Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERTIFICATION POLICIES AND PRACTICES FOR NATURAL PERSON CERTIFICATES FROM "AC FNMT USUARIOS"

	NAME	DATE
Prepared by:	FNMT-RCM	30/01/2025
Revised by:	FNMT-RCM	31/01/2025
Approved by:	FNMT-RCM	03/02/2025

DOCUMENT HISTORY		
Version	**Date**	**Description**
1.0	25/03/2014	Document creation
1.1	24/06/2016	Modifications in accordance with ETSI 101 456 audit
1.2	03/01/2017	Modifications in accordance with ETSI EN 319 412 - 2
1.3	22/12/2017	Annual revision of the document.
1.4	05/03/2019	Removal of certificate suspension practices
1.5	06/04/2020	Modifications in accordance with RFC3647
1.6	28/04/2021	Annual revision. Section 4.9.12: reference to DGPC
1.7	24/03/2022	Removal references to the repealed Law 59/2003. Modifications in accordance with Spanish regulation of the remote video identification methods for issuing qualified electronic certificates. Sections: 3.2.3.3, 4.2.1 y 4.2.2.
1.8	31/05/2023	Refund Policy Update
1.9	03/02/2025	Annual revision. Procedure for revocation request modified.

Reference: DPC/CPUS0109/SGPSC/2025

Document classified as: *Public*

Table of contents

1. INTRODUCTION

1.1. OVERVIEW

1. This document is an integral part of the Trust Services Practices and Electronic Certification General Statement (*GCPS*) of the FNMT-RCM, and its aim is to inform the public about the conditions and characteristics of the certification services and services for the issuing of electronic Certificates by the FNMT-RCM as a Trust Services Provider, containing the obligations and procedures that with which it agrees to comply in regard to the issuing of the Natural Person Certificate issued by the "AC FNMT Usuarios"

2. Specifically, for the purposes of the interpretation of these *Specific Certification Policies and Practices*, the "Definitions" section of the *GCPS*.

3. The *Natural Person Certificates* issued by the FNMT-RCM, whose Specific Certification Practices and Certification Policy are defined in this document, are technically considered to be *Qualified Certificates*, in compliance with the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, and in accordance with the Law 06/2020, of 11 November, regulating certain issues in electronic trust services, regarding the applicants's identity validation and circumstances, and the reliability and warranty of the Trust Services provided by the FNMT-RCM

1.2. DOCUMENT NAME AND IDENTIFICATION

4. 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.

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

   a. 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.

   b. 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.

6. This document therefore sets out the *Specific Certification Policies and Certification Practices* for the *Natural Person Certificates.*

Name: *Certification Policy for Natural Person Certificates*

Reference/ OID[1]: 1.3.6.1.4.1.5734.3.10.1.

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

Version: 1.9

Date of issue: 03/02/2025

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

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

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

7. 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)*.

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

9. The FNMT-RCM provides this document, as well as the *GCPS* document to the *Electronic Community* and other interested parties, specifying the following:

   a. The terms and conditions that regulate the use of the *Certificates* issued by the FNMT-RCM.

   b. The *Certification Policy* that applies to *Certificates* issued by the FNMT-RCM.

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

c. The limits of usage for the *Certificates* issued under the terms of this *Certification Policy*.

d. The obligations, guarantees and responsibilities of the parties involved in the issuing and use of the *Certificates*.

e. The periods of conservation of the information gathered in the registration process and the events occurring in the systems of the *Trust Services Provider* in relation to the management of the life cycle of the *Certificates* issued under the terms of this *Certification Policy.*

1.3. PKI PARTICIPANTS

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

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

1.3.1. Certification Authority

11. 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 - AC RAIZ FNMT-RCM Certificate

AC RAIZ FNMT-RCM Certificate	
Subject	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Issuer	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	5D 93 8D 30 67 36 C8 06 1D 1A C7 54 84 69 07
Validity	Not before: 29 October 2008 Not after: 1 January 2030
Public key length	RSA 4.096 bits

AC RAIZ FNMT-RCM Certificate	
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 AC Certificate

Subordinate AC Certificate	
Subject	CN = AC FNMT Usuarios, OU = CERES, O = FNMT-RCM, C = ES
Issuer	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	45 5f 3A E1 5C 21 CD BA 54 4F 82 AA 47 51 EB DB
Validity	Not before: 28 October 2014 Not after: 28 October 2029
Public key length	RSA 2048
Signature algorithm	RSA - SHA256
Key identifier	B1 D4 4F C4 23 79 FA 44 05 09 C6 EB 39 CF E8 35 B0 B8 20 64

1.3.2. Registration Authority

12. The Registration Authority deals with identifying the applicant, and with checking the documentation supporting the facts recorded in the *Certificates*, validating and approving applications for those *Certificates* to be issued, revoked and, where appropriate, renewed.

13. 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. Certificate Subscribers

14. The *Subscribers* for the certificates issued under the present *SPPS* are natural person who shall mantain under their sole control the *Private Keys* associated to their *Certificates*.

1.3.4. Relying parties

15. Relying parties are natural or legal persons other than the *Subscriber* that receive and/or use *Certificates* issued by FNMT-RCM and, as such, are subject to the provisions of this *SPPS* where they decide to effectively rely on such *Certificates*.

1.3.5. Other participants

16. No stipulation.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

17. 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" and ETSI IN 319 412-2 "Certificate profile for certificates issued to natural persons"

18. The *Natural Person Certificate* is the electronic certificate issued by the FNMT-RCM that links a *Subscriber* to a series of *Signature verification data* and confirms his/her identity.

19. The *Certificates* issued under the terms of this *Certification Policy* will be considered to be valid as electronic signature and identification systems, in accordance with the Law 39/2015, of October 1st, on the Common Administrative procedures of public administrations based on *Qualified electronic certificates* that are admitted by virtue of their inclusion in the Trust Service lists (TSL) in accordance with the technical specifications specified in the Annex of Commission Decision 2009/767/EC, of 16 October (modified by Commission Decision 2010/425/EU, of 28 July 2010), which adopts measures that facilitate the use of electronic procedures through single-service windows, in accordance with Directive 2006/123/EC, of 12 December 2006, of the European Parliament and Council, regarding services of the internal market. These Trust Service lists contain information regarding *Certification Service Providers* that issues *Qualified electronic certificates* to the public, supervised in each member State, including the FNMT-RCM.

1.4.2. Prohibited certificate uses

20. 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*.

21. 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.
- To sign or seal software or components.
- To generate time stamps for *Electronic dating* procedures.
- To provide services for no consideration or for valuable consideration, except where previously authorised on a case-by-case basis, including, but not limited to:
    - Providing *OCSP* services.
    - Generating *Revocation Lists.*
    - Providing notification services.

1.5. POLICY ADMINISTRATION

1.5.1. Organization administering the document

22. 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

23. FNMT-RCM's contact address as *Trust Service Provider* is as follows:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

Email: ceres@fnmt.es

Telephone: + 34 91 740 69 82

24. 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.

25. 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

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

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

27. 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:

- *Natural Person Certificate:* Qualified certificate issued by the "AC FNMT Usuarios" to a natural person who acts as the Signer. This is a specific type of certificate issued by the FNMT-RCM, and therefore shall be subject to the conditions established in its specific policy and certification practices.
- *Subscriber:* The individual who signs the terms and conditions of use of a Certificate. In the case of the Natural Person Certificates issued under the terms of this Policy, this is the same person as the Holder.
- *Trust Service:* An electronic service that consists of one of the following activities: the creation, verification, validation, management, and conservation of Electronic Signatures, electronic seals, Timestamps, electronic documents, electronic delivery services, website authentication, and Electronic Certificates, including Electronic Signature and electronic stamp certificates.
- *Titular* (de un *Certificado*): Es la persona física, mayor de 18 años o menor emancipado, cuya identidad queda vinculada a los *Datos de verificación de firma* (*Clave Pública*) del *Certificado* expedido por el *Prestador de Servicios de Confianza*. Por tanto, la identidad del *Titular* se vincula a lo firmado electrónicamente utilizando los *Datos de creación de firma* (*Clave Privada*) asociados al *Certificado*.

1.6.2. References

28. 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 REPOSITORIES RESPONSIBILITIES

2.1. REPOSITORY

29. 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

30. 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

31. 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.

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

2.4. ACCESS CONTROLS ON REPOSITORIES

33. 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

34. *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

35. 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.

36. 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

37. 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).

38. The Common Name field of *Electronic Signature Certificates* defines the *Natural person* to whom the *Certificate* has been issued.

3.1.3. Anonymity or pseudonymity of subscribers

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

3.1.4. Rules used to interpreting various name forms

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

3.1.5. Uniqueness of names

41. 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 trademark

42. 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 the Private Key

43. FNMT-RCM neither generates nor stores the *Private Keys* associated with *Certificates,* issued under these *SPPS*, the generation of which is exclusively controlled by the *Subscriber.*

3.2.2. Authentication of Organization and Domain Identity

44. *Certificates* issued by FNMT-RCM under these *SPPS* do not include information inregards relationship between the Subscriber (always a natural person) and any organization, therefore, the validation of said information is not applicable.

3.2.3. Authentication of individual applicant identity

45. The FNMT-RCM, as a Trust Services Provider, before it issues the Natural Person Certificate, will identify the Applicant of the Certificate, either by physical presence in front of a person with the capacity to carry out the accreditation with the participation of a Registry Office with which the FNMT-RCM has signed an agreement, or to which a rule or administrative resolution applies, or by means of a valid electronic certificate that confirms the identity of the natural person making the application, or using other nationally recognized identification methods that provide equivalent security in terms of reliability to physical presence, in accordance with the eIDAS Regulation. For this purpose, the FNMT-RCM will accept electronic natural person Certificates issued by it and the electronic Certificates that are incorporated into the DNIe.

46. The FNMT-RCM will develop the appropriate controls to verify the veracity of the information included in the Certificate.

3.2.3.1 Direct check by physical presence

47. *Applicants* for *Natural Person Certificates* must physically visit a *Registry Office* to formalize the procedure for the confirmation of personal identity, visiting the authorized *Registry Office,* with the following identification media. Spanish citizens: National Identity Document,

Passport or with other means allowed by law for the purposes of identification (which indicate the National Identity Document Number). UE citizens: Foreign Identification Card or Citizen Registration Certificate of Union (where Tax ID number is included), and Passport or identity document of country of origin, or Official document of grant of the Tax ID number and Passport or identity document of country of origin. Foreign citizens: Foreign Identification Card (where Tax ID number is included) or Official document of grant of the Tax ID number and Passport. The person responsible for accreditation in the *Registry Office* will verify that the documents provided comply with all of the requirements to confirm the identity of the *Applicant*.

48. The appearance by the *Applicant* will not be required if the signature on the application for the issuing of a *Certificate* has been legitimated in the presence of a notary, if an electronic certificate is used as a means of identification as specified in the following section, or if the *Certificate* is requested, in accordance with the conditions in the section "*Renewal of Natural Person Certificates*" of this document.

3.2.3.2 Verification using electronic identification means

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

- A *Natural Person Certificate* issued under the terms of this *Policy*.
- One of the electronic *Certificates* incorporated into the DNIe

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

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

51. The FNMT-RCM will issue the *Natural Person Certificate* without the need for the applicant to visit a Registry Office, using nationally recognized identification methods that provide equivalent security in terms of reliability to physical presence to identify the *Applicant*, in accordance with the eIDAS Regulation.

52. The applicant will identify him/herself through the unassisted remote video-identification system (asynchronous). The remote video-identification process will include, among other measures, the verification and validation of the identity document, as well as its correspondence with the certificate applicant, through technologies such as facial recognition, and to verify that an applicant is a living person who is not being impersonated. This process requires the subsequent review of the captured evidence (identity document, facial image, and video) by an agent. Such accreditation will be carried out in accordance with ar. 24.1.d) of the eIDAS Regulation, the Law 6/2020, of 11 November, art.7.2 and the Order ETD/465/2021, of May 6, which regulates the methods of remote video identification for the issuance of qualified electronic certificates.

3.2.4. Non-verified Subscriber information

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

3.2.5. Validation of authority

54. Once the identity of the *Applicant* has been confirmed by the *Registry Office*, the *Registry Office* will validate the information and send it to the FNMT-RCM, along with the application code sent to the *Applicant* by email. This information will be sent via secure communications established for such purpose between the *Registry Office* and the FNMT-RCM. The personal information and their processing, in such case, shall be subject to the specific legislation.

55. Prior to the issuance of the Certificate, the FNMT_RCM establishes additional controls, such as confirming that the applicant is not registered as deceased in the records that the Ministry of Justice communicates to this Entity for this purpose.

56. Certificates will not be issued to minors, unless they hold and prove their emancipated status. The Registry Office will be in charge of carrying out the validations related to this point.

3.2.6. Criteria for interoperation

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

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

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

59. 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

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

3.3.2. Identification and authentication for re-key after revocation

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

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

62. 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.

63. 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

64. The Applicant for this type of Certificate can only be a natural person, of legal age or minor, who proves his emancipated status, in possession of his National Identity Document number or Foreigner Identification Number.

4.1.2. Registration process and responsibilities

65. The interested party visits the website of the *Trust Services Provider* of the FNMT-RCM at the URL http://www.cert.fnmt.es, where the instructions for the entire process for obtaining the *Natural Person Certificate* will be displayed. The *Applicant* must enter their National Identity Document number or Tax Identification Number, first surname, and email address in the information collection form provided for this. The *Applicant* will also indicate his/her desire to obtain a *Natural Person Certificate* and give consent for the FNMT-RCM to consult the Identity Data Verification System.

66. The *Public* and *Private Keys* are then generated (on a cryptographic device - Token or cryptographic card - if the *Applicant* has one, or in the browser if they do not have one of these devices), which will be linked to the *Certificate* that will be generated in a later phase, and the FNMT-RCM assigns the application a unique code.

67. The *Applicant* must previously consult the General and Specific Certification Practice Statements at the URL http://www.ceres.fnmt.es/dpcs/ with the conditions of use and obligations of the parties.

68. When this application is made, the *Public Key* that is generated is sent to the FNMT-RCM, along with the corresponding proof of possession of the *Private Key*, for the later issuing of the *Certificate*. The sending of the *Public Key* to the CA for the generation of the *Certificate* is done using a standard format, PKCS#10 or SPKAC, and using a secure channel.

69. After the FNMT-RCM receives this information, it will use the applicant's *Public Key* to verify the validity of the information in the application, verifying only the possession and correspondence of the pair of Cryptographic keys by the applicant.

70. This information shall not result in the generation of a *Certificate* by the FNMT-RCM until it receives confirmation from the *Registry Office* of the identification of the applicant. This notwithstanding, the possibility of electronic identification of the applicant for the *Natural Person Certificate* will be taken into account, generating, in such case, the *Certificate* without the *Applicant* being required to physically visit a *Registry Office* to accredit his/her identity.

71. The *Natural Person Certificate* application procedure is completed with the transmission by the FNMT-RCM of an email to the address provided by the *Applicant*, specifying the unique application code assigned and informing the *Applicant* of the upcoming phases in the process to obtain the *Certificate*.

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

4.2. CERTIFICATION APPLICATION PROCESSING

4.2.1. Performing identification and authentication functions.

73. *Applicants* will supply the requested information and evidence of their personal identity. The FNMT-RCM, through the Registry Office, will verify the identity of the applicant and will keep the documentation that proves it.

74. For the issuance of Electronic Signature Certificates, the FNMT-RCM may identify the applicant, as an alternative to appearing at the Registry Office, by using a qualified Electronic Signature Certificate as described in section "3.2.3.2 *Verification using electronic identification means*". For the issuance of Electronic Signature Certificates, the FNMT-RCM may identify the *Applicant*, as an alternative to appearing at the *Registry Office*, by means of the FNMT-RCM's unassisted remote video identification system, as described in section "3.2.3.3. *Indirect verification by means of assurance equivalent to physical presence in accordance with national law*". In order to initiate the identity verification process, the *Applicant* must have previously applied for the Certificate of Natural Person and obtained the corresponding application code. In addition, the *Applicant* must also accept the terms of use and privacy policy.

75. After obtaining the evidence to verify the identity by remote means, the FNMT-RCM, through a qualified operator authorized by the *Registration Authority*, will review the recorded identification process and will check the evidence generated by the system to accept or reject the validity of the identification process, in accordance with the applicable regulations on the causes for rejection of the video identification.

76. The personal data collected to perform the identity verification will be stored by the FNMT-RCM for the periods of time established by the specific applicable regulations.

4.2.2. Approval or rejection of certificate applications

77. 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 and, once received at the FNMT-RCM and provided that they are in conformity, the Certificate will be issued. In case of video identification, its admission or rejection will be communicated to the applicant in order to restart the process or obtain the identification by other means.

78. The transmission of information to the FNMT-RCM will be carried out through secure communications established for this purpose between the Registry Office and the FNMT-RCM.

79. 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.

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

4.2.3. Time to process Certificate Applications

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

4.3. CERTIFICATE ISSUANCE

4.3.1. CA actions during issuance

82. 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.

83. The issuance of *Certificates* results in the generation of electronic documents confirming the Subscribers identity, 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.

84. 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.

85. 108. FNMT-RCM will in no case have a Certificate include information other than that referred to herein, or any circumstances, specific attributes of the Signatories or restrictions other than the ones indicated in the present *SPPS*.

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

- To check that the *Certificate Applicant* use the *Private Key* for the *Public Key* linked to the *Certificate.* FNMT-RCM will therefore check that the *Private Key* corresponds to the *Public Key*.
- To ensure that the information included in the Certificate is based on the information provided by the relevant Registration Office.
- Not to ignore known facts potentially affecting Certificate reliability.
- To ensure that the DN (distinguished name) assigned to a Subject under this SPPS is unique.

87. The following steps will be taken to issue the *Certificate*:

1. Certificate data structure composition.

   The data collected when processing the Certificate application is used to compose the distinguished name (*DN*) based on standard *X.500*, making sure that the name is meaningful and unambiguous.

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

88. 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

89. Upon the *Certificate* being issued, FNMT-RCM will inform *Applicants* that the *Certificate* is available for download.

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1. Conduct constituting certificate acceptance

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

91. The FNMT-RCM will make available exclusively to the *Holder* for retrieval the *Natural Person Certificate,* at the website http://www.cert.fnmt.es

92. In this guided process, the *Applicant* will be asked to enter the National Identity Document (DNI) or Foreign Resident Identification Number (NIE), first surname, and the corresponding application code obtained in this process. This application code will be used as the accepted key for the generation by the *Holder* of an electronic signature of the conditions of use of the *Certificate*, as a mandatory requirement to download the certificate and accept the conditions of use, sending these signed conditions to the FNMT-RCM. If the *Natural Person Certificate* has not been generated yet for any reason, the process will inform the applicant of this.

93. When the *Natural Person Certificate* is downloaded, it will be installed on the support on which the *Keys* will be generated during the application process (cryptographic token or if not, the Navigator from which the application was made). The aforementioned website of the FNMT-RCM indicates the supported *Browsers* and the certificate installation requirements.

4.4.2. Publication of certificate by the CA

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

4.4.3. Notification of issuance to other entities

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

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber's Private Key and certificate usage

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

97. The *Certificates* issued under the terms of this *Certification Policy* will be considered to be valid as electronic signature and identification systems, in accordance with the Law 39/2015, of October 1st, on the Common Administrative procedures of public administrations based on *Qualified electronic certificates*.

4.5.2. Relaying party Public Key and certificate usage

98. 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

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

4.6.1. Circumstances for certificate renewal

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

4.6.2. Who may request renewal

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

4.6.3. Processing certificate renewal requests

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

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

104. 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

105. 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

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

4.7. CERTIFICATE RE-KEYS

107. 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.

108. *Natural Person Certificates* may only be renewed a single time. *Holders* who have already renewed their *Certificates* and would like to continue using a *Natural Person Certificate* under the terms of these *Specific Certification Practices and Policies*, must request a new *Certificate* and confirm their identity in accordance with the procedure described in the section "Verification of identity by physical visit" in this document.

109. The renewal of the *Natural Person Certificates* issued by the FNMT-RCM to the *Subscribers* of the *Certificates* may be requested provided that at the time of the request they have a *Certificate* in force and the associated *Signature creation data*, and that this request is made during the sixty (60) days prior to the *Expiration* of the *Certificate*.

110. The renewal of a *Natural Person Certificate* shall consist of the generation of new *Signature verification data* and *Signature creation data*, as well as the issuing of a new *Natural Person Certificate*. The renewal request will be made through the URL http://www.ceres.fnmt.es.

111. The *Certificate* that is close to expiration shall remain valid until its period of effectiveness expires. If the revocation of the *Natural Person Certificate* is requested during the periods of time that the *Holder* has two active *Certificates*, the FNMT-RCM shall revoke both *Certificates*.

112. The procedure established for the renewal of a *Natural Person Certificate* does not require the physical visit by the person making the request, because the person will be identified telematically by using his/her *Signature creation data*. Both application process as well as the process for obtaining the *Certificate* will be done telematically, requiring in any case the generation of an *Advanced electronic signature* by the person making the request, using a *Qualified Certificate*, of the renewal application document. However, telematic renewal of the *Natural Person Certificate* shall only be allowed if less than 5 years have elapsed since the physical visit and identification of the *Holder* established in article 7.6 of the Law 06/2020, of 11 November, regulating certain issues in electronic trust services.

113. The functions of the DNIe shall be taken into account for the purposes of identification, in accordance with its specific legislation.

114. The use of renewed *Natural Person Certificates* is subject to the same general and specific conditions that are in effect at any given time and that are established for this type of *Certificates* in their corresponding *Certification Practices Statement*.

4.7.1. Circumstances for certificate re-key

115. *Certificates* shall be re-keyed where the current keys are to expire soon, upon request by the renewal applicant.

4.7.2. Who may request re-key

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

4.7.3. Processing certificate re-keying requests

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

4.7.4. Notification of certificate re-key

118. 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

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

4.7.6. Publication of the re-keyed certificate

120. 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

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

4.8. CERTIFICATE MODIFICATION

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

4.8.1. Circumstance for certificate modification

123. The modification is not stipulated.

4.8.2. Who may request certificate modification

124. The modification is not stipulated.

4.8.3. Processing certificate modification requests

125. The modification is not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

126. The modification is not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

127. The modification is not stipulated.

4.8.6. Publication of the modified certificate by the CA

128. The modification is not stipulated.

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

129. The modification is not stipulated.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

130. *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.

a) Revocation of the *Certificate* in any of the events provided for herein.

131. 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*.

132. For the aforementioned purposes, the issuing of a *Natural Person Certificate*, when there is another for the same *Subscriber* in force shall immediately result in the revocation of the previous *Certificate*. The only exception to this occurs when the issuing of a *Natural Person Certificate* is as a result of a renewal process for the certificate within a period of sixty (60) days prior to the expiration date, in which the *Certificate* that is close to expiring shall remain valid until its validity period has expired. During this time, if the *Certificate* in question is revoked in accordance with the following section, the validity of both *Certificates* shall be extinguished.

133. 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

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

135. 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* support.

- Use by third parties of the *Signature Creation Data* corresponding to the *Signature Verification Data* contained in the *Certificate* and linked to the personal identity of the *Holder*.
- 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) Judicial or administrative resolutions that order this.

c) Decease or full or supervening incapacity of the *Holder*.

d) Inaccuracies in the information provided by the *Applicant* to obtain the *Certificate*, or the alteration of the information provided to obtain the *Certificate*, or the modification of the verified circumstances for the issuing of the *Certificate*, in such a way that it is no longer consistent with reality.

e) Contravening of a significant obligation of this *Certification Practices Statement* by the *Certificate Holder* or *Applicant*, if, in the latter case, this may have affected the procedure for the issuing of the *Certificate*.

f) The violation or endangerment of the secrecy of the *Signature Creation Data*.

g) Contravening of a significant obligation in this *Certification Practices Statement* by a *Registry Office*, if this may have affected the procedure for the issuing of the *Certificate*.

h) Termination of the contract signed between the *Holder* and the FNMT-RCM.

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

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

137. 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 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 f) above, after the revocation *Requestor* is identified.

138. Nevertheless, the FNMT-RCM may revoke the *Natural Person Certificates* itself in the cases included to in b) to i) in this *Certification Practices Statement*.

139. 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.

140. 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

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

4.9.2. Who can request revocation

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

- the *Certification Authority* and the *Registration Authority*
- the *Subscriber* 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.

143. 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

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

145. The revocation of a *Natural Person Certificate* may only be requested by the *Subscriber* or person with sufficient powers of representation, in the case of supervening incapacity of the *Holder*, under the terms specified in these *Specific Certification Policies and Practices*.

146. 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.

147. 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.

148. If the *Subscriber* is in possession of a *Natural Person Certificate* and its associated *Signature creation data*, it is possible to authenticate the *Subscriber*'s identity based on this certificate, so the revocation of the *Certificate* may be requested via Internet, or any other equivalent method that allows the connection to the URL http://www.ceres.fnmt.es, following the directions indicated on the website. This service will be available twenty-four (24) hours a day, 365 days a year, except in circumstances beyond the control of FNMT-RCM or during maintenance operations. The FNMT-RCM will announce maintenance operations at the URL http://www.ceres.fnmt.es, if possible, with at least forty-eight (48) hours' notice, and will try to resolve the situation within a period of no more than twenty-four (24) hours.

149. 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 applicant 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*.

150. If the A*pplicant* cannot provide the required data or it is resolved that this person does not fulfill the requirements to ask for a revocation, the revocation request will be dismiss.

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

152. 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

153. 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

154. FNMT-RCM processes *Certificate* revocation immediately upon checking the *applicant's* identity or, as the case may be, once the authenticity of a request made by means of a court or administrative decision has been checked. In any case, the *Certificate* will be effectively revoked within less than 24 hours of the revocation request being received.

4.9.6. Revocation checking requirement for relying parties

155. 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

156. *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

157. *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

158. 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. Online revocation/status checking requirements

159. 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

160. Not defined.

4.9.12. Special requirements related to key compromise

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

4.9.13. Circumstances for suspension

162. *Certificate* suspension is not supported.

4.9.14. Who can request suspension

163. *Certificate* suspension is not supported.

4.9.15. Procedure for suspension request

164. *Certificate* suspension is not supported.

4.9.16. Limits on the suspension period

165. *Certificate* suspension is not supported.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational characteristics

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

4.10.2. Service availability

167. 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

168. Not stipulated.

4.11. END OF SUBSCRIPTION

169. 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.

170. 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.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policies and practices

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

4.12.2. Session key encapsulation and recovery policies and practices

172. No stipulation.

5. PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

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

5.1. PHYSICAL SECURITY CONTROLS

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

5.1.1. Site location and construction

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

5.1.2. Physical access

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

5.1.3. Power and air conditioning

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

5.1.4. Water exposures

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

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

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

5.1.7. Waste disposal

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

5.1.8. Off-site backup

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

5.2. PROCEDURE CONTROLS

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

5.2.1. Trusted roles

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

5.2.2. Number of persons required per task

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

5.2.3. Identification and authentication for each role

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

5.2.4. Roles requiring separation of duties

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

5.3. PERSONNEL CONTROLS

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

5.3.1. Qualifications, experience, and clearance requirements

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

5.3.2. Background check procedures

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

5.3.3. Training requirements

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

5.3.4. Retraining frequency and requirements

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

5.3.5. Job rotation frequency and sequence

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

5.3.6. Sanctions for unauthorized actions

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

5.3.7. Independent contractor requirements

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

5.3.8. Documentation supplied to personnel

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

5.4. AUDIT-LOGGING PROCEDURES

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

5.4.1. Types of events recorded

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

5.4.2. Frequency for processing logs

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

5.4.3. Retention period for audit logs

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

5.4.4. Protection of audit log

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

5.4.5. Audit log backup procedures

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

5.4.6. Audit collection system (internal vs. external)

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

5.4.7. Notification to event-causing subject

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

5.4.8. Vulnerability assessments

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

5.5. RECORDS ARCHIVAL

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

5.5.1. Types of records archived

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

5.5.2. Retention period for archive

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

5.5.3. Protection of archive

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

5.5.4. Archive backup procedures

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

5.5.5. Requirements for time-stamping of records

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

5.5.6. Archive collection system (internal or external)

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

5.5.7. Procedures to obtain and verify archive information

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

5.6. CA KEY CHANGEOVER

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

5.7. COMPROMISE AND DISASTER RECOVERY

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

5.7.1. Incident and compromise handling procedures

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

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

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

5.7.3. Entity Private Key compromise procedures

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

5.7.4. Business continuity capabilities after a disaster

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

5.8. TRUST SERVICE PROVIDER TERMINATION

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

6. TECHNICAL SECURITY CONTROLS

221. 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

222. 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

223. No stipulation.

6.1.1.3 Subscribers Key Pair Generation

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

6.1.2. Private key delivery to subscriber

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

226. 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

227. 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

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

6.1.5. Key sizes and algorithms used

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

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

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

6.1.6. Public key parameters generation and quality checking

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

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

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

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

234. 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.

235. The key usage purposes of *Natural Person Certificates* are exclusively encryption, authentication and signature.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

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

6.2.2. Private Key (n out of m) Multi-person Control

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

6.2.3. Private Key Escrow

238. 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

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

6.2.5. Private Key Archival

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

6.2.6. Private Key Transfer into or from a Cryptographic Module

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

6.2.7. Private Key Storage on Cryptographic Module

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

6.2.8. Activating Private Keys

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

244. 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

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

6.2.10. Destroying Private Keys

246. 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

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

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

248. See the relevant section in the *GCPS*

6.3.2. Certificate operational periods and key pair usage periods

249. 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 Key pair: until 28 October 2029.
- *Electronic Signature Certificates* and Key pair: not in excess of 4 years.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

250. 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

251. 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

252. No stipulations.

6.5. COMPUTER SECURITY CONTROLS

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

6.5.1. Specific Computer Security Technical Requirements

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

6.5.2. Computer Security Rating

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

6.6. LIFE CYCLE TECHNICAL CONTROLS

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

6.6.1. System development controls

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

6.6.2. Security management controls

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

6.6.3. Life cycle security controls

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

6.7. NETWORK SECURITY CONTROLS

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

6.8. TIME-STAMPING

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

6.9. OTHER ADDITIONAL CONTROLS

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

6.9.1. Control of the ability to provide services

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

6.9.2. Control of systems development and computer applications

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

7. CERTIFICATE, CRLS AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

265. *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".

7.1.1. Version number

266. *Electronic Signature Certificates* conform to standard X.509 version 3.

7.1.2. Certificate extensions

267. 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

268. 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 formats

269. *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.

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

7.1.5. Name constraints

271. 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

272. 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 the policy constraints extension

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

7.1.8. Policy qualifiers syntax and semantics

274. 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 semantic for the critical certificate policies extension

275. 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

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

7.2.2. CRL and CRL entry extensions

277. 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
Issue date	UTC issuance time.
Date of next upgrade	Issue date + 24 hours
Authority key identifier	Issuer key hash
ExpiredCertsOnCRL	NotBefore CA value
Distribution Point	Distribution point URLs and CRL scope
Certificates revoked	Certificates revocation list, containing at least serial number and revocation date for each entry

7.3. OCSP PROFILE

7.3.1. Version number

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

7.3.2. OCSP extensions

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

8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS

280. 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".

281. 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".

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

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

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

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

284. The corresponding audit plans will be prepared periodically.

285. 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.

286. 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

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4. TOPICS COVERED BY ASSESSMENT

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

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6. COMMUNICATION OF RESULTS

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

8.7. AUTOEVALUATION

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

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

9.1.1. Certificate issuance or renewal fees

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

9.1.2. Certificate access fees

295. No stipulation.

9.1.3. Revocation or status information access fees

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

9.1.4. Fees for other services

297. The FNMT-RCM may apply rates and payment means which it considers appropriate at any time by the remote video-identification process. The price and terms of payment of the video-identification service may be consulted on the website of the FNMT – RCM.

9.1.5. Refund policy

298. The *Certificates* issued under this DPPP are free. The remote video-identification process has a price for the service.

299. The remote video-identification process has a return policy, which establishes that, once the identity accreditation has been approved by our qualified agents, the service will have been executed in its entirety. Therefore, the right of withdrawal is not applicable to the Applicant in accordance with the provisions of Article 103. a) of Royal Legislative Decree 1/2007, of November 16, 2007, which approves the revised text of the General Law for the protection of Consumers and Users and other supplementary laws.

9.2. FINANCIAL RESPONSIBILITY.

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

9.2.1. Insurance coverage

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

9.2.2. Other assets

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

9.2.3. Insurance or warranty coverage for end-entities

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

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1. Scope of confidential information

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

9.3.2. Information not within the scope of confidential information

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

9.3.3. Responsibility to protect confidential information

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

9.4. PRIVACY OF PERSONAL INFORMATION

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

9.4.1. Privacy plan

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

9.4.2. Information treated as private

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

9.4.3. Information not deemed private

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

9.4.4. Responsibility to protect private information

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

9.4.5. Notice and consent to use private information

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

9.4.6. Disclosure pursuant to judicial or administrative process

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

9.4.7. Other information disclosure circumstances

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

9.5. INTELLECTUAL PROPERTY RIGHTS

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

9.6. REPRESENTATION AND WARRANTIES

9.6.1. CA representations and warranties

317. FNMT-RCM's representations and warranties as *Trust Service Provider* to the *Signatory*, and to the other members of the *Electronic Community*, shall be mainly set out in the document containing the terms of use or the *Certificate* issuance agreement, and, secondarily, in this *Certification Policy and Practice Statement*.

318. 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.

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

9.6.2. RA representations and warranties

320. 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:

i) Certifiably verify the identity and any personal circumstances of the *Applicants* of the relevant *Certificates* for the purposes of the *Certificates*, using any of the means permitted by Law, and in accordance with the provisions in the *GCPS*, and specifically in this *Specific Certification Practices Statement*.

ii) Conserve all of the information and documentation related to the *Natural Person Certificates*, whose application, renewal or revocation it manages, for the period of time established in the legislation in effect.

iii) Allow the FNMT-RCM access to the files and to audit its procedures in relation to the data obtained in its role as a Registry Office.

iv) Inform the FNMT-RCM of any aspect that affects the *Certificates* issued by said Entity (eg: requests for issuance, renewal ...).

v) Notify the FNMT-RCM promptly of the applications for the issuing of *Certificates*.

vi) In regard to the expiration of the validity of the *Certificates*:

1. Duly verify the causes for the revocation that could affect the validity of the *Certificates*.

2. Notify the FNMT-RCM promptly of the applications for the revocation of the *Certificates*.

vii) In regard to the Protection of personal information, the provisions in the corresponding section of the *GCPS* shall apply.

viii) The *Registry Offices*, through the personnel assigned to the service by virtue of labour or civil service relationships, must exercise public functions in accordance with the specific legislation that applies to the FNMT-RCM.

321. In any case, the FNMT-RCM may bring suit against the Registry Office that carried out the identification procedure, initiating the corresponding actions, if the cause of the damages originated through the culpable or negligent actions of the Registry Office.

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

9.6.3. Subscriber representations and warranties

9.6.3.1 Signatory representations and warranties

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

324. The *Applicant* shall hold the FNMT-RCM harmless and defend at his/her own expense against any action that may be undertaken against the Entity as a result of false information provided

during the aforementioned *Certificate* issuing procedure, or against any damages suffered by the FNMT-RCM as a result of an action or omission of the *Applicant.*

6.1.1.2 RA Subscriber representations and warranties

325. In addition to the obligations and responsibilities of the parties listed in this the *GCPS*, the *Holder* of the *Natural Person Certificate*, as the signer of the *Certificate* and the *Keys*, has the following obligations:

- Adequately store the *Certificate* and the *Signature Creation Data*, and in such case, the *Certificate* support or card, providing the means necessary to prevent their use by persons other than the *Holder* or the legitimate possessor of the *Certificate*.
- Not use the *Certificate* when any of the information included in the *Certificate* is incorrect or inaccurate, or there are security reasons that advise against the use of the *Certificate*.
- Notify the FNMT-RCM of the loss, theft, or suspected theft of the *Certificate*, the *Signature Creation Data*, the *Certificate* support or card of the *Holder*, in order to initiate, in such case, the process to revoke the *Certificate*.

326. The *Subscriber* shall be responsible for notifying the FNMT-RCM regarding any variation in the status or information in regard to the information reflected in the *Certificate*, to revoke and reissue the *Certificate*.

327. Likewise, the *Subscriber* shall be responsible in relation to the members of the *Electronic Community* and other User Entities, or in such case, to third parties, for improper use of the *Certificate*, or false information in it, or actions or omissions that cause damages to the FNMT-RCM or third parties

328. The *Subscriber* shall therefore be responsible and obliged not to use the *Certificate* if the *Trust Services Provider* has terminated its activity as a *Certificate* issuing Entity and the substitution stipulated by Law has not taken place. In any case, the *Subscriber* shall not use the *Certificate* in the cases in which the *Signature / Seal Creation Data* of the Provider may be threatened and/or compromised, and the Provider has communicated this, or in such case, if the *Subscriber* has become aware of these circumstances.

9.6.4. Relying party representations and warranties

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

9.6.5. Representations and warranties of other participants

330. No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

331. No stipulation.

9.8. LIMITATIONS OF LIABILITY

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

9.9. INDEMNITIES

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

9.9.1. CA indemnity

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

9.9.2. Subscribers indemnity

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

9.9.3. Relying parties indemnity

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

9.10. TERM AND TERMINATION

9.10.1. Term

337. This *Certification Policies and Practice Statement* shall enter into force upon being published.

9.10.2. Termination

338. This *Certification Policies and Practice Statement* shall be repealed when a new version of the document is published. The new version shall fully supersede the previous document. FNMT-RCM agrees to review that Statement on a yearly basis.

9.10.3. Effects of termination and survival

339. For valid *Certificates* issued under a previous *Certification Policies and Practice Statement*, the new version will prevail over the previous version to the extent not in conflict therewith.

9.11. INDIVIDUAL NOTICES AND COMMUNICATION WITH PARTICIPANTS

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

9.12. AMENDMENTS

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

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

9.12.3. Circumstances under which an OID must be changed

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

9.13. DISPUTE RESOLUTION PROVISION

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

9.14. GOVERNING LAW

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

9.15. COMPLIANCE WITH APPLICABLE LAW

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

9.16. MISCELLANEOUS PROVISIONS

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

9.16.1. Entire Agreement

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

9.16.2. Assignment

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

9.16.3. Severability

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

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

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

9.16.5. Force Majeure

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

9.17. OTHER PROVISIONS

353. None stipulated.