Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SPECIFIC CERTIFICATE POLICIES AND CERTIFICATION PRACTICES STATEMENTS FOR CONSULAR CERTIFICATES

	NAME	DATE
Prepared by:	FNMT-RCM	20/06/2025
Revised by:	FNMT-RCM	20/06/2025
Approved by:	FNMT-RCM	23/06/2025

VERSION	DATE	DESCRIPTION
1.0	15/11/2024	Document creation: Specific Certification Policies and Certification Practices for Consular Certificates
1.1	23/06/2025	General review. The identity validation process is modified.

Reference: DPC/DCPCON_0101/SGPSC/2025
Document classified as: *Public*

Table of contents

1. INTRODUCTION

1.1. OVERVIEW

1. This document forms an integral part of the FNMT-RCM's *General Statement of Practices for Trust and Electronic Certification Services (GCPS),* and its purpose is to provide public information on the conditions and characteristics of the certification services and services for the issuance of electronic *Certificates* by the FNMT-RCM as a *Trust Service Provider.* setting out the obligations and procedures that it undertakes to comply with in relation to the *Consular Certificate* issued by the CA Consulares G2, specifically for Spaniards residing or non-resident abroad who wish to apply for a certificate and are not in possession of their National Identity Document (DNI) in force for legal reasons or have never had it

2. In particular, for the purposes of interpreting these *Particular Certification Policies and Practices*, the "Definitions" section of the *General Statement of Trust Services and Electronic Certification Practices* should be taken into account.

3. *Consular Certificates* issued by the FNMT-RCM whose *Certification Policy and Particular Certification Practices* are defined in this document are considered *Qualified Certificates* in accordance with 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, amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 as regards the establishment of the European Digital Identity Framework (hereinafter, Regulation (EU) No 910/2014), which establishes a more homogeneous framework with regard to electronic identification, defining new security standards, and in accordance with Law 6/2020, of 11 November, regulating certain aspects of electronic trust services, in terms of verifying the identity and other circumstances of applicants and the reliability and guarantees of the certification services provided by the FNMT – RCM

1.2. DOCUMENT NAME AND IDENTIFICATION

4. The FNMT-RCM's *Statement of Certification Practices* as a *Trust Service Provider* is structured, on the one hand, by the common part of the FNMT-RCM's *General Statement of Trust Services and Electronic Certification Practices* (GCPS), since there are similar levels of action for all the Entity's trust services and, on the other hand, by the specific sections of this document that constitutes the *Statement of Particular Certification Policies and Practices*. However, the *Law on the Issuance* of each type of *Certificate* or group of *Certificates* may establish special characteristics applicable to the bodies, agencies, entities and personnel using the FNMT-RCM's trust services.

5. Therefore, the structure of the FNMT-RCM *Statement of Certification Practices* is as follows:

   a. On the one hand, the ***General Statement of Trust Services Practices and Electronic Certification***, which should be considered the main body of the *Statement of Certification Practices* in which the liability regime applicable to the members of the *Electronic Community* is described, the security controls applied to the procedures and facilities of the FNMT-RCM, in what can be published without harming their effectiveness, the rules of secrecy and confidentiality, as well as issues relating to the ownership of their goods and assets, the protection of personal data and other matters of a general information nature that must be made available to the public, regardless of their role in the Electronic Community.

b. And, on the other hand, for each trust service or set or group of *Certificates*, identified and differentiated from the rest by its particular or differentiating type and regime, there are specific ***Certification Policies*** that describe the obligations of the parties, the limits of use of the *Certificates* and responsibilities and ***Particular Certification Practices*** that develop the terms defined in the corresponding policy and provide additional or specific to the general ones established in the *General Statement of Trust Services and Electronic Certification Practices*.

   This *Statement of Particular Certification Policies and Practices* specifies what is articulated in the main body of the *General Statement of Trust Services Practices and Electronic Certification* and, therefore, are an integral part of it, both forming the FNMT-RCM *Statement of Certification Practices*. However, they are only applicable to the set of *Certificates* characterized and identified in the corresponding *Particular Certification Policies and Practices* and may also have specialties set out in the *Law on the Issuance* of the *Certificate* or the corresponding group of *Certificates*, in the event that there are specific characteristics or functionalities.

6. This document defines the set of *Certification Practices* adopted by the FNMT-RCM as a *Trust Service Provider* for the management of the life cycle of *Consular Certificates* for Spaniards residing abroad and do not have a DNI for a lawful reason (or having one, it has lost its validity).

Name: *Consular Certificate* Certification Policy

Reference / OID[1]: 1.3.6.1.4.1.5734.3.26.1.0

Associated policy type: 0.4.0.194112.1.0

Version: 1.1

Date of issue: 23/06/2025

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

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

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

7. These Particular Certification Policies and Practices for *Consular Certificates* are part of the Statement of Certification Practices and will take precedence over the provisions of

[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.*

the main body of the *General Statement of Trust Services and Electronic Certification Practices*.

8. Therefore, in the event that there is a contradiction between this document and the provisions of the *General Statement of Trust Services and Electronic Certification Practices*, the provisions herein will take precedence.

9. The FNMT-RCM thus makes available to the *Electronic Community* and other interested parties, both this document and the GCPS document of the FNMT-RCM, which detail:

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

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

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

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

e. The retention periods of the information collected in the registration process and of the events produced in the *Trust Services Provider's* systems related to the management of the life cycle of the *Certificates* issued under this *Certification Policy*.

1.3. PKI PARTICIPANTS

10. The parties involved in the management and use of the *Trust Services* described in this *Statement of Certification Policies and Particular Certification Practices* (*SPPS*) are the following:

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

1.3.1. Certification Authority

11. The FNMT-RCM is the *Certification Authority* that issues the Electronic Certificates that are the subject of this *Statement of Particular Certification Policies and Practices* (SPPS). For these purposes, there are the following Certification Authorities:

a) Root Certification Authority. This Authority exclusively issues *Certificates* from subordinate Certification Authorities. The root Certificate of this CA is identified by the following information:

Table 1 – CA ROOT FNMT-RCM G2 Certificate

CA Certificate RAIZ FNMT-RCM G2	
Subject	CN=CA RAIZ FNMT-RCM G2, ORG_ID=VATES-Q2826004J, O=FNMT-RCM,C=ES
Issuer	CN=CA RAIZ FNMT-RCM G2, ORG_ID=VATES-Q2826004J, O=FNMT-RCM,C=ES
Serial Number (hex)	1F:B6:4F:91:9E:C5:01:EA:B1:21:28:BB:11:7A:00:3C:7C:5A:EF:1A
Validity	Not before: October 10, 2024; Not after: October 4, 2049.
Public Key Length	ECC 384
Signature algorithm	SHA-384 ECDSA
Key Identifier	A4:D6:B7:70:E7:65:A9:BF:17:EC:D7:B5:E0:3B:85:2D:61:2F:A7:1D

b) Subordinate Certification Authorities: they issue the *Certificates* of the final entity subject to this SPPS. The *Certificate* of said Authority is identified by the following information:

Table 2 – Subordinate CA Certificate

Subordinate CA Certificate	
Subject	CN=CA CONSULARES G2, ORG_ID=VATES-Q2826004J, O=FNMT-RCM, C = ES
Issuer	CN=CA RAIZ FNMT-RCM G2, ORG_ID=VATES-Q2826004J, O=FNMT-RCM,C=ES
Serial Number (hex)	43 5A 58 19 18 E0 46 DB 23 CA 63 DA E0 FA 06 87 31 1B 4C 35
Validity	Not before: October 10, 2024; Not after: October 07, 2039
Public Key Length	ECDSA (P-256)
Signature algorithm	SHA-384 with ECDSA
Key Identifier	F3:A6:1C:1B:06:71:63:2E:0A:93:51:FF:0D:2D:E6:66:A0:05:84:D7

1.3.2. Registration Authority

12. The Registration Authority carries out tasks of identification of the applicant, holder of the certificates, as well as the verification of the documentation and evidence accrediting the circumstances contained therein, the validation and approval of the applications for issuance, revocation and, where appropriate, the renewal of said Certificates.

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* of the *Consular Certificates* will be, under the approach set out in this report, Spanish citizens residing or non-resident abroad who, for lawful reasons, are not in possession of their National Identity Document or who, having it, it is not valid, who keep under their exclusive use the *Signature Creation Data* associated with said *Certificates*

1.3.4. Relying Parties

15. The relying parties are those natural or legal persons, other than the *Subscriber*, who receive and/or use *Certificates* issued by the FNMT-RCM and, as such, the provisions of this SPPS apply to them when they decide to effectively rely on such *Certificate*

1.3.5. Other participants

16. Not stipulated.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

17. The *Consular Certificates* to which this SPPS applies are *Qualified Certificates* in accordance with Regulation (EU) No. 910/2014 and in accordance with the requirements established in the European standards ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

18. The *Consular Certificate* is the electronic certification issued by the FNMT-RCM that links a Subscriber with *Signature Verification Data* and confirms their identity.

19. *Electronic Signature Certificates* issued under this *Certification Policy* are issued to natural persons and are considered valid as electronic identification and signature systems, in accordance with Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations, based on qualified electronic certificates that are admitted by virtue of their inclusion in the lists of trust services (TSL) in accordance with the technical specifications set out in Annex to Commission Decision 2009/767/EC of 16 October 2009 (as amended by Commission Decision 2010/425/EU of 28 July 2010) adopting measures to facilitate the use of electronic procedures through one-stop-shops, pursuant to Directive 2006/123/EC, of 12 December 2006 of the European Parliament and of the Council on services in the internal market. These lists of trust services contain

information relating to the *Trust Service Providers* that issue qualified *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 *User Entity* or a third party wishes to rely on the *Electronic Signature* made with one of these *Certificates*, without accessing the *Information and Consultation Service on the validity status of the certificates* issued under this *Certification Policy*, it will not be covered by these *Specific Certification Policies and Practices*, and there will be no legitimacy to claim or take legal action against the FNMT RCM for damages, losses or conflicts arising from the use of or reliance on a *Certificate*.

21. This type of *Certificate* may not be used for:

- Sign another *Certificate*, except in cases expressly authorized in advance.
- Sign software or components.
- Generate *Time Stamps* for *Electronic Dating* procedures.
- To provide services free of charge or for consideration, except in cases expressly authorized in advance, such as but not limited to:
    - Provide *OCSP* services.
    - Generate *Revocation Lists*.
    - Provide notification services.

1.5. POLICY ADMINISTRATION

1.5.1. Organization administering the document

22. The Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, Entidad Empresarial, Medio Propio (hereinafter, FNMT-RCM), with NIF Q2826004-J, is the Certification Authority that issues the *Certificates* to which this *Statement of Certification Practices and Policies* applies.

1.5.2. Contact details

23. The contact address of the FNMT-RCM as a *Trust Service Provider* is as follows:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda
Dirección de Servicios Digitales e Innovación- CERES Department
C/ Jorge Juan, 106
28071 – MADRID
Email: ceres@fnmt.es
Mobile: (+ 34) 91 740 69 82

24. To report security issues related to a certificate, such as suspected key compromise, misuse, or fraud, please send us a Certificate Incident Report to the following email address: incidentes.ceres@fnmt.es.

1.5.3. Person determining CPS suitability for the policy

25. The FNMT-RCM Management has, within its powers, the capacity to specify, review and approve the review and maintenance procedures, both for the *Particular Certification Practices* and for the corresponding *Certification Policy*.

1.5.4. CPS approval procedure

26. The FNMT – RCM, through its *Trust Services Provider* management committee, ensures compliance with the *Statements of Certification Policies and Practices*, approves them and carries out the relevant review process, on an annual basis.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

27. For the purposes of the provisions of this document, particularizing the definitions of the *General Statement of Trust Services and Electronic Certification Practices* and only when the terms begin with a capital letter and are in italics, the following shall be understood:

- *Consular Certificate*: Signature Certificate whose Subscriber is a natural person with Spanish nationality, of legal age, resident or non-resident abroad, in possession of a Central Consular Identification Number (NICC) and who is not in possession of their National Identity Document (DNI) in force for lawful reasons or has never had it, in accordance with the provisions of Royal Decree 991/2024, of 1 October, on the registration of persons of Spanish nationality in the Registration Registers of Consular Offices abroad. This is a specific type of certificate issued by the FNMT – RCM and, therefore, will be subject to the conditions established in its Particular Certification Policy and Practices.
- *Central Consular Identification Number:* A unique and non-transferable and permanent identification number, granted by the Consular Registration Registry, in coordination with the Ministry of the Interior, in accordance with Royal Decree 991/2024, of 1 October, on the registration of Spanish nationals in the Registration Registers of Consular Offices abroad.
- *Trust Service*: An electronic service that consists of any of the following activities: the creation, verification, validation, management and conservation of Electronic Signatures, electronic stamps, Time Stamps, electronic documents, electronic delivery services, website authentication and Electronic Certificates, including Electronic Signature and Electronic Seal certificates.
- *Subscriber*: An individual who subscribes to the terms and conditions of use of a Certificate. In the Consular Certificates issued under this Policy, it coincides with the person of the Holder.
- *Holder (of a Certificate):* It is the natural person, with Spanish nationality, of legal age, either habitually resident abroad or temporarily there, in possession of a Central Consular Identification Number (NICC) and who is not in possession of their National Identity Document (DNI) in force for lawful reasons or has never had it, whose identity is linked to the Signature Verification Data (Public Key) of the Certificate issued by the Trust Service Provider. Therefore, the identity of the Holder is linked to what is electronically signed using the Signature Creation Data (Private Key) associated with the Certificate.

1.6.2. Acronyms

28. For the purposes of this SPPS, the following acronyms apply, the meaning of which is in accordance with the European standard ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates"

CA: Certificate Authority
AR: Registration Authority
ARL: Certificate Authority Revocation List
CN: Common Name
CRL: Certificate Revocation List
CPS: *Certificate* Revocation List
DN: Distinguished Name
***GCPS*:** General Statement of Trust Services and Electronic Certification Practices
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
NICC: Central Consular Identification Number
OCSP: Online *Certificate* Status Protocol
OID: Object IDentifier
PKCS: Public Key Cryptography Standards
UTC: Coordinated Universal **Time**

2. PUBLISHING AND REPOSITORIES

2.1. REPOSITORY

29. The FNMT-RCM, as a *Trust Service Provider*, maintains a repository of public information, available 24 hours a day, 7 days a week every day of the year, at the address:

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

2.2. PUBLICATION OF CERTIFICATION INFORMATION

30. The information relating to the issuance of electronic *Certificates* subject to this *DPPP* 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 modification to the *General Statement of Trust Services and Electronic Certification Practices* or to the *Particular Certification Policies and Practices* will be published immediately at the URL where they are accessed.

32. As for the frequency of publication of CRLs, it is defined in the section "4.9.7 Frequency of generation of CRLs".

2.4. CONTROL OF ACCESS TO REPOSITORIES

33. All the aforementioned repositories are freely accessible for consultation and, where appropriate, downloading of information. Likewise, the FNMT-RCM has established controls to prevent unauthorized persons from adding, modifying or deleting information included in its repositories and to protect the authenticity and integrity of such information.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMES

34. The encryption of the *Certificates* follows the RFC 5280 standard "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All fields defined in the *Certificates* profile in the *Certification Policies and Particular Certification Practices*, except in the fields specifically stated otherwise, use UTF8String encoding.

3.1.1. Types of names

35. The electronic *Certificates* of the end entity subject to this *SPPS* contain a distinguished name (*DN*) in the Subject Name field, which is composed as described in the information relating to the *Certificate* profile.

36. In the identity accreditation procedure, as a prior step to the issuance of a *Consular Certificate* of electronic signature, the FNMT-RCM, through the *Registration Office*, will verify the true identity of the Subscriber.

3.1.2. Meaning of names

37. All distinguished names (*DN*) in the Subject Name field are meaningful. The description of the attributes associated with the *Certificate Subscriber* is human-readable (see section 7.1.4 Format of names herein).

38. The Common Name field of the *Consular Certificates* defines the *Subscriber* to whom the *Certificate* has been issued.

3.1.3. Pseudonyms

39. Regarding the identification of *Subscribers* through the use of the *Certificates* issued under this Certification Policy, the FNMT – RCM does not allow the use of pseudonyms.

3.1.4. Rules used to interpret various name formats

40. The requirements defined by the X.500 standard of reference in the standard apply ISO/IEC 9594.

3.1.5. Uniqueness of names

41. The distinctive name (DN) assigned to the *Certificates* issued to a *Subscriber*, under these SPPS and within the domain of the *Trust Service Provider*, it will be unique.

3.1.6. Trademark Recognition and Authentication

42. The FNMT-RCM does not assume any commitment regarding the use of distinctive signs, registered or not, in the issuance of the *Certificates* issued under this *Certification Policy*. The request for *Certificates* is only allowed that include distinctive signs whose right of use is owned by the *Owner* or is duly authorized. The FNMT-RCM is not obliged to previously verify the ownership or registration of the distinctive signs before the issuance of the *Certificates*, even if they appear in public registers.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Methods for proving possession of the private key

43. The FNMT-RCM does not generate or store the *Private Keys* associated with the *Certificates* issued under these *Certification Policies and Particular Certification Practices*, which are generated under the exclusive control of the *Subscriber*.

3.2.2. Authentication of the organization's identity

44. The *Certificates* issued under these *Certification Policies and Particular Certification Practices* do not incorporate information on the relationship of the Subscriber (always a natural person) with any organization, so the validation of such information is not applicable.

3.2.3. Authentication of the identity of the applicant natural person

45. The FNMT-RCM, as a *Trust Service Provider*, before issuing *a Consular 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 *Registration Office* with which the FNMT-RCM has signed an agreement, or to which a rule or administrative resolution applies, or by means of using those means that guarantee the verification of the specific attributes of the person with a high level of confidence, in accordance with Regulation (EU) No. 910/2014 in its Article 24.1.c). To this end, the use of video-identification is foreseen as a nationally recognized method that provides equivalent security, in terms of reliability, to the physical presence of applicants, in accordance with the provisions of Article 7.2 of Law 6/2020, of 11 November.

46. The FNMT-RCM will carry out 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 *Consular 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: Passport, once they have obtained the* NICC. 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

following section of this document.

3.2.3.2 *Indirect verification by means of assurance equivalent to physical presence in accordance with national law*

49. The FNMT-RCM may issue the *Consular Certificate* by means of the identification of the Applicant using nationally recognized identification methods that provide equivalent security in terms of reliability to physical presence, in accordance with Regulation (EU) No 910/2014, such as the remote video identification of an applicant. It is required to verify the authenticity and validity of the identity document, as well as its correspondence with the applicant for the certificate. To this end, the video remote identification system used in the process must incorporate the technical and organizational means necessary to verify the authenticity, validity and integrity of the identification documents used, verify the correspondence of the holder of the document with the applicant carrying out the process, using technologies such as facial recognition, and verify that this is a living person who is not being impersonated.

50. The *Applicant* will identify themselves through the non-assisted (asynchronous) video remote identification system. Identity verification will be based on facial recognition using biometric procedures, the provision of the identification document required to prove their identity and the obtaining of other evidence. Such accreditation shall be carried out in accordance with Article 24(1)(c) of Regulation (EU) No 910/2014; Article 7.2 of Law 6/2020, of 11 November and complying with the organizational and technical conditions and requirements established by Order ETD/465/2021 of 6 May, which regulates the methods of remote video identification for the issuance of qualified electronic certificates.

3.2.4. Unverified Subscriber Information

51. All information incorporated into the electronic *Certificate* is verified by the *Registration Authority*.

3.2.5. Validation of authorization

52. Once the *Registration Office* has confirmed the identity of the *Applicant*, the data will be validated together with the application code sent to the *Applicant* by email. This transmission of information will be carried out through secure communications established for this purpose. Personal data and their processing, where appropriate, will be subject to specific legislation.

53. Prior to the issuance of the *Certificate*, the FNMT-RCM establishes additional controls, such as, for example, confirming that the applicant is not registered as deceased in the registers that the Ministry of Justice communicates to this Entity for that purpose. fin.

54. *Certificates* will not be issued to minors.

3.2.6. Interoperation criteria

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

3.3. IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS

56. Under these *Certification Policies*, the FNMT-RCM does not contemplate any key regeneration process.

57. The conditions for authenticating a renewal request are set out in the section corresponding to the *Certificate* renewal process of this document.

3.3.1. Routine renewal

58. Under these *Certification Policies*, the FNMT-RCM does not contemplate any routine renewal process.

3.3.2. Renewal after a revocation

59. Under these *Certification Policies*, the FNMT-RCM does not contemplate any renewal process after a revocation.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

60. Prior to the effective revocation of the *Certificates*, the Registration Authority will reliably identify the *Applicant* for the *Revocation* in order to link them with the unique data of the *Certificate* to be revoked.

61. The conditions for authenticating a request for revocation are developed in the section corresponding to the process of revocation of *Certificates* in this document.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

4.1. APPLICATION FOR CERTIFICATES

4.1.1. Who can apply for a Certificate

62. The *Applicant* for this type of *Certificate* can only be a natural person, of legal age, resident or non-resident abroad, in possession of their Central Consular Identification Number (NICC) and who is not in possession of their National Identity Document (DNI) in force for lawful reasons or has never had it.

4.1.2. Registration process and responsibilities

63. The interested party accesses the website of the FNMT-RCM *Trust Service Provider*, through the address http://www.cert.fnmt.es, where the instructions for the complete process of obtaining the *Consular Certificate* will be displayed. The Applicant must enter their Passport ID Number, their first surname and their email address at the data collection point provided for this purpose. Likewise, the *Applicant* will express their willingness to obtain a *Consular Certificate* and will give their consent for the FNMT-RCM to consult the Consular Registration System.

64. Subsequently, the *Public* and *Private Keys* are generated (in the browser) that will be linked to the *Certificate* that will be generated at a later stage, and the FNMT – RCM assigns a request a unique code.

65. The Applicant must consult the General and Particular Statements of Certification Practices in advance at the address http://www.ceres.fnmt.es/dpcs/ with the conditions of use and obligations for the parties.

66. When making this request, the generated *Public Key* is sent to the FNMT-RCM, together with the corresponding proof of possession of the *Private Key*, for the subsequent issuance 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.

67. The FNMT-RCM, after receiving this information, will verify, by means of the *Applicant's Public Key*, the validity of the information in the application, the possession and correspondence of the pair of cryptographic *Keys* by the *Applicant*, as well as the size of the keys generated.

68. This information will not lead to the generation of a *Certificate* by the FNMT-RCM, as long as it does not receive confirmation of the electronic identification of the *Applicant*, carried out through their remote identification by video with the subsequent confirmation of the identity of the *Applicants* by the qualified agent with previous training or carried out through an identity confirmation made by a *Registration Office*.

69. The application procedure for the *Consular Certificate* ends with the FNMT – RCM sending an email to the address provided by the *Applicant* indicating the unique application code assigned and informing them of the next stages of the process of obtaining the *Certificate*.

70. Section 9.8 "Responsibilities" of this document sets out the responsibilities of the parties in this process.

4.2. PROCEDURE FOR APPLYING FOR CERTIFICATES

4.2.1. Performance of identification and authentication functions

71. For the issuance of *Consular Certificates, 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. The FNMT-RCM will admit, in any case, the function and report done by the *Registration Office*.

72. For the issuance of *Consular Certificates*, the FNMT-RCM, as an alternative to appearing at the *Registry Office*, could identify the *Applicant* by means of the FNMT-RCM's non-assisted video remote identification system, as described in section "3.2.3.2. *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 made the application for the *Consular Certificate* and obtained the corresponding application code. In addition, the *Applicant* must also accept the conditions of use and privacy policy.

73. 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 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 video identification.

74. The personal data collected to carry out 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 the certificate application

75. In the case of *Consular Certificates*, once the identity of the *Applicant* has been confirmed, the application must be reviewed by an agent who has previously received specific training on the characteristics verifiable by the identification method, its procedures, test methods and common methods of forgery. To do this, the agent will be responsible for verifying the identity of the *Applicant* based on the data received together with the application code. If the data are correct and compliance is verified, in addition to checking compliance with the security measures determined for this purpose, the Certificate will be issued by the FNMT-RCM.

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

77. The FNMT-RCM will collect from the *Applicants* the information that is necessary for the issuance of the Certificates and for the verification of identity, storing the information required by the electronic signature legislation for the period of fifteen years. (15) years processing it with due diligence to comply with current national legislation on the protection of personal data.

78. Personal data and their processing will be subject to specific legislation.

4.2.3. Time to process the request

79. The approved application for the *Consular Certificates* is automatically processed by the system in real time, so there is no established time for this process.

4.3. ISSUANCE OF THE CERTIFICATE

4.3.1. Actions of the CA during issuance

80. Once the FNMT-RCM has received the *Applicant's* personal data, as well as their application code, and their identity has been confirmed in accordance with the previous section, the *Consular Certificate* will be issued.

81. The issuance of *Consular Certificates* involves the generation of electronic documents that confirm the identity of the *Holder*, as well as their correspondence with the associated *Public Key*. The issuance of FNMT-RCM *Consular Certificates* can only be carried out by the FNMT-RCM itself, in its capacity as *Trust Service Provider*, and there is no other entity or body with the capacity to issue them.

82. The FNMT - RCM, by means of its *Electronic Signature* or *Electronic Seal*, authenticates the *Consular Certificates* and confirms the identity of the *Holder*. On the other hand, and in order to avoid the manipulation of the information contained in the *Certificates*, the FNMT - RCM will use cryptographic mechanisms that provide authenticity and integrity to the *Certificate*.

83. Under no circumstances shall the FNMT-RCM include in a *Certificate* information other than that shown herein, nor circumstances, specific attributes of the *Subscribers* or limits other than those provided for in this *Statement of Certification Practices*.

84. In any event, the FNMT-RCM shall act effectively to:

- Verify that the *Applicant* for the *Consular Certificate* uses the *Private Key* corresponding to the *Public Key* linked to the identity of the *Holder* of the Consular Certificate. To this end, the FNMT-RCM will check the correspondence between the *Private Key* and the *Public Key*.
- Ensure that the information included in the *Consular Certificate* is based on the information provided by the *Applicant*.
- Not ignore well-known facts that may affect the reliability of the *Consular Certificate*.
- Ensure that the DN (distinctive name) assigned in the *Certificate* is unique in the entire *Public Key Infrastructure* of the FNMT-RCM.

85. The issuance of *Consular Certificates* will take into account:

1. Composition of the data structure that makes up the *Certificate*

   With the data collected during the *Certificate* application process, the distinctive name (DN) is composed according to the X.500 standard, ensuring that this name makes sense and does not give rise to ambiguities.

2. Generation of the *Certificate* according to the corresponding *Certificate* Profile

86. The format of the *Certificates*, issued by the FNMT-RCM under this *Certification Policy*, in line with ITU-T X.509 version 3 and in accordance with the legally applicable regulations on *Qualified Certificates*, can be consulted on the website http://www.cert.fnmt.es/dpcs/

4.3.2. Certificate Issuance Notification

87. Once the *Consular Certificate* has been issued, the FNMT-RCM will inform the *Applicant* about the availability of the *Certificate* for download.

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1. Acceptance process

88. In the process of applying for the *Certificate*, the *Applicant* accepts the conditions of use and expresses his/her willingness to obtain the *Certificate*, as necessary requirements for its generation.

89. The FNMT-RCM will make its *Consular Certificate* available exclusively to the *Holder* so that it can be downloaded from the website http://www.cert.fnmt.es.

90. In this guided download process, the *Applicant* will be asked to enter his/her Passport ID Number, first surname, as well as the corresponding application code obtained in the process. This application code will be used, as an agreed key, for the generation by the *Holder* of an electronic signature of the conditions of use of the *Certificate*, as a requirement to access the download of the same and as acceptance of said conditions of use, sending them signed to the FNMT – RCM. If the *Consular Certificate* has not yet been generated for any reason, the process will inform you of this fact.

91. At the time of downloading the *Consular Certificate*, it will be installed in the medium in which the *Keys* were generated during the application process (*Browser* from which the application was made). The aforementioned FNMT-RCM website indicates the supported *Browsers* and installation rules for the certificates.

4.4.2. Publication of the certificate by the CA

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

4.4.3. Notification of the issue to other entities

93. No issuance notifications are made to other entities.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Private Key and Certificate Use

94. The FNMT-RCM does not generate or store the *Private Keys* associated with the *Certificates* issued under this *Certification Policy*. The condition of custodian, *Subscriber* and responsible for the control of the keys of the *Certificate* corresponds to the *Certificate Holder*.

95. *Consular Certificates* issued under this *Certification Policy* are qualified certificates issued to natural persons and are considered valid as electronic identification and signature systems, in accordance with Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations.

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

96. Third parties who rely on the *Electronic Signatures* made with the *Private Keys* associated with the *Certificate* will comply with the obligations and responsibilities defined in this *SPPS*.

4.6. RENEWAL OF THE CERTIFICATE

97. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* while maintaining the *public Key* of the same.

4.6.1. Circumstances for the renewal of the certificate

98. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* while maintaining the *public Key* of the same.

4.6.2. Who can apply for certificate renewal

99. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* while maintaining the *public Key* of the same.

4.6.3. Processing of Certificate Renewal Applications

100. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* while maintaining the *public Key* of the same.

4.6.4. Notification of certificate renewal

101. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* while maintaining the *public Key* of the same.

4.6.5. Conduct Constituting Acceptance of Certificate Renewal

102. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* while maintaining the *public Key* of the same.

4.6.6. Publication of the renewed certificate

103. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* while maintaining the *public Key* of the same.

4.6.7. Notification of certificate renewal to other entities

104. Under these Certification Policies, the FNMT-RCM does not renew *Certificates* while maintaining the *public Key* of the same.

4.6.8. Processing of Certificate Change Requests

105. No modification is stipulated.

4.7. RENEWAL WITH REGENERATION OF CERTIFICATE KEYS

106. Under these Certification Policies, the renewal with regeneration of *Consular Certificates* is always carried out by issuing new keys, following the same process as that described for the issuance of a new Certificate.

4.7.1. Circumstances for renewal with key regeneration

107. The keys of the *Certificates* shall be renewed due to the imminent expiration of the current keys, at the request of the applicant for renewal.

4.7.2. Who can apply for renewal with key regeneration

108. The same process as described for the issuance of a new *Certificate* shall be followed.

4.7.3. Processing Renewal Requests with Key Regeneration

109. The same process as described for the issuance of a new *Certificate* shall be followed.

4.7.4. Notification of renewal with key regeneration

110. The same process as described for the issuance of a new *Certificate* shall be followed.

4.7.5. Conduct that constitutes acceptance of renewal with key regeneration

111. The same process as described for the issuance of a new *Certificate* shall be followed.

4.7.6. Publication of the renewed certificate

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

4.7.7. Notification of renewal with key regeneration to other entities

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

4.8. MODIFICATION OF THE CERTIFICATE

114. It is not possible to make modifications to the *Certificates* issued. Therefore, any need for modification entails the issuance of a new *Certificate*.

4.8.1. Circumstances for the modification of the certificate

115. The modification is not stipulated.

4.8.2. Who can request the modification of the certificate

116. The modification is not stipulated.

4.8.3. Processing of Certificate Change Requests

117. The modification is not stipulated.

4.8.4. Notification of certificate amendment

118. The modification is not stipulated.

4.8.5. Conduct Constituting Acceptance of Certificate Amendment

119. The modification is not stipulated.

4.8.6. Publication of the amended certificate

120. The modification is not stipulated.

4.8.7. Notification of the modification of the certificate to other entities

121. The modification is not stipulated.

4.9. REVOCATION OF THE CERTIFICATE

122. *Consular Certificates* issued by the FNMT-RCM shall be null and void in the following cases:

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

b) Cessation of activity as a *Trust Service Provider* of the FNMT-RCM, unless, with the express consent of the *Subscriber*, the *Certificates* issued by the FNMT-RCM have been transferred to another *Trust Service Provider*.

In these two cases [a) and b)], the loss of effectiveness of the *Certificates* will take place from the time these circumstances occur.

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

123. The effects of the revocation of the *Certificate*, i.e. the termination of its validity, will take effect from the date on which the FNMT-RCM has certain knowledge of any of the determining facts and from the time of recording it in its *Information and Consultation Service on the status of the certificates*.

124. For the purposes listed above, the issuance of a *Consular Certificate* when there is another valid in favor of the same *Holder*, will entail the immediate revocation of the previous *Certificate*.

The FNMT-RCM makes available to *Subscribers*, trusted third parties, software providers and third parties a means of communication through the FNMT-RCM electronic office: https://www.sede.fnmt.gob.es/

4.9.1. Circumstances for revocation

4.9.1.1 Circumstances for the revocation of the certificate of the subscriber

125. A request for the revocation of the *Certificates* may be made during the period of validity stated in the *Certificate*.

126. The following shall be admissible grounds for the revocation of a *Consular Certificate*:

a) The request for revocation by the *Subscriber*. In any case, it must give rise to this request:

- Loss of *Certificate* Support
- The use by a third party of the *Signature Creation Data*, corresponding to the *Signature Verification Data* contained in the *Certificate* and linked to the personal identity of the *Holder*.
- The violation or endangerment of the secrecy of the *Signature Creation Data* or the private key associated with the *Certificate*.

- The non-acceptance of the new conditions that may entail the issuance of new *Statements of Certification Practices*, during the period of one month after their publication.

b) Judicial or administrative resolution ordering it.

c) Death or supervening disability, total or partial, of the *Account Holder*

d) Inaccuracies in the data provided by the *Applicant* to obtain the *Certificate*, or alteration of the data provided to obtain the *Certificate* or modification of the circumstances verified for the issuance of the *Certificate*, so that it was no longer in accordance with reality.

e) Contravention of a substantial obligation of this *Statement of Certification Practices* by the *Subscriber* or the *Applicant* for the *Certificate* if, in the latter case, it could have affected the procedure for issuing the *Certificate*.

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

g) Contravention of a substantial obligation of this *Statement of Certification Practices* by a *Registry Office* if it could have affected the procedure for issuing the *Certificate*.

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

i) Cessation of the activity of the *Trust Service Provider* unless the management of the electronic *Certificates* issued by it is transferred to another *Trust Service Provider.*

127. In no case does the FNMT-RCM assume any obligation to verify the points referred to in letters c) to f) of this paragraph, and they must be notified to this entity in a reliable manner by delivering the documents and information necessary to verify it.

128. The FNMT-RCM will only be liable for the consequences arising from not having revoked a *Certificate* in the following cases:

- That the revocation should have been made at the *Subscriber's* reliable request or through the systems made available by the FNMT-RCM for this purpose.
- That the request for revocation or the cause that motivates it, has been notified to it by means of a judicial or administrative resolution.
- That the causes c) to f) of this section are reliably accredited, after identification of the *Subscriber* and/or *Applicant* for the revocation (or person with sufficient powers of representation, if the *Subscriber* is incapacitated).

129. The FNMT-RCM may revoke the *Subscribers' Certificates* when causes b) to i) of this section occur.

130. Actions constituting a crime or misdemeanour of which the FNMT-RCM is not aware that are carried out on the data and/or *Certificate* and inaccuracies regarding the data or lack of diligence in their communication to the FNMT-RCM, will result in the FNMT-RCM being exonerated from liability.

131. The revocation of the *Certificates* implies, in addition to their extinction and the impossibility of continuing to use the associated *Signature Creation Data* or private keys,

the termination of the relationship and regime of use of said *Certificate* and its *Private Key* with the FNMT-RCM.

4.9.1.2 Circumstances for subordinate CA certificate revocation

132. The provisions of the "Action Plan for the Compromise of the Public Key Infrastructure of FNMT-RCM" will be complied with

4.9.2. Who can apply for revocation

133. The revocation of a *Certificate* may only be requested by:

- the *Certificate Authority* and the *Registration Authority*
- the *Subscriber* or authorized person
- where appropriate, the *Subscriber*, through the telephone number provided for this purpose (after identification of the Applicant) whose number is made public on the FNMT – RCM website and which will be operational available at all times.

134. The FNMT-RCM may revoke the *Certificates* in the cases set out in this Statement of Certification Practices and Policies.

4.9.3. Procedure for requesting revocation

135. The request for the revocation of *Consular Certificates* may be made during the period of validity stated in the *Certificate*.

136. The revocation of a *Consular Certificate* may only be requested by the *Holder* or person with sufficient powers of representation, if there is a supervening incapacity of the *Holder*, under the terms set forth in these *Certification Policies and Particular Certification Practices.*

137. The revocation process can be carried out uninterruptedly available 24 hours a day, 7 days a week, through the telephone Revocation Service made available to users for this purpose, ensuring the revocation of the *Certificate* within a period of less than 24 hours. This service will be available twenty-four (24) hours a day, every day of the year, except for circumstances beyond the control of the FNMT-RCM or maintenance operations. The FNMT-RCM will notify maintenance operations or unavailability of the service in http://www.ceres.fnmt.es, if possible, at least forty-eight (48) hours in advance and will try to resolve them within a period of no more than twenty-four (24) hours.

138. During the telephone revocation, the applicant for the revocation will have to confirm the data requested and provide those that are essential for the unequivocal validation of his or her capacity to request such revocation.

139. If the person who is requesting revocation cannot provide the required data or it is resolved that this person does not fulfill the requirements to ask for a revocation, the request for the revocation will be dismissed.

140. As soon as the revocation becomes effective, the *Subscriber* and applicant for the revocation will be notified via the e-mail address.

141. Once the FNMT-RCM has proceeded to revoke the *Certificate*, the corresponding *List of Revoked Certificates* will be published in the secure *Directory*, containing the serial number of the revoked *Certificate*, as well as the date, time and cause of revocation. Once a *Certificate* has been revoked, its validity is definitively extinguished, with no possibility of reversing its status.

4.9.4. Grace period of the revocation request

142. There is no grace period associated with this process, since the revocation is carried out immediately upon verified receipt of the request for revocation.

4.9.5. Time frame for processing the revocation request

143. The FNMT – RCM immediately revokes the *Certificate* at the time of verifying the identity of the *Applicant* or, where appropriate, the veracity of the application made by judicial or administrative decision. In any case, the effective revocation of the *Certificate* will be carried out in less than 24 hours from the receipt of the revocation request.

4.9.6. Obligation to verify revocations by relying parties

144. Third parties who trust and accept the use of the *Certificates* issued by the FNMT – RCMs are obliged to verify, through one of the available mechanisms (CRL and/or OCSP Revocation Lists), 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 generation frequency

145. *Revocation Lists* (CRLs) of *Consular Certificates* are issued at least every 12 hours, or when a revocation occurs, and have a validity period of 24 hours. The *CRLs* of the *Certificates of Authority* are issued every 6 months, or when there is a revocation of a subordinate *Certificate Authority* and have a validity period of 6 months.

4.9.8. Maximum latency period of CRLs

146. The publication of the *Revocation Lists* takes place at the time of the generation of said Lists, so that the latency period between the generation of the CRL and its publication is zero.

4.9.9. Availability of the online certificate status verification system

147. Information on the status of the *Certificates* will be available online 24 hours a day, 7 days a week. In the event of a system failure, the Business Continuity Plan will be implemented to resolve the incident as soon as possible.

4.9.10. Requirements for online revocation checks

148. Online checking of the revocation status of *Consular Certificates* can be carried out through the *Certificate Status Information Service*, offered through OCSP as described in section 4.10 of this document. The person interested in using this service must:

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

4.9.11. Other forms of notice of revocation available

149. Not defined.

4.9.12. Special requirements for revocation of compromised keys

150. See the corresponding section in the *GCPS*.

4.9.13. Circumstances for suspension

151. The suspension of Certificates is not contemplated.

4.9.14. Who can apply for suspension

152. The suspension of Certificates is not contemplated.

4.9.15. Procedure for requesting suspension

153. The suspension of Certificates is not contemplated.

4.9.16. Limits on the period of suspension

154. The suspension of Certificates is not contemplated.

4.10. CERTIFICATE STATUS INFORMATION SERVICES

4.10.1. Operational characteristics

155. The information relating to the validation of the *electronic Certificates* covered by this *SPPS* is accessible through the means described in the *GCPS*.

4.10.2. Service Availability

156. The FNMT-RCM guarantees access to this service, available 24 hours a day, 7 days a week, by *Users* and the parties relying on the *Certificates*, in a secure, fast and free manner.

4.10.3. Optional Features

157. Not stipulated.

4.11. TERMINATION OF SUBSCRIPTION

158. The subscription will end at the time of expiration of the validity of the *Certificate*, either due to expiration of the period of validity or due to its revocation. If the *Certificate* is not renewed, the relationship between the *Subscriber* and the FNMT-RCM will be considered terminated.

159. For the purposes listed above, it is hereby stated that the request for the issuance of a *Consular Certificate* issued by the FNMT-RCM when there is another valid in favor of the same *Subscriber*, and belonging to the same *Issuance Law*, will entail the revocation of the first one obtained.

4.12. CUSTODY AND RECOVERY OF KEYS

4.12.1. Key Custody and Recovery Practices and Policies

160. The FNMT-RCM will not recover the *Private Keys* of the *Certificate* holders.

4.12.2. Session Key Protection and Recovery Practices and Policies

161. Not stipulated.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

162. See the corresponding section in the *GCPS*.

5.1. PHYSICAL SECURITY CHECKS

163. See the corresponding section in the *GCPS*.

5.1.1. Location of the facilities

164. See the corresponding section in the *GCPS*.

5.1.2. Physical Access

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

5.1.3. Electricity and Air Conditioning

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

5.1.4. Exposure to water

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

5.1.5. Fire Prevention and Protection

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

5.1.6. Media Storage

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

5.1.7. Waste Disposal

170. See the corresponding section in the GCPS.

5.1.8. Off-site backups

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

5.2. PROCEDURAL CONTROLS

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

5.2.1. Trust roles

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

5.2.2. Number of people per task

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

5.2.3. Identification and authentication for each role

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

5.2.4. Roles requiring segregation of duties

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

5.3. PERSONNEL CONTROLS

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

5.3.1. Knowledge, qualifications, experience and accreditation requirements

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

5.3.2. Background Check Procedures

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

5.3.3. Training requirements

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

5.3.4. Requirements and frequency of training updates

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

5.3.5. Sequence and frequency of job turnover

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

5.3.6. Penalties for unauthorized actions

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

5.3.7. Recruitment requirements

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

5.3.8. Provision of documentation to staff

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

5.4. AUDIT PROCEDURES

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

5.4.1. Types of events logged

187. Véase el apartado correspondiente en la *GCPS*

5.4.2. Frequency of Log Processing

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

5.4.3. Retention period of records

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

5.4.4. Protecting records

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

5.4.5. Procedures for backing up audited records

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

5.4.6. Registration Collection Systems

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

5.4.7. Notification to the subject causing the events

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

5.4.8. Vulnerability Analysis

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

5.5. ARCHIVING RECORDS

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

5.5.1. Types of Archived Records

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

5.5.2. File retention period

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

5.5.3. File Protection

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

5.5.4. File Backup Procedures

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

5.5.5. Requirements for time-stamping of records

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

5.5.6. File System

201. See the corresponding section in the GCPS.

5.5.7. Procedures for obtaining and verifying archived information

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

5.6. CHANGING CA KEYS

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

5.7. INCIDENT AND VULNERABILITY MANAGEMENT

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

5.7.1. Incident and vulnerability management

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

5.7.2. Dealing with corrupted data and software

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

5.7.3. Procedure for compromise of the private key of the CA

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

5.7.4. Business continuity after a disaster

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

5.8. TERMINATION OF THE ACTIVITY OF THE TRUST SERVICE PROVIDER

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

6. TECHNICAL SECURITY CONTROLS

210. See the corresponding 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

211. In relation to the generation of the CA *Keys* that the FNMT-RCM needs for the development of its activity as a *Trust Service Provider*, see the corresponding section in the *GCPS*.

6.1.1.2. RA Key Pair Generation

212. Not stipulated.

6.1.1.3. Subscribers Key Pair Generation

213. In relation to the generation of the *Subscriber* ' s *Keys*, the FNMT-RCM does not generate or store the *Private Keys* associated with the *Certificates* issued under these *Certification Policies and Particular Certification Practices*, which are generated under the exclusive control of the *Subscriber*.

6.1.2. Private key delivery to subscriber

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

215. In any case, if the FNMT-RCM or any *Registration Office* becomes aware of unauthorized access to the *Subscriber's Private Key*, the *Certificate* associated with said *Private Key* will be revoked.

6.1.3. Public key delivery to certificate issuer

216. The *Public Key*, generated by the *Subscriber* together with the *Private Key* in a key generation and custody device, is delivered to the *Certification Authority* by sending the request for the *Certificate*.

6.1.4. Distribution of the CA Public Key to Trusting Parties

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

6.1.5. Key sizes and algorithms used

218. The algorithms used are:

- For CA FNMT G2 root: ecdsa-with-SHA384.
- For subordinate, Consular CA: ecdsa-with-SHA384.
- For *Consular Certificates*: ecdsa-with-SHA256.

219. As for the size of the keys, depending on each case, it is:

- Keys to the CA FNMT-RCM G2 root: ECC P-384.
- Codes of the Subordinate CA Consular G2: ECC P-256
- Keys of the *Consular Certificates*: ECC P-256 or RSA Encryption with a length of 2048 bits.

6.1.6. Public key generation and quality verification parameters

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

6.1.7. Supported Uses of Keys (KeyUsage field X.509v3)

221. FNMT *Certificates* include the Key Usage extension and extended Key Usage, indicating the authorized uses of the *Keys*.

222. The *Certificate* of the FNMT-RCM G2 root CA has enabled the uses of *Keys* to sign/seal the *Certificates* of the Subordinate FNMT CAs and the ARLs.

223. The Consular CA *Certificate* that issues the *Consular Certificates* is exclusively authorized for use to sign/seal Final Entity *Certificates* and CRLs.

224. *Consular Certificates* are exclusively enabled to use authentication and signature in all cases and the use of an encryption key is added to *Consular Certificates* with RSA key.

6.2. CRYPTOGRAPHIC PROTECTION OF THE KEY PRIVATE Y CONTROLS OF THE MODULES

6.2.1. Standards for cryptographic modules

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

6.2.2. Multi-person control (n of m) of the private key

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

6.2.3. Private Key Custody

227. The operations of copying, safeguarding or retrieving the *Private Keys* of the FNMT-RCM *Certification Authorities* are carried out under the exclusive control of the authorized personnel, using, at least, dual control and in a secure environment.

6.2.4. Private Key Backup

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

6.2.5. Private Key Archiving

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

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

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

6.2.7. Storing the Private Key in the Cryptographic Module

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

6.2.8. Private Key Activation Method

232. *Certificate Authority Private Keys* are generated and safeguarded by a cryptographic device that meets FIPS PUB 140-2 Level 3 security requirements.

233. The mechanisms for activating and using the *Certification Authority 's Private Keys* are based on the segmentation of management and operational roles that the FNMT- RCM has implemented multi-person access mechanisms based on cryptographic cards and their corresponding simultaneous use schemes.

6.2.9. Private Key Deactivation Method

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

6.2.10. Private Key Destruction Method

235. The FNMT-RCM will destroy or store the *Trust Service Provider* Keys in an appropriate manner once their validity period has expired, in order to prevent their inappropriate use.

6.2.11. Classification of cryptographic

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

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archiving

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

6.3.2. Certificate Operation Periods and Key Pair Usage Periods

238. The periods of operation of the *Certificates* and their associated *Keys* are:

- *Certificate* of the CA FNMT G2 root and its pair of *Keys*: until October 4, 2049.
- The *Certificate* of the subordinate CA that issues the *Consular Certificates*: until October 7, 2039.
- *Consular Certificates* and their pair of *Keys*: not older than 4 years.

6.4. ACTIVATION DATA

6.4.1. Generation and installation of activation data

239. The activation data, both for the *Keys* of the root Consular CA and for the *Keys* of the subordinate CA that issues the *Consular Certificates*, are generated during the ceremony of *Keys* for the creation of these *Certification Authorities*.

6.4.2. Protection of activation data

240. The activation data of the *Certificate Authority 's Private Keys* are protected, in accordance with the method described in section "6.2.8 *Private Key* activation method " of this document, with multi-person access mechanisms based on cryptographic cards and their corresponding simultaneous use schemes.

6.4.3. Other aspects of activation data

241. Not stipulated.

6.5. COMPUTER SECURITY CONTROLS

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

6.5.1. Specific technical requirements for IT security

243. See the corresponding section in the *GCPS*.

6.5.2. Assessment of the level of IT security

244. See the corresponding section in the *GCPS*.

6.6. TECHNICAL LIFE CYCLE CONTROLS

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

6.6.1. System Development Controls

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

6.6.2. Safety management controls

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

6.6.3. Lifecycle security controls

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

6.7. NETWORK SECURITY CONTROLS

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

6.8. SOURCE OF TIME

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

6.9. OTHER ADDITIONAL CONTROLS

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

6.9.1. Control of the capacity to provide services

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

6.9.2. Control of the development of computer systems and applications

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

7. PROFILES OF CERTIFICATES, CRLS AND OCSP

7.1. CERTIFICATE PROFILE

254. Consular Certificates are issued as "qualified" in accordance with the European standards ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI EN 319 412-2 " “Certificate profile for certificates issued to natural persons”

7.1.1. Version number

255. *Consular Certificates* are in accordance with the X.509 version 3 standard.

7.1.2. Certificate Extensions

256. On the website http://www.cert.fnmt.es/dpcs/ the document describing the profile of the *Consular Certificates* issued under this policy is published, including all their extensions.

257. All certificates issued under these certification policies shall contain a non-critical extension, qcStatements, using the qcStatement-2 predefined in RFC 3739, wherein all values in sematicsInformation shall be:

• semanticsIdentifier: id-etsi-qcs-semanticsId-Natural

• nameRegistrationAuthorities: https://exteriores.gob.es (URI generalName type)

7.1.3. Algorithm Object Identifiers

258. The object identifiers (OIDs) corresponding to the cryptographic algorithms used are:

- For the *CA FNMT G2 Root* and the CA Consular G2 *Subordinate* it is 1.2.840.10045.4.3.3 (ecdsa-with-SHA384).
- For the *Consular Certificates* it is 1.2.840.10045.4.3.2 (ecdsa-with-SHA256).

7.1.4. Name formats

259. The coding of *Certificates* follows RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All the fields defined in the profile of the *Certificates* of these *Certification Policies*, except in the fields specifically expressed otherwise, use the UTF8String encoding.

260. On page http://www.cert.fnmt.es/dpcs/ is published the document describing the profile of the *Consular Certificates* issued under this policy, including all its extensions.

261. The semantics of the serialNumber field will be as follows:

EX:ES-XXXXXXXXT,

where "xxxxxxxxT" is the Central Consular Identification Number (NICC) which is a unique and non-transferable and permanent identification number, granted by the Consular Registration Registry, in coordination with the Ministry of the Interior, in accordance with Royal Decree 991/2024, of October 1, on the registration of people of Spanish nationality in the Registration Registers of Consular Offices abroad.

7.1.5. Name restrictions

262. The distinctive name (*DN*) assigned to the *Subject* of the *Certificate* within the scope of this *SPPS* shall be unique and with the composition defined in the *Certificate* profile.

7.1.6. Certificate Policy Object Identifier

263. The object identifier (OID) of the *Consular Certificate* policy is as defined in the section "1.2 Name of the document and identification" of this document.

7.1.7. Use of Extension Policy Constraints

264. The "Policy Constrains" extension of the CA root *Certificate* is not used.

7.1.8. Syntax and semantics of policy qualifiers

265. The "Certificate Policies" extension includes two fields of Policy Qualifiers:

- CPS Pointer: contains the URL where the *GCPS* is published and the *Certification Policies and Particular Certification Practices* applicable to the *Certificates*.
- User notice: contains a text that can be displayed on the user's screen of the *Certificate* during its verification.

7.1.9. Semantic treatment for the extension "certificate policy"

266. The extension "Certificate Policy" includes the policy OID field, which identifies the policy associated with the *Certificate* by the FNMT-RCM, as well as the two fields listed in the previous section.

7.2. PROFILE OF THE CRL

7.2.1. Version number

267. The profiles of the CRLs are in accordance with the X.509 version 2 standard.

7.2.2. CRL and extensions

268. The profile of the CRLs follows the following structure:

Table 3 – CRL Profile

Fields and extensions	Value
Version	V2
Signature algorithm	ecdsa-with-SHA384
CRL Number	Incremental Value
Issuer	Issuer DN
Issue date	UTC issue time
Date of next upgrade	Issue date + 24 hours
Authority Key Identifier	Hash of the sender key
ExpiredCertsOnCRL	NotBefore de la CA
Distribution Point	Distribution point URLs and scope of the CRLs
Revoked Certificates	List of revoked certificates, containing at least for each entry, serial number, and date of revocation

7.3. OCSP PROFILE

7.3.1. Version number

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

7.3.2. OCSP Extensions

270. See the corresponding section in the *GCPS.*

8. COMPLIANCE AUDITS

271. The system for issuing *Certificates* is subject to an annual audit process in accordance with the 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".

272. Likewise, the Certificates are considered qualified, so the audit guarantees compliance with the requirements established in the European standards ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates".

273. The system for issuing *Certificates* is subject to additional audits:

- Audit of the Information Security Management System in accordance with UNE-ISO/IEC 27001 "Information Security Management Systems (ISMS). Requirements".
- Audit of the Information Privacy Management System in accordance with UNE-ISO/IEC 27701 "Information Privacy Management Systems (IMMS). Requirements".
- Audit as dictated in the National Security Scheme (Royal Decree 311/2022, of 3 May, which regulates the National Security Scheme in the field of Electronic Administration).
- Audit of the Quality Management System in accordance with ISO 9001.
- Audit of the Social Responsibility Management System in accordance 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/EC, and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (GDPR / LOPD-GDD).

274. Risk analyses are also carried out, in accordance with the provisions of the Information Security Management System.

8.1. FREQUENCY OF AUDITS

275. Corresponding audit plans shall be drawn up periodically.

276. The *Certificate Authority* issuing *Consular Certificates* is subject to periodic audits, in accordance with the European standard ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" and ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons". The audit is conducted annually by an accredited third-party firm.

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

8.2. QUALIFICATION OF THE AUDITOR

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

8.3. AUDITOR'S RELATIONSHIP WITH THE AUDITED COMPANY

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

8.4. ELEMENTS SUBJECT TO AUDIT

280. See the corresponding section in the *GCPS*.

8.5. DECISION-MAKING VS. DEFICIENCY DETECTION

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

8.6. COMMUNICATION OF RESULTS

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

8.7. SELF-ASSESSMENT

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

9. OTHER LEGAL AND ACTIVITY MATTERS

9.1. RATES

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

9.1.1. Certificate Issuance or Renewal Fees

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

9.1.2. Certificate access fees

286. Not stipulated.

9.1.3. Status or Revocation Information Access Fees

287. The FNMT-RCM provides information services on the status of certificates through CRL or OCSP free of charge.

9.1.4. Fees for Other Services

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

9.1.5. Refund Policy

The Certificates issued under this *SPPS* do not entail any cost for the *Subscribers*, so there is no need to establish a refund policy.

9.2. FINANCIAL RESPONSABILITY

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

9.2.1. Liability Insurance

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

9.2.2. Other assets

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

9.2.3. Insurance or warranty coverage for end-entities

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

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1. Scope of confidential information

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

9.3.2. Information not within the scope of confidential information

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

9.3.3. Responsibility to protect confidential information

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

9.4. PRIVACY OF PERSONAL INFORMATION

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

9.4.1. Privacy plan

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

9.4.2. Information treated as private

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

9.4.3. Information not deemed private

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

9.4.4. Responsibility to protect private information

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

9.4.5. Notice and Consent to Use of Private Information

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

9.4.6. Disclosure under judicial or administrative process

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

9.4.7. Other circumstances of disclosure of information

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

9.5. INTELLECTUAL PROPERTY RIGHTS

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

9.6. OBLIGATIONS AND GUARANTEES

9.6.1. CA Obligations

306. The obligations and responsibilities of the FNMT-RCM, as a *Trust Service Provider*, towards the *Holder* of the *Consular Certificate* and the rest of the members of the Electronic Community, will be determined mainly by the document relating to the conditions of use or the contract for the issuance of the *Certificate*. and, subsidiarily, by these Particular Certification Policies and Practices and by the GCPS.

307. The FNMT – RCM complies with the requirements of the technical specifications of the ETSI EN 319 411 standard for the issuance of qualified *Certificates* and undertakes to continue complying with this standard or those that replace it.

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

9.6.2. RA Obligations

309. In addition to the obligations and responsibilities of the parties listed in this document and in the *General Statement of Trust Services and Electronic Certification Practices*, *Registry Offices* are obliged to:

i) To reliably verify the identity and any personal circumstances of the *Applicants* for the *Certificates* relevant to their own purpose, using any of the means admitted by law, and in accordance with the provisions of the *GCPS* and in particular in this *Statement of Particular Certification Practices*.

ii) Keep all the information and documentation related to the *Consular Certificates*, whose application, renewal or revocation is managed during the period of time established in current legislation.

iii) To allow the FNMT-RCM access to the archives and the audit of its procedures in relation to the data obtained in its capacity as *Registry Office*.

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

v) To promptly notify the FNMT-RCM of requests for the issuance of *Certificates*.

vi) With respect to the expiration of the validity of the *Certificates*:

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

2. To promptly notify the FNMT-RCM of requests for the revocation of the *Certificates*.

vii) With respect to the Protection of Personal Data, the provisions of the corresponding section of the *GCPS* will apply.

viii) The Registry Offices, through the personnel assigned to the service by employment or civil servant relationship, must exercise public functions in accordance with the specific legislation applicable to the FNMT-RCM.

310. In any case, the FNMT-RCM may repeat against the *Registry Office* that it has carried out the identification procedure, initiating the corresponding actions, if the cause of the damage has its origin in the latter's intentional or culpable action.

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

9.6.3. Obligations of the Subscriber

9.6.3.1. Responsibility of the Applicant

312. The *Applicant* shall be responsible for the fact that the information submitted during the application for the *Certificate* is true and that the application and download of the *Certificate* is made from a computer or device that it can use, with a high level of confidence, under its exclusive control.

313. The *Applicant* shall keep the FNMT-RCM safe and defend at its own expense against any action that may be taken against this Entity as a result of the falsity of the information provided in the aforementioned procedure for the issuance of the *Certificate*, or against any damage and prejudice suffered by the FNMT-RCM as a result of an act or omission of the *Applicant*.

9.6.3.2. Subscriber's Liability

314. In addition to the obligations and responsibilities of the parties listed in the *GCPS*, the *Holder* of the *Consular Certificate*, as *Subscriber* of the *Certificate* and its *Keys*, has the obligation to:

- Properly safeguard the Certificate, the Signature Creation Data and, where appropriate, the card or support of the Certificate, putting the necessary means to prevent its use by persons other than its Holder.
- Do not use the *Certificate* when any of the data included in the *Certificate* is inaccurate or incorrect, or there are security reasons that make it advisable.

- Notify the FNMT-RCM of the loss, misplacement or suspicion of the *Certificate*, the *Signature Creation Data*, the card or support of the *Certificate* of which you are the *Holder*, in order to initiate, where appropriate, the procedures for its revocation.

315. It will be the responsibility of the *Holder* to inform the FNMT-RCM of any change in status or information with respect to what is reflected in the *Certificate*, for its revocation and reissuance.

316. Likewise, it will be the *Holder* who must answer to the members of the *Electronic Community* and other *User Entities* or, where appropriate, to third parties for the improper use of the *Certificate*, or for the falsehood of the statements contained therein, or acts or omissions that cause damage to the FNMT-RCM or to third parties.

317. It shall be the responsibility and, therefore, obligation of the *Holder* not to use the *Certificate* in the event that the *Trust Service Provider* has ceased its activity as a *Certificate* Issuing Entity and the subrogation provided for by law has not occurred. In any case, the *Owner* will not use the *Certificate* in cases in which the *Provider's Signature / Seal Creation Data* may be threatened and/or compromised, and this has been communicated by the *Provider* or, where appropriate, the *Owner* has been aware of these circumstances.

9.6.4. Obligations of the Relying Parties

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

9.6.5. Obligations of other participants

319. Not stipulated.

9.7. DISCLAIMER OF WARRANTIES

320. Not stipulated.

9.8. LIMITS OF LIABILITY

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

9.9. INDEMNITIES

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

9.9.1. Indemnification of the CA

323. Not stipulated.

9.9.2. Indemnification of Subscribers

324. Not stipulated.

9.9.3. Indemnification of Relying Parties

325. Not stipulated.

9.10. VALIDITY PERIOD OF THIS DOCUMENT

9.10.1. Deadline

326. This *Statement of Certification Practices and Policies* shall enter into force upon publication.

9.10.2. Termination

327. This *Statement of Certification Practices and Policies* shall be repealed at the time a new version of the document is published. The new version will replace the previous document in its entirety. The FNMT – RCM undertakes to submit this Statement to an annual review process.

9.10.3. Effects of termination

328. For current *Certificates* issued under a previous *Statement of Certification Practices and Policies*, the new version shall prevail over the previous version in all matters that do not conflict with the former.

9.11. INDIVIDUAL NOTIFICATIONS AND COMMUNICATION WITH PARTICIPANTS

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

9.12. MODIFICATIONS TO THIS DOCUMENT

9.12.1. Procedure for modifications

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

9.12.2. Reporting period and mechanism

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

9.12.3. Circumstances under which an OID should be changed

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

9.13. CLAIMS AND DISPUTE RESOLUTION

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

9.14. IMPLEMENTING REGULATIONS

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

9.15. COMPLIANCE WITH APPLICABLE REGULATIONS

335. The FNMT-RCM states that it complies with the applicable regulations.

9.16. MISCELLANEOUS PROVISIONS

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

9.16.1. Entire Agreement

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

9.16.2. Allocation

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

9.16.3. Severity

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

9.16.4. Compliance

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

9.16.5. Force Majeure

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

9.17. OTHER PROVISIONS

342. Not contemplated.