trust Service and Electronic Certification Practices Statement*, that formulated herein shall prevail.

16. The *Issuance Law* of each *Certificate* or group of *Certificates* shall represent, as appropriate and given its singularity, a special standard with regard to that established in these *Specific Certification Policies and Practices* for the various public bodies or entities using the services of the FNMT-RCM, when thus required by the nature of their competences or functions. The *Issuance Law*, if set up, shall be included in the binding document to be formalized between the FNMT-RCM and the Administrations, public bodies and entities, and/or in the conditions of use or issue contract, and/or in the *Certificate* itself.

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

Name: *Electronic Signature Certificate for Public Administration Personnel* Certification Policy

Reference / OID[1]:

- 1.3.6.1.4.1.5734.3.3.4.4.1: *Certificate* in cryptographic card.
- 1.3.6.1.4.1.5734.3.3.4.4.2: *Certificate* in software.
- 1.3.6.1.4.1.5734.3.3.5.2: *Certificate* with a pseudonym for use in the Justice Administration.
- 1.3.6.1.4.1.5734.3.3.11.1: *Certificate* with a pseudonym for use in the Public Administration.

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

[1] *Note*: The OID or policy identifier is a reference to be included in the *Certificate* in order for users to be able to determine the applicable practices and procedures to issue the *Certificate* in question.

Although this document describes a single policy for this type of *Certificates*, there may be three different references to the same to distinguish and identify specific elements in the *Certificate* format, the *Certificate* profiles, the *Certification Authority* used for issuing it or the relevant issue procedures.

Therefore, the *Certificate Certification Policy and Practices* for Public Administration Personnel shall be described singly, identifying any possible special features and associating them to the corresponding OID or references.

Name: *Electronic Seal Certificate* for Public Administrations, public bodies or public-law entities Certification Policy

Reference / OID: 1.3.6.1.4.1.5734.3.3.9.1

Type of associated policy: QCP-l OID: 0.4.0.194112.1.1

Version: 3.7

Approval date: 28/04/2021

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. The *Electronic Signature Certificate for Public Administration Personnel* 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. The *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.

20. 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

21. 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

22. 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 = Public Sector CA, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES
Issuer	OU = FNMT-RCM ROOT CA, O = FNMT-RCM, C = ES
Serial number (hex)	02

Subordinate CA Certificate	
Validity	Not before: 21 May 2010 Not after: 21 May 2022
Public key length	RSA 2048 bytes
Signature algorithm	RSA – SHA256
Key identifier	83:0F:F2:05:AE:69:48:50:59:C3:FB:23:76:A7:F2:F9:EE:1C:2A:61 :DE:25:9D:D0:9D:0B:B6:AD:69:F8:88:32

1.3.2. Registration Authority

23. 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.

24. *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

25. *Signatories* are natural persons, *Public Administration Personnel*, who maintain the *Signature creation data* associated with that *Certificate* for their own use only.

1.3.4. Certificate Subscribers

26. *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

27. 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

28. No stipulation.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

29. 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”.

30. The *Electronic Signature Certificates* issued under this *Certification Policy* are issued to civil servants, employees and authorised personnel working for Public Administrations, bodies, public bodies and public-law entities. 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.

31. *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.

32. The scope of application of *Certificates* issued under the *Justice Administration Pseudonym Certificate* Policies exclusively comprises the Justice Administration.

33. *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*.

34. 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*.

35. 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

36. 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*.

37. 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.

38. FNMT-RCM shall have no control over actions taken with and use of *Electronic Signature Certificates* and the *Private key* by *Public Administration Personnel* 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.

39. 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.

40. 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.

41. 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*.

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

43. 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

44. 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

45. 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

46. 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

47. 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

48. 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 at least on a yearly basis.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

49. 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 Signature Certificate:* For the purposes of this SPPS, this is a qualified *Certificate* issued to *Public Administration Personnel* 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*:
  - *Certificate* in *Cryptographic card*
  - *Certificate* in software
  - *Certificate with a pseudonym for use in the Justice Administration*
  - *Certificate with a pseudonym for use in the Public Administration*
- *Certificate with a pseudonym for use in the Public Administration:* This is an *Electronic Signature Certificate* containing a natural person's *validation data* and confirming the pseudonym given by the administration in accordance with Public Sector Legal Regime Act 40/2015, 1 October, and Justice Administration Information and Communication Technologies.
- *Certificate with a pseudonym for use in the Justice Administration:* 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.
- *Certification Practice Statement (CPS):* a readily accessible statement made available to the public electronically and free of charge by FNMT-RCM. It is deemed to be a security document detailing, within the framework of the eIDAS Regulation, the obligations *Trust Service Providers* agree to fulfil in regard to management of *Signature creation and verification data* and *Electronic certificates*, the terms applicable to the application for, issuance, use and termination of the *Certificates*, organisational and technical security measures, profiles and information mechanisms as to the validity of *Certificates.*
- *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.*

- *Public Administration Personnel*: 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.
- *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

50. 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

51. 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

52. 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

53. 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.

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

2.4. ACCESS CONTROLS ON REPOSITORIES

55. 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

56. *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

57. 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.

58. 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

59. 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).

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

61. 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

62. *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.

63. In the identity proofing procedure prior to issuing an *Electronic Signature Certificate* for *Public Administration Personnel* with a pseudonym, the *Registry Office* will verify the *Signatory*'s true identity and will keep the supporting documentation.

64. Pseudonyms may not be used to identify the *Subscriber.*

3.1.4. Rules for interpreting various name forms

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

3.1.5. Uniqueness of names

66. 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

67. 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

68. 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*.

69. FNMT-RCM neither generates nor stores the *Private Keys* 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

70. 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*.

71. The identity checks of *Public Administration Personnel, 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.

72. 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.

3.2.3. Authentication of individual applicant identity

73. 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.

74. 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

75. *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.

76. 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

77. 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, incumbency 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 Administration Personnel*) were identified by physical presence (as described in the preceding paragraph), and the period of time elapsed since that physical presence does not exceed the legally established.

3.2.4. Non-verified Subscriber information

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

3.2.5. Validation of authority

79. 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.

80. 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*, for whose issuance the representation capacity has been accredited.

3.2.6. Criteria for interoperation

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

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

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

83. 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

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

3.3.2. Identification and authentication for re-key after revocation

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

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

86. 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.

87. 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

88. Only *Public Administration Personnel*, previously authorised by the *Subscriber*, may apply for this type of *Certificates*.

4.1.2. Registration process and responsibilities

89. *Applicants, Public Administration Personnel,* 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.

90. 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.

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

92. 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

93. For *Electronic Signature Certificates*, *Applicants* will supply the requested information and evidence of their personal identity and *Public Administration Personnel* status.

94. 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*.

95. 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:

   1) Check that the *Certificate Subscriber* exists and that its details are correct.

   2) 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*.

96. 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

97. 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.

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

99. 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.

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

4.2.3. Time to process applications

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

102. For *Electronic Seal Certificate* the minimum required time will be used, 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

103. 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.

104. 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.

105. 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*.

106. 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.

107. 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 Administration Personnel,* 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.

108. 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

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

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1. Conduct constituting certificate acceptance

110. 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

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

4.4.3. Notification of issuance to other entities

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

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Private key and certificate usage

113. 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 Administration Personnel* and, for *Electronic Seal Certificates*, with *Responsible for the Registry Operations* or the person authorised by the latter.

4.5.2. Relying party public key and certificate usage

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

4.6. CERTIFICATE RENEWAL

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

4.6.1. Circumstances for certificate renewal

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

4.6.2. Who may request renewal

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

4.6.3. Processing certificate renewal requests

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

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

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

4.6.6. Publication of the renewal certificate by the CA

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

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

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

4.7. CERTIFICATE RE-KEY

123. Under these Certification Policies, *Certificate* re-key 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

124. *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

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

4.7.3. Processing certificate re-keying requests

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

4.7.4. Notification of certificate re-key

127. 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

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

4.7.6. Publication of the re-keyed certificate

129. 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

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

4.8. CERTIFICATE MODIFICATION

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

4.8.1. Circumstance for certificate modification

132. The modification is not stipulated.

4.8.2. Who may request certificate modification

133. The modification is not stipulated.

4.8.3. Processing certificate modification requests

134. The modification is not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

135. The modification is not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

136. The modification is not stipulated.

4.8.6. Publication of the modified certificate by the CA

137. The modification is not stipulated.

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

138. The modification is not stipulated.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

139. *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.

140. 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*.

141. Revocation of the *Certificate*s implies, aside from their termination, end of the relationship and system of use of the *Certificate* with the FNMT-RCM.

142. 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.*

143. 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

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

145. 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:

- Loss of the Certificate format.
- 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) Breach or compromise of the *Trust Service Provider's Signature creation data*.

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

146. 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.

147. 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.

148. The FNMT-RCM may revoke the *Certificates* itself in the cases included to in b) to k) in this *Certification Practices Statement*.

149. 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.

150. 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

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

4.9.2. Who can request revocation

152. 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.

153. 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

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

155. 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.

156. 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.

157. 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:

1) 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*.

2) 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.

158. Likewise, the FNMT-RCM shall consider that the person requesting revocation of a *Certificate* of this type shall have the corresponding authorization if the request is conducted through its *Registry Office*. The FNMT-RCM shall not assess the appropriateness of the revocation requested whenever it is conducted through the abovementioned *Registry Office*.

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

1) The *Signatory* and the requestor in the case of an *Electronic Signature Certificate.*

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

160. 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

161. 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

162. 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

163. 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

164. *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

165. *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

166. 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

167. 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

168. Not defined.

4.9.12. Special requirements related to key compromise

169. See the relevant section in the GCPS.

4.9.13. Circumstances for suspension

170. *Certificate* suspension is not supported.

4.9.14. Who can request suspension

171. *Certificate* suspension is not supported.

4.9.15. Procedure for suspension request

172. *Certificate* suspension is not supported.

4.9.16. Limits on suspension period

173. *Certificate* suspension is not supported.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational characteristics

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

4.10.2. Service availability

175. 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

176. Not stipulated.

4.11. END OF SUBSCRIPTION

177. 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

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

4.12.2. Session key encapsulation and recovery policy and practices

179. No stipulation.

5. PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

180. See the relevant section in the GCPS.

5.1. PHYSICAL SECURITY CONTROLS

181. See the relevant section in the GCPS.

5.1.1. Site location and construction

182. See the relevant section in the GCPS.

5.1.2. Physical access

183. See the relevant section in the GCPS.

5.1.3. Power and air conditioning

184. See the relevant section in the GCPS.

5.1.4. Water exposures

185. See the relevant section in the GCPS.

5.1.5. Fire prevention and protection

186. See the relevant section in the GCPS.

5.1.6. Media storage

187. See the relevant section in the GCPS.

5.1.7. Waste disposal

188. See the relevant section in the GCPS.

5.1.8. Off-site backup

189. See the relevant section in the GCPS.

5.2. Procedural Controls

190. See the relevant section in the GCPS.

5.2.1. Trusted roles

191. See the relevant section in the GCPS.

5.2.2. Number of persons required per task

192. See the relevant section in the GCPS.

5.2.3. Identification and authentication for each role

193. See the relevant section in the GCPS.

5.2.4. Roles requiring separation of duties

194. See the relevant section in the GCPS.

5.3. Personnel Controls

195. See the relevant section in the GCPS.

5.3.1. Qualifications, experience, and clearance requirements

196. See the relevant section in the GCPS.

5.3.2. Background check procedures

197. See the relevant section in the GCPS.

5.3.3. Training requirements

198. See the relevant section in the GCPS.

5.3.4. Retraining frequency and requirements

199. See the relevant section in the GCPS.

5.3.5. Job rotation frequency and sequence

200. See the relevant section in the GCPS.

5.3.6. Sanctions for unauthorized actions

201. See the relevant section in the GCPS.

5.3.7. Independent contractor requirements

202. See the relevant section in the GCPS.

5.3.8. Documentation supplied to personnel

203. See the relevant section in the GCPS.

5.4. AUDIT-LOGGING PROCEDURES

204. See the relevant section in the GCPS.

5.4.1. Types of events recorded

205. See the relevant section in the GCPS.

5.4.2. Frequency of processing log

206. See the relevant section in the GCPS.

5.4.3. Retention period for audit log

207. See the relevant section in the GCPS.

5.4.4. Protection of audit log

208. See the relevant section in the GCPS.

5.4.5. Audit log backup procedures

209. See the relevant section in the GCPS.

5.4.6. Audit collection system (internal vs. external)

210. See the relevant section in the GCPS.

5.4.7. Notification to event-causing subject

211. See the relevant section in the GCPS.

5.4.8. Vulnerability assessments

212. See the relevant section in the GCPS.

5.5. RECORDS ARCHIVAL

213. See the relevant section in the GCPS.

5.5.1. Types of records archived

214. See the relevant section in the GCPS.

5.5.2. Retention period for archive

215. See the relevant section in the GCPS.

5.5.3. Protection of archive

216. See the relevant section in the GCPS.

5.5.4. Archive backup procedures

217. See the relevant section in the GCPS.

5.5.5. Requirements for time-stamping of records

218. See the relevant section in the GCPS.

5.5.6. Audit collection system (internal vs. external)

219. See the relevant section in the GCPS.

5.5.7. Procedures to obtain and verify archive information

220. See the relevant section in the GCPS.

5.6. CA KEY CHANGEOVER

221. See the relevant section in the GCPS.

5.7. COMPROMISE AND DISASTER RECOVERY

222. See the relevant section in the GCPS.

5.7.1. Incident and compromise handling procedures

223. See the relevant section in the GCPS.

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

224. See the relevant section in the GCPS.

5.7.3. Entity private key compromise procedures

225. See the relevant section in the GCPS.

5.7.4. Business continuity capabilities after a disaster

226. See the relevant section in the GCPS.

5.8. TRUST SERVICE PROVIDER TERMINATION

227. See the relevant section in the GCPS.

6. TECHNICAL SECURITY CONTROLS

228. 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

229. 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

230. No stipulation.

6.1.1.3 Subscriber key pair generation

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

1) *Public Administration Personnel* in the case of *Electronic Signature Certificates*.

2) The *Registration Operations Officer* or the person authorised thereby in the case of *Electronic Seal Certificates.*

6.1.2. Private key delivery to the subscriber

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

233. 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

234. 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

235. See the relevant section in the GCPS.

6.1.5. Key sizes and algorithms used

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

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

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

6.1.6. Public key parameters generation and quality checking

238. See the relevant section in the GCPS.

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

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

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

241. 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.

242. The key usage purposes for final entity *Certificates* issued under this *SPPS* are exclusively encryption, authentication and signature.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic module standards and controls

243. See the relevant section in the GCPS.

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

244. See the relevant section in the GCPS.

6.2.3. Private key escrow

245. 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

246. See the relevant section in the GCPS.

6.2.5. Private key archival

247. See the relevant section in the GCPS.

6.2.6. Private key transfer into or from a cryptographic module

248. See the relevant section in the GCPS.

6.2.7. Private key storage on cryptographic module

249. See the relevant section in the GCPS.

6.2.8. Activating private keys

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

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

6.2.9. Deactivating private keys

252. See the relevant section in the GCPS.

6.2.10. Destroying private keys

253. 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

254. See the relevant section in the GCPS.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

255. See the relevant section in the GCPS.

6.3.2. Certificate operational periods and key pair usage periods

256. 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 21 May 2022.
- *Electronic Signature Certificates* and Key pair: not in excess of 12 months.
- *Electronic Seal Certificates* and Key pair: not in excess of 12 months.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

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

6.4.2. Activation data protection

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

6.4.3. Other aspects of activation data

259. No stipulations.

6.5. COMPUTER SECURITY CONTROLS

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

6.5.1. Specific computer security technical requirements

261. See the relevant section in the GCPS.

6.5.2. Computer security rating

262. See the relevant section in the GCPS.

6.6. LIFE CYCLE TECHNICAL CONTROLS

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

6.6.1. System development controls

264. See the relevant section in the GCPS.

6.6.2. Security management controls

265. See the relevant section in the GCPS.

6.6.3. Life cycle security controls

266. See the relevant section in the GCPS.

6.7. NETWORK SECURITY CONTROLS

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

6.8. TIME-STAMPING

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

6.9. OTHER ADDITIONAL CONTROLS

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

6.9.1. Control of the ability to provide services.

270. See the relevant section in the GCPS.

6.9.2. Control of systems development and computer applications

271. See the relevant section in the GCPS.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

272. *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".

273. *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

274. All the *Certificates* issued under this *Certification Policy* are conform to standard X.509 version 3.

7.1.2. Certificate extensions

275. 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

276. 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

277. *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.

7.1.5. Name constraints

278. 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

279. 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

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

7.1.8. Policy qualifiers syntax and semantics

281. 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

282. 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

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

7.2.2. CRL and CRL entry extensions

284. The CRL profile has the following structure:

Table 3 – CRL profile

Fields and extensions	Value
Version	V2
Signature algorithm	Sha256WithRSAEncryption
CRL number	Incremental value
Issuer	Issuer DN
Issuance date	UTC issuance time.
Date of next upgrade	Issuance date + 24 hours
Authority key identifier	Issuer key hash
ExpiredCertsOnCRL	NotBefore of the CA
Distribution point	Distribution point URLs and CRL scope
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

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

7.3.2. OCSP extensions

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

287. 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".

288. 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".

289. 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 as ruled in the National Security Scheme (Royal Decree 3/2010, of January 8, 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).

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

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

291. The corresponding audit plans will be prepared periodically.

292. 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" The audit is carried out on a yearly basis by an external accredited firm.

293. 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

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4. TOPICS COVERED BY ASSESSMENT

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

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6. COMMUNICATION OF RESULTS

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

8.7. AUTOEVALUATION

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

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

9.1.1. Certificate issuance or renewal fees

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

9.1.2. Certificate access fees

302. No stipulation.

9.1.3. Revocation or status information access fees

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

9.1.4. Fees for other services

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

9.1.5. Refund policy

305. 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

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

9.2.1. Insurance coverage

307. See the relevant section in the GCPS.

9.2.2. Other assets

308. See the relevant section in the GCPS.

9.2.3. Insurance or warranty coverage for end-entities

309. See the relevant section in the GCPS.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1. Scope of confidential information

311. See the relevant section in the GCPS.

9.3.2. Information not within the scope of confidential information

312. See the relevant section in the GCPS.

9.3.3. Responsibility to protect confidential information

313. See the relevant section in the GCPS.

9.4. PRIVACY OF PERSONAL INFORMATION

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

9.4.1. Privacy plan

315. See the relevant section in the GCPS.

9.4.2. Information treated as private

316. See the relevant section in the GCPS.

9.4.3. Information not deemed private

317. See the relevant section in the GCPS.

9.4.4. Responsibility to protect private information

318. See the relevant section in the GCPS.

9.4.5. Notice and consent to use private information

319. See the relevant section in the GCPS.

9.4.6. Disclosure pursuant to judicial or administrative process

320. See the relevant section in the GCPS.

9.4.7. Other information disclosure circumstances

321. See the relevant section in the GCPS.

9.5. INTELLECTUAL PROPERTY RIGHTS

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

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA representations and warranties

323. 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*.

324. 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.

325. 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.

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

9.6.2. RA representations and warranties

327. 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:

- Verify unequivocally the data of the *Public Administration Personnel* as *Certificate* Users, to act as Signatories of the same, with relation to their identity and status of the position, job, employment or any other data that shows or describes their relationship with the Administration, body or entity which it works for.

- Verify unequivocally *Applicant* identification data, representative of *Certificate Subscriber*, and verify they belong to the organization unit as person in charge of the same.

- Not use the *Certificate* in case the *Signature creation data* of the Subject may be threatened and / or compromised.

- The *Trust Service Provider*, through the *Person responsible for the Registry Operations* shall oversee the fulfilment of the procedures approved by FNMT-RCM for the identification of *Certificate Applicants*, and specifically in the case of *Electronic Signature Certificates* for *Public Administration Personnel* with a pseudonym, verification of the *Signatory* true identity and preservation of the documentation attesting to that identity.

- Likewise, *Certificate* users will be informed how to use them properly, in accordance with the terms of use, the Certification Policies and Practices and the applicable laws.

- In the event the *Certificate* is in a card, download *Certificate* and its keys directly onto the encryption card provided to its personnel. In any case, no private keys associated to Certificates shall be kept in the *Registry Office* computers, in accordance with the FNMT-RCM guidelines described in the procedure manuals given to the *Registry Offices*, in these *Specific Certification Policies and Practices* and in the *TSPS*.

- Not conduct any registrations or process any applications from personnel working for an entity other than the one represented by the Registry Office, without detriment to the creation of centralized Registry Offices or agreements between administrations to conduct registrations.

- 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 conduct registrations or process *Certificates* issued under this policy and whose title, referred to the administration body, corresponds to a Public Administration entity it has no authority over or if it has no powers to act as a *Registry Office*.
- Not conduct registrations or process *Certificates* issued under this policy, for an organization unit not reporting to the *Certificate Subscriber* administration body.
- 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.

328. Regarding the activities of the Registration Office staff, FNMT-RCM shall be subject of obligations and responsibilities contained in Law 59/2003, December 19, about electronic signature, without prejudice of the specialties in the article 11 of RD 1317/2001, November 30, by which the article 81 Law 66/1997, December 30, about Financial measures, administrative and social order in security service provision of Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, in the communications throughout electronic, computer and telematic means with Public Administrations.

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

9.6.3. Subscriber and signatory representations and warranties

330. 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*.

331. The *Signatory* and/or *Subscriber* 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.

332. In any case, the *Signatory* and/or *Subscriber* shall not use the *Signature creation data* / *Seal*, associated with their *Certificate* where its validity period has expired, or the *Signature Creation data* / *Seal* of the *Trust Service Provider* may be under threat and/or compromised and thus has been advised by the Provider or, as the case may be, the *Signatory* / *Subscriber* suspects or has learned of any such circumstances. The *Signatory / Subscriber's* breach of this requirement shall make the *Signatory / Subscriber* liable for the consequences of acts, documents or transactions signed /sealed 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.

333. In addition, the *Signatory / Subscriber* 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.

334. The *Signatory / Subscriber* will be liable for the use of the *Signatory's Certificate* if the *Trust Service Provider* has discontinued its activity as *Certificate* Issuer and no substitution shall have occurred as provided for by Law.

9.6.4. Relying party representations and warranties

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

9.6.5. Representations and warranties of other participants

336. No stipulation.

9.7. DISCLAIMER OF WARRANTIES

337. No stipulation.

9.8. LIMITATIONS OF LIABILITY

338. 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 Administration Personnel* 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.
- The relationships between the FNMT-RCM and the *Subscriber* and the *Public Administration Personnel (*using the *Certificate* provided by the abovementioned *Subscriber)* shall be primarily determined, for the purposes of the use of the *Certificates*, through a document pertaining to the conditions of use or, if applicable, to the *Certificate* issue contract, and, secondly, by these *Specific Certification Policies and Practices* and by the *GCPS*, in compliance with the agreements or document on the relationship between the FNMT-RCM and the corresponding Public Administration.

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

9.9. INDEMNITIES

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

9.9.1. CA indemnity

341. See the relevant section in the GCPS.

9.9.2. Subscribers indemnity

342. See the relevant section in the GCPS.

9.9.3. Relying parties indemnity

343. See the relevant section in the GCPS.

9.10. TERM AND TERMINATION

9.10.1. Term

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

9.10.2. Termination

345. 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 at least a yearly basis.

9.10.3. Effect of termination and survival

346. 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

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

9.12. AMENDMENTS

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

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

9.12.3. Circumstances under which OID must be changed

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

9.13. DISPUTE RESOLUTION PROVISIONS

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

9.14. GOVERNING LAW

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

9.15. COMPLIANCE WITH APPLICABLE LAW

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

9.16. MISCELLANEOUS PROVISIONS

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

9.16.1. Entire agreement

355. See the relevant section in the GCPS.

9.16.2. Assignment

356. See the relevant section in the GCPS.

9.16.3. Severability

357. See the relevant section in the GCPS.

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

358. See the relevant section in the GCPS.

9.16.5. Force Majeure

359. See the relevant section in the GCPS.

9.17. OTHER PROVISIONS

360. None stipulated.