Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERTIFICATION POLICY AND PRACTICE STATEMENT FOR ELECTRONIC TIME STAMP CREATION CERTIFICATES

	NAME	DATE
Prepared by:	FNMT-RCM	17/06/2020
Reviewed by:	FNMT-RCM	18/06/2020
Approved by:	FNMT-RCM	19/06/2020

DOCUMENT HISTORY			
Version	**Date**	**Description**	**Author**
1.0	5/03/2019	Document creation	Quality Assurance Area
1.1	19/06/2020	General review	Quality Assurance Area

Reference: DPC/DPCTSU_0101/SGPSC/2020

Document classified as: *Public*

Table of contents

Tables

1. INTRODUCTION

1. The Spanish mint Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, hereinafter FNMT-RCM, with tax identification number Q2826004-J, is a public business entity as defined in Public Sector Legal System Act 40/2015, 1 October, which, being a public body, has distinct public legal personality, its own assets and cash flows, and independent management in terms of that Act.

2. It reports to the Ministry of Finance, which is responsible, through the Office of the Under-Secretary for Finance, for overseeing the Entity's strategy and for controlling its effectiveness as provided for in the aforementioned Act 40/2015.

3. FNMT-RCM has a long-standing track record engaging in its industrial activities, and is supported by the State. Ever since the entry into force of article 81 of Tax, Administrative and Social Measures Act 66/1997, 30 December, as amended, FNMT-RCM has contributed to broadening the range of services which it has been authorised to provide and has achieved a leading position in the provision of trust services.

4. In addition, through the CERES (Certificación ESpañola) Department, FNMT-RCM is an accredited *Qualified Trust Service Provider*, as defined in 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, through an independent entity within the framework of a certification scheme, as established in European standard ETSI EN 319 401 "General Policy Requirements for Trust Service Providers".

1.1. OVERVIEW

5. The purpose of this document is to provide public information as to the terms and features of *TSU Certificate* user trust services provided by FNMT-RCM as a *Trust Service Provider*, with specific reference to the obligations it agrees to fulfil in connection with:

   - management of *TSU Certificates* issued for provision of the *Time Stamping Service*, and the terms applicable to the application for, issuance, use and termination of *TSU Certificates*, and
   - provision of the *Certificate* status checking service and terms applicable to use of the service and warranties given.

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

7. FNMT-RCM is a Time Stamping Authority (TSA) and may establish such Time Stamping Units (TSU) as it shall consider appropriate in order to guarantee the provision of its Time Stamping Services, managing them based on distinct and specific policies and practices. The *Time Stamping Service Policy and Practice* Statement is duly identified with its requisite OID (0.4.0.2023.1.1) and is available at www.cert.fnmt.es/dpcs.

1.2. DOCUMENT NAME AND IDENTIFICATION

8. The name of this document is "*Certification Policy and Practice Statement for TSU Certificates issued by CA Time Stamping Units*" and the document will hereinafter be referred to, within the scope herein defined, as the "*Specific Policy and Practice Statement*" or abbreviated as "*SPPS*".

9. 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*.

10. 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*.

11. This *Certification Policy* is identified as follows:

Name: *TSU Certificate* Certification Policy

Policy Reference / OID[1]: 1.3.6.1.4.1.5734.3.18.1

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

Version: 1.1

Issue date: 19/06/2020

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

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

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

12. A *TSU Certificate* issued under this policy is a type of certificate issued for the provision of the Time Stamping Service.

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

1.3. PKI PARTICIPANTS

13. 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 or owners
4. Relying parties
5. Other participants

1.3.1. Certification Authority

14. 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 – FNMT-RCM ROOT CA Certificate

Subject	OU = FNMT-RCM ROOT CA, O = FNMT-RCM, C = ES
Issuer	OU = FNMT-RCM ROOT CA, O = FNMT-RCM, C = ES
Serial number (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07
Validity	Not before: 29 October 2008. Not after: 1 January 2030
Public key length	RSA 4.096 bytes
Signature algorithm	RSA – SHA256
Key identifier	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

b) Subordinate Certification Authorities: They issue the *TSU Certificates* subject of this *SPPS*. Those Authorities' certificates are identified by the following information:

Table 2 – Certificate of the subordinate CA Time Stamping Units

Subject	CN = CA Time Stamping Units, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES
Issuer	OU = FNMT-RCM ROOT CA, O = FNMT-RCM, C = ES
Serial number (hex)	2C:ED:1A:5E:02:80:5B:BC:5D:DF:8A:3A:EC:AA:98:5A
Validity	Not before: 28 November 2019. Not after: 28 November 2029.
Public key length	RSA 4096 bytes
Signature algorithm	RSA – SHA256
Key identifier	40 B9 55 04 A8 4F 7F 60 90 ED 11 95 25 C3 25 FA 5A F4 85 D5

1.3.2. Registration Authority

15. FNMT-RCM is the only *Registration Authority* involved in the process to issue this type of *Certificates*. It deals with identification and verification mainly for the purpose of ensuring that the *Certificate* is issued to the *Subscriber* controlling the domain name incorporated to the *Certificate*.

1.3.3. Subscribers

16. A *TSU Certificate* subscriber for the provision of the Time Stamping Service shall be the legal person to which this type of *Certificate* is issued and which enters into an agreement describing the terms of use of the *Certificate.*

1.3.4. Relying parties

17. Relying parties are natural or legal persons other than the Subscriber that receive and/or use *Certificates* issued by FNMT-RCM. The user entity, third parties relying on the *Certificates* and, generally, members of the *Electronic Community*, will be responsible for verifying and checking the status of *Certificates*, and *Certificates* may in no case be presumed to be valid in the absence of any such checks.

1.3.5. Other participants

18. *Time Stamping Authority*: The Time Stamping Authority is FNMT-RCM where it provides the electronic time stamp creation Trust Service under its relevant Specific Practice Statement, or, as appropriate, third parties to which this type of certificates are issued, as providers of their own time stamping service.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

19. *TSU Certificates* issued under this *Certification Policy* are used to create electronic time stamps.

20. *TSU Certificates* issued under this *Certification Policy* to FNMT-RCM itself are used to provide the qualified *Time Stamping Service*, in accordance with the Time Stamping Policy and Practice Statement, available at http://www.cert.fnmt.es/dpcs/.

21. The Certificate used by FNMT-RCM to create electronic Time Stamps through its Time Stamping Service may be downloaded from the website:

    https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

22. All *TSU Certificates* are *Qualified Certificates* as defined in 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 (eIDAS Regulation) and subject to the requirements established in European standards ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates", ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" and ETSI EN 319 422 "Time stamping protocol and electronic time-stamp profiles".

1.4.2. Prohibited certificate uses

23. As recommended in standards ETSI EN 319 421 and ETSI EN 319 422, those *TSU Certificates* include the privateKeyUsage extension restricting the use of the Private key by establishing an end date before the public key end date, thereby ensuring sufficient time for the renewal of the stamps issued by a TSU before its certificate expires.

24. If a *User entity* or a third party wishes to rely on these *Certificates* without accessing the *Status information and checking service* for *Certificates* issued under this *Certification Policy*, no cover will be obtained under these *Specific Certification Policies and 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*.

25. This type of *Certificates* may not be used for the following:

    - To sign or seal any other *Certificate*, except where previously authorised on a case-by-case basis.

- For personal or private uses, barring relations with Administrations where permitted.
- To sign or seal software or components.
- To provide services for no consideration or for valuable consideration, except where previously authorised on a case-by-case basis, including, but not limited to:
    - Providing *OCSP* services.
    - Generating *Revocation Lists*.
    - Providing notification services.
- Any use exceeding the purpose of this type of Certificates without the prior consent of FNMT-RCM.

1.5. POLICY ADMINISTRATION

1.5.1. Organisation administering the document

26. 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

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

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

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

Email: ceres@fnmt.es

Telephone: 902 181 696

28. To report security issues such as suspected key compromise, misuse of certificates, fraud or other matters, contact incidentes.ceres@fnmt.es.

1.5.3. Person determining CPS suitability for the policy

29. 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

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

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

31. 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:

- *Time Stamping Authority (TSA)*: A trust system managed by a *Trust Service Provider* responsible for issuing *Electronic time stamps*. From a legal viewpoint, it is a specific case of a *Trust Service Provider* and the provider is consequently referred to as a *Time Stamping Authority*.
- *TSU Certificate:* An Electronic seal certificate used for creating *Electronic time stamps* in providing the *Time Stamping Service*.
- *Certification Practice Statement (CPS):* A readily accessible statement made available to the public electronically and free of charge by FNMT-RCM. It is deemed to be a security document detailing, within the framework of the eIDAS Regulation, the obligations *Trust Service Providers* agree to fulfil in regard to management of *Signature creation and verification data* and *Electronic certificates*, the terms applicable to the application for, issuance, use and termination of the *Certificates*, organisational and technical security measures, profiles and information mechanisms as to the validity of *Certificates.*
- *Specific Policy and Practice Statement (SPPS):* A specific *CPS* which applies to the issuance of a given set of *Certificates* issued by FNMT-RCM under the specific terms contained in that Statement and to which the specific Policies defined therein apply.
- *Supervisory body:* body designated by a Member State responsible for supervisory tasks in the provision of trust services, in accordance with article 17 of the eIDAS Regulation. In Spain, that is currently the Ministry of Energy, Tourism and Digital Agenda.
- *Time Stamping Policy (specific)*: Document laying down the rules altogether indicating the applicability of a given type of *Time Stamping* to the *Electronic Community* and/or application class with common security requirements.
- *Time Stamping Service Provider*: Natural or legal person issuing *Electronic time stamps* pursuant to *Time Stamping* laws.
- *Subscriber's Representative*: individual authorised representative or person authorised by that representative, of the *Certificate Subscriber* organisation, to apply for and use that *Certificate*.
- *Time Stamping*: Inclusion of the date and time on an electronic document by means of indelible electronic procedures, based on the specifications *Request For Comments*:

3161 – *"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"*, allowing objective document dating.

- *Electronic time stamp:* Electronic data linking other electronic data to an exact moment in time so as to provide evidence that the latter data existed at that moment in time.
- *Time Stamping Service:* On-demand service provided by FNMT-RCM to interested parties so requesting, which, based on the specifications Request For Comments: RFC 3161 – "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" and ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", dates documents objectively so that a moment in time may be indubitably attributed to the existence of an electronic document. FNMT-RCM will only provide this service to certain entities and restrictions on use and the parties' representations and warranties will be described in the relevant specific service policies and practices.
- *Subscriber*: A public legal person, body or organisation entrusted with FNMT-RCM's activities as a *Trust Service Provider*, which subscribes to service terms and conditions. Under these *Certification Policies*, that service consists of issuing *TSU Certificates*. Reference is made to the *Subscriber* in the *Subject* field of the *Certificate*, and the *Subscriber* is the *Certificate* owner and is responsible for using and has exclusive control and decision-making capacity over the *Certificate.*
- *Coordinated Universal Time* (*UTC)*: The time in the reference time zone with respect to which all other zones are calculated worldwide. It is the successor to GMT as a time standard and, unlike GMT, is based on atomic references.
- *Time Stamping Unit (TSU):* Hardware and software altogether managed independently and which only has one stamp key active for the issuance of *Electronic time stamps* from time to time.

(Italicised terms are defined in this document or in the Trust Services Practices and Electronic Certification General Statement)

1.6.2. References

32. 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

RA: Registration Authority

ARL: Certification Authority Revocation List

CN: Common Name

CRL: *Certificate* Revocation List

DN: Distinguished Name

CPS: Certification Practice 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.

OCSP: Online Certificate Status Protocol

OID: Object IDentifier

PDS: Public Key Infrastructure (PKI) Disclosure Statement.

PKCS: Public Key Cryptography Standards developed by RSA Laboratories.

UTC: Coordinated Universal Time.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORY

33. 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:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

2.2. PUBLICATION OF CERTIFICATION INFORMATION

34. Information on the issuance of electronic *Certificates* subject of this *SPPS* includes the following:

- Certification practice and policy statements.
- *Certificate* Profiles.
- PKI disclosure statements (PDS).
- Terms and conditions of use of the *Certificates*, as a binding legal instrument.

35. Additionally, root and FNMT-RCM subordinate CA Certificates, and additional information, may be accessed and downloaded at:

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

2.3. TIME AND FREQUENCY OF PUBLICATION

36. FNMT-RCM will revise its certification policies and practices and update this *SPPS* on a yearly basis, following the guidelines established in paragraph "1.5.4. CPS approval procedure" of this *SPPS* document.

37. 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.

38. The CRL publication frequency is defined in section "4.9.7 CRL issuance frequency" of the *GCPS*.

2.4. ACCESS CONTROLS ON REPOSITORIES

39. 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

40. *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 *Certification Policies and Specific Certification Practices,* other than fields specifically providing otherwise, use the UTF8String encoding.

3.1.1. Types of names

41. 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 (section 7.1 hereof).

42. The Common Name field contains the name of the automatic process application or system for which the Certificate is issued.

3.1.2. Need for names to be meaningful

43. 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).

3.1.3. Anonymity or pseudonymity of subscribers

44. FNMT-RCM does not accept the use of pseudonyms under this *Certification Policy*.

3.1.4. Rules for interpreting various name forms

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

3.1.5. Uniqueness of names

46. The distinguished name (*DN*) assigned to the *Certificate Subscriber* within the *Trust Service Provider's* domain will be unique.

3.1.6. Recognition, authentication and role of trademarks

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

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Methods to prove possession of private key

48. FNMT-RCM neither generates nor stores the Key pair associated with the *TSU Certificates* issued under this Certification Policy to third parties, and does everything that is necessary during the *Certificate* Application procedure in order to make sure that the Subscriber is in possession of the Private Key associated with the Public Key to be certified.

49. The Keys FNMT-RCM needs to provide its *Time Stamping Service* will be generated by itself using its own infrastructure in a secure physical environment.

3.2.2. Authentication of organisation identity

50. FNMT-RCM verifies the legal existence and identity of the *Certificate* subscriber's organisation using different methods, depending on the type of organisation. Before entering into any institutional relationship with Subscribers, FNMT-RCM uses the website addresses and means referred to in these Specific Certification Practices and otherwise the *GCPS* to inform about the terms of service and representations, warranties and responsibilities of the parties involved in the issuance and use of the Certificates issued thereby in its capacity as Trust Service Provider.

51. The activities to check the *TSU Certificate Subscriber's* identity will be carried out by authorised personnel of FNMT-RCM's Registration Office, thereby guaranteeing the organisation's identity.

52. Where the *Subscriber* is a private entity, FNMT-RCM's RA will check that it is in existence, legally recognised, in operation at that time and formally registered, by carrying out a direct search using the Companies Register's service available for that purpose.

53. In the case of public entities, FNMT-RCM's RA shall check the above by directly searching the list of public sector entities kept by the Office of the General State Comptroller, which reports to the Ministry of Finance, or the relevant Official Gazette.

54. If the nature of the *Subscriber* differs from the above two cases, the legal existence and identity checks shall be carried out by directly searching the relevant official register.

55. FNMT-RCM checks that the name and tax identification number of the *Certificate* subscriber's organisation included in the application for the Certificate match the name and tax identification number formally entered in the registers searched as described in the preceding sections.

3.2.3. Authentication of individual applicant identity

56. The identity check is carried out by duly qualified and authorised FNMT-RCM personnel, observing at all times the necessary security measures, in a highly secure environment. The *TSU Certificate* Applicant shall be the Subscriber's representative or a person duly authorised by the same.

3.2.4. Non-verified Subscriber information

57. All information included in the electronic *Certificate* is verified by the *Registration Authority* and non-verified information is not therefore included in the "Subject" field of the certificates issued.

3.2.5. Validation of authority

58. The Registration Authority verifies that the Applicant for a *TSU Certificate* issued under this SPPS has been previously authorised by the Subscriber to submit that application. These checks shall always be carried out in any application for a new *TSU Certificate*.

59. FNMT-RCM's RA verifies that the *Applicant* has sufficient authority through the electronic signature used for the application form, as described in section 3.2.3 of this SPPS, and accepts the use of a qualified *Certificate* by the representative of a sole or joint director of the legal person subscriber or a qualified *Certificate* by *Public Servants*, where authority to issue the same has been established.

60. Where the above-mentioned form is signed using a qualified *Certificate* other than those mentioned in the preceding section, FNMT-RCM's RA checks the power of attorney of the application signatory by searching official registers (Companies Register, Official Gazettes, etc. depending on the nature of the power). If the search results do not provide evidence of sufficient authority, FNMT-RCM's RA contacts the *Subscriber* to obtain such evidence.

3.2.6. Criteria for interoperation (interaction)

61. There is no interaction with Certification Authorities external to FNMT-RCM.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

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

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

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

64. The authentication terms for a revocation request are set out in the section of this *SPPS* dealing with the *Certificate* revocation procedure (see section 4.9 hereof).

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

65. The Keys FNMT-RCM needs to provide the *Time Stamping Service* in its activity as a Trust Service Provider will be generated by itself using its own infrastructure in a secure physical environment and at least by two persons authorised to do so.

66. The key generation procedure, so-called "Key generation ceremony", is documented in the internal procedure "FNMT-RCM key life-cycle management as certification and stamping service provider".

4.1. CERTIFICATE APPLICATION

4.1.1. Who can submit a Certificate application

67. Applications for *TSU Certificates* issued under this policy may only be submitted by the Subscriber's authorised representative. Before the application is submitted, the certificate Subscriber shall have its representative perfect the agreement containing the certificate terms of use, representations and warranties.

4.1.2. Registration process and responsibilities

68. The Applicant will use a *TSU Certificate* application form to provide identification particulars, including, but not limited to, Tax Identification Number (NIF), first surname, and the subscriber's organisation Tax Identification Number (NIF).

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

70. FNMT-RCM will compile the evidence taken from the checks made, which will be stored in a repository.

71. In order for the *TSU Certificate* FNMT-RCM needs to provide its *Time Stamping Service* to be issued

a. FNMT-RCM's RA will verify that FNMT-RCM personnel responsible for dealing with *TSU Certificate* request and registration have the necessary authorisation and that this is documented in the internal procedure "FNMT-RCM key life-cycle management as certification and stamping service provider".

b. FNMT-RCM will compile the evidence taken from the checks made to be stored in a repository. The entire procedure will be documented as part of the "Key generation ceremony".

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

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing identification and authentication functions

73. FNMT-RCM will verify the accuracy of the data included in the application and, as the case may be, the *Representative's* authority making such checks and storing such evidence as may be appropriate.

4.2.2. Approval or rejection of certificate applications

74. The RA involved in processing issuance of *TSU Certificates* is always FNMT-RCM itself.

75. FNMT-RCM's RA carries out checks required to prove possession of the *Private key* and to authenticate the identity of the Organisation and of the person applying for the *Certificate*.

76. If any of those checks cannot be confirmed, FNMT-RCM will reject the *Certificate* applied for, reserving the right not to reveal the reasons for such rejection.

4.2.3. Time to process applications

77. The time to process applications for *TSU Certificates* is established at not more than 72 hours after FNMT-RCM's *Registration Office* receives all the documentation necessary to carry out the checks required prior to issuance of the *Certificate.*

4.3. CERTIFICATE ISSUANCE

4.3.1. CA actions during issuance

78. Upon FNMT-RCM's RA approving the *Certificate* application, the system carries out a number of checks, such as size of the *Public key* generated, and then issues the *Certificate* in accordance with the profile approved for each type of *Certificate*.

79. FNMT-RCM Certificates may only be issued by FNMT-RCM in its capacity as Trust Service Provider, and no other entity or organisation has authority to issue the same. The FNMT-RCM Certification Authority only accepts Certificate generation applications from authorised sources. The information contained in each application is fully protected against

alterations through Electronic Signature or Electronic Seal mechanisms. In any case, FNMT-RCM will use its best efforts:

- To 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) of the Subject assigned in the Certificate is unique within the scope of this SPPS.

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

1. Certificate data structure composition.

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

   The attribute CN contains the name of the automatic process application or system for which the Certificate is issued.

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

81. 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

82. Upon the *TSU Certificate* being issued, FNMT-RCM will inform the *Subscriber* that the *Certificate* is available.

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1. Conduct constituting certificate acceptance

83. During the *TSU Certificate* application process, the *Subscriber* accepts the terms of use and expresses its willingness to obtain the *Certificate*, and the requirements necessary for the *Certificate* to be generated.

4.4.2. Publication of the certificate by the CA

84. *Certificates* generated are stored in a secure repository of FNMT-RCM.

4.4.3. Notification of issuance to other entities

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

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber private key and certificate usage

86. FNMT-RCM neither generates nor stores the Private Keys associated with *TSU Certificates* issued to subscribers other than FNMT-RCM under this Certification Policy.

87. The Keys FNMT-RCM needs to provide its *Time Stamping Service* will be generated by itself using its own infrastructure, in certified cryptographic devices, in a secure physical environment and at least by two persons authorised to do so.

88. The TSU Private keys used by the FNMT-RCM Qualified Time Stamping Service are generated and guarded by a cryptographic device that meets the FIPS PUB 140-2 Level 3 security requirements, with algorithms and parameters suitable for the use of the key (Time stamp) and the expected duration, according to the recommendations of ETSI TS 119 312 or equivalent national regulations. The technical components necessary for the creation of Keys are designed so that a Key is only generated once, and so that a Private Key cannot be calculated from its Public Key.

89. The activity of creating Qualified Electronic Time Stamps is carried out within the cryptographic device, which provides Confidentiality to the Seal creation data of the Trust Services Provider. When the Seal creation data is outside the cryptographic device, the FNMT-RCM applies the appropriate technical and organizational measures to guarantee its Confidentiality.

90. Copy, save, or retrieve of the Seal creation data is performed under the exclusive control of authorized personnel, using at least dual control and in a secure environment.

91. A copy of the files and components necessary for the restoration of the security environment of the cryptographic device is kept, in case they have to be used, in security envelopes properly guarded inside a fireproof cabinet, which can only be obtained by authorized personnel.

4.5.2. Relying party public key and certificate usage

92. Third parties relying on *electronic seals* based on the *Private keys* associated with the *TSU Certificate* shall observe the representations and warranties defined in this *SPPS*.

4.6. CERTIFICATE RENEWAL

93. FNMT-RCM does not renew *Certificates* under these *Certification Policies* maintaining their *Public key* as defined in section “4.7 Certificate re-key” below.

4.7. CERTIFICATE RE-KEY

94. *TSU Certificate* re-key is always carried out issuing new keys, following the same process described for a new *Certificate* to be issued.

4.7.1. Circumstances for certificate re-key

95. FNMT-RCM stamping unit keys will be renewed in the following circumstances:

- Where the current keys will expire soon
- Where the certificate associated with the private key does not comply with the rules or laws in force or which are to enter into force
- Where the certificate associated with the private key is in conflict with commercial products or products which may stand in the way of the carrying on of the Stamping Authority's business
- Whenever the CGPSC considers it advisable from a technical or commercial viewpoint to create a new stamping unit with new features
- Due to obsolescence of the cryptographic algorithms to the extent that their security may be compromised before the associated certificate expiration date. In cases where this actually occurs, the Stamping Authority's Key Compromise Plan will additionally be activated, on the ground of algorithm compromise.
- Due to key compromise, in which case action will be taken in accordance with the provisions of the Stamping Authority's Key Compromise Plan.

4.7.2. Who may request re-key

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

4.7.3. Processing certificate re-keying requests

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

4.7.4. Notification of certificate re-key

98. 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

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

4.7.6. Publication of the re-keyed certificate

100. 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

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

4.8. CERTIFICATE MODIFICATION

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

4.9. CERTIFICATE REVOCATION AND SUSPENSION

103. *TSU Certificates* issued by FNMT-RCM will cease to be valid in the following cases:

a) Termination of the *Certificate* validity period.

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

In these two cases [a) and b)], the *Certificates* will cease to be valid forthwith upon the occurrence of these circumstances.

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

104. 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*.

105. 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/

with clear instructions so that they may report any issue relating to this type of *Certificates* in the event of *Private Key* compromise, improper use of *Certificates* or other types of fraud, compromise, misuse or misconduct.

106. The provisions of the "FNMT-RCM Stamping Unit Compromise Action Plan" will in addition be observed.

4.9.1. Circumstances for revocation

4.9.1.1 Reasons for revoking a subscriber certificate

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

108. A *TSU Certificate* shall be revoked in the following events:

a) Revocation request by authorised persons. This request shall in any case be based on:

- Loss of *Certificate* media.
- Third-party use of the *Private Key* associated with the *Certificate.*
- Breach or compromise of the *Private Key* associated with the *Certificate*.

b) Court or administrative ruling ordering revocation.

c) Termination or dissolution of the *Subscriber's* legal personality.

d) Inaccurate data supplied by the *Subscriber* to obtain the *Certificate*, or alteration of the data supplied to obtain the *Certificate* or change of the circumstances checked for the *Certificate* to be issued, to the extent that the *Certificate* is no longer current.

e) Breach of a material obligation provided for in this *Certification Practice Statement* by the *Subscriber*, or a *Registration Office* if, in the latter case, that may have affected the procedure to issue the *Certificate*.

f) Breach or compromise of the FNMT-RCM *Signature / Seal Creation Data* with which it signs / seals the *Certificates* it issues.

g) Breach of the requirements defined by the audit schemes to which the *Certification Authority* issuing the *Certificates* covered by this *SPPS* is subject, and specifically the requirements as to algorithms and key sizes, resulting in an unacceptable risk for the parties relying on these *Certificates*.

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

- Where the *Subscriber* requested revocation following the procedure established for this type of *Certificates.*
- Where it received notice of the revocation request or the underlying cause by means of court or administrative decision.

110. 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.

111. 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

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

4.9.2. Who can request revocation

113. Revocation of a *TSU Certificate* may only be requested by the *Subscriber* through its representative, or persons authorised thereby.

114. In addition, 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

115. A *TSU Certificate* revocation request may be made by 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.

116. 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.

117. 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.

118. 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. Therefore, the requestor shall submit to FNMT-RCM's *Registration Office* the duly completed and signed form created ad hoc. Once the *Registration Office* receives the documentation, it shall check and validate the information, and the requestor's authority to request revocation, and revocation of the *Certificate* shall be processed if everything is in order.

119. As soon as revocation is effective, the certificate *Subscriber* and the *Subscriber's Representative* requesting revocation will both be notified through the email address provided.

120. 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.

121. Revocation of a *TSU Certificate* issued to FNMT-RCM shall take place observing the "FNMT-RCM key life-cycle management as certification and stamping service provider" procedure.

4.9.4. Revocation request grace period

122. 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

123. FNMT-RCM processes revocation of the *TSU Certificate* immediately upon making the checks described above or, as the case may be, once the authenticity of a request made by means of a court or administrative decision has been checked.

4.9.6. Revocation checking requirement for relying parties

124. Third parties relying on and accepting the use of the *Certificates* issued by FNMT-RCM must check:

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

4.9.7. CRL issuance frequency

125. End-entity *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

126. *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

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

4.9.10. On-line revocation checking requirements

128. The revocation status of the *TSU Certificate* 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

129. Not defined.

4.9.12. Special requirements related to key compromise

130. There are no special requirements for revocation of certificates on the ground of key compromise, and the provisions for the other the grounds for revocation shall apply.

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

4.9.13. Circumstances for suspension

132. Certificate suspension is not supported.

4.9.14. Who can request suspension

133. Certificate suspension is not supported.

4.9.15. Procedure for suspension request

134. Certificate suspension is not supported.

4.9.16. Limits on suspension period

135. Certificate suspension is not supported.

4.10. CERTIFICATE STATUS SERVICES

136. The *Certificate status information and checking service* works as follows: the OCSP server receives the OCSP request made by an *OCSP Client* and checks the status of the *Certificates* included therein. If the request is valid, an OCSP response will be issued reporting on the then-current status of the *Certificates* included in the request. That response is signed / sealed with the FNMT-RCM *Signature / Seal Creation Data* thereby ensuring integrity and authenticity of the revocation status information supplied on the *Certificates* subject of the request.

137. The User entity will be responsible for acquiring an *OCSP Client* to operate with the OCSP server made available by FNMT-RCM.

138. FNMT-RCM operates and maintains its CRL and OCSP service maintenance capabilities with sufficient resources to provide a response time not in excess of ten seconds under normal operating conditions.

4.10.1. Operational characteristics

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

4.10.2. Service availability

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

141. If the service is unavailable due to maintenance operations, FNMT-RCM will notify this circumstance at http://www.ceres.fnmt.es, if possible at least forty-eight (48) hours in advance, and will endeavour to solve this within not more than twenty-four (24) hours.

4.10.3. Optional features

142. No stipulation.

4.11. END OF SUBSCRIPTION

143. Subscription will end when the *TSU Certificate* ceases to be valid, whether upon the validity period ending or due to revocation thereof.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policy and practices

144. FNMT-RCM will not recover the *Private keys* from the *Certificate Owners*.

4.12.2. Session key encapsulation and recovery policy and practices

145. No stipulation.

5. PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

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

5.1. PHYSICAL SECURITY CONTROLS

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

5.2. PROCEDURAL CONTROLS

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

5.3. PERSONNEL CONTROLS

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

5.4. AUDIT LOGGING PROCEDURES

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

5.5. RECORDS ARCHIVAL

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

5.6. CA KEY CHANGEOVER

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

5.7. COMPROMISE AND DISASTER RECOVERY

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

5.8. TRUST SERVICE PROVIDER TERMINATION

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

6. TECHNICAL SECURITY CONTROLS

155. 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

156. In connection with the *Key* information FNMT-RCM needs to carry out its activity as a *Time Stamping Trust Service Provider,* it will generate the *TSU Certificate* Keys as described in the "FNMT-RCM key life-cycle management as certification and stamping service provider" procedure. See the relevant section in the *GCPS*.

6.1.1.2 RA Key pair generation

157. No stipulation

6.1.1.3 Subscriber Key pair generation

158. As for *Key* generation for a *Subscriber* other than FNMT-RCM, Key generation and custody is guaranteed by the actual *Certificate Subscriber.*

6.1.2. Private key delivery to Subscriber

159. There is no *Private key* delivery to the *Owner*.

6.1.3. Public key delivery to Certificate issuer

160. The *Public key* generated with the *Private key* on the key generation and custody device is delivered to the Certification Authority sending a PKCS#10 certification request.

6.1.4. CA public key delivery to relying parties

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

6.1.5. Key sizes and algorithms used

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

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

- Root FNMT CA keys: 4096 bytes.
- Subordinate CA keys: 4096 bytes.
- *TSU Certificate* Keys: 3072 bytes.

6.1.6. Public key parameters generation and quality checking

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

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

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

166. The root CA *Certificate Key* usage purposes are to sign/seal subordinate CA *Certificates* and ARLs. The *Certificate* usage purposes of subordinate CAs issuing *TSU Certificates* are exclusively to sign/seal end-user *Certificates* (*TSU Certificates*) and CRLs.

167. The *TSU Certificate* is to be used for authentication and digital signature purposes only.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

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

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

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

6.3.2. Certificate operational periods and key pair usage periods

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

- Root CA *Certificate* and *Key* pair: see section "1.3.1. Certification Authority" of this SPPS.
- *Certificates* of subordinate CAs issuing *TSU Certificates* and their *Key pair*: see section "1.3.1. Certification Authority" of this SPPS.

- *TSU Certificates* and *Key* pair*:* maximum validity period of *Certificates* and their *Key* pair*:* not in excess of 5 years.

6.4. ACTIVATION DATA

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

6.5. COMPUTER SECURITY CONTROLS

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

6.6. LIFE CYCLE TECHNICAL CONTROLS

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

6.7. NETWORK SECURITY CONTROLS

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

6.8. TIME-STAMPING

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

6.9. OTHER ADDITIONAL CONTROLS

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

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

177. *TSU Certificates* conform to European standard ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" and ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles".

7.1.1. Version number

178. *TSU Certificates* conform to standard X.509 version 3.

7.1.2. Certificate extensions

179. The document describing the *TSU Certificate* profile, including all extensions, is posted at http://www.cert.fnmt.es/dpcs/.

7.1.3. Algorithm object identifiers

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

7.1.4. Name forms

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

7.1.5. Name constraints

182. The distinguished name (*DN*) assigned to the *Certificate Subscriber* in the *Trust Service Provider's* domain shall be unique and be composed as defined in the *Certificate* profile.

7.1.6. Certificate policy object identifier

183. The *TSU Certificate* policy object identifier (OID) is defined in section "1.2 Document name and identification" above.

7.1.7. Usage of policy constraints extension

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

7.1.8. Policy qualifiers syntax and semantics

185. 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 the wording that may be displayed on the *Certificate* user's screen during verification.

7.1.9. Processing semantics for the critical certificate policies extension

186. 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

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

7.2.2. CRL and CRL entry extensions

188. The CRL profile has the following structure:

Table 3 – CRL profile

Fields and extensions	Value
Version	V2
Signature algorithm	Sha256WithRSAEncryption.
CRL number	Incremental value
Issuer	Issuer DN
Issuance date	UTC issuance time.
Date of next upgrade	Issuance date + 24 hours (except for ARL, which is Issuance date + 1 year)
Distribution point	Distribution point URLs and CRL scope
ExpiredCertsOnCRL	NotBefore CA value
Revoked Certificates	Certificate revocation list, containing at least serial number and revocation date for each entry

7.3. OCSP PROFILE

7.3.1. Version number

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

7.3.2. OCSP extensions

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

191. 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".

192. In the case of qualified *Certificates,* the audit additionally ensures compliance with the requirements set in European standards ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates", ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" and ETSI EN 319 422 "Time stamping protocol and electronic time-stamp profiles".

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

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

8.2. QUALIFICATIONS OF ASSESSOR

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4. TOPICS COVERED BY ASSESSMENT

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

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6. COMMUNICATION OF RESULTS

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

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

9.1.1. Certificate issuance or renewal fees

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

9.1.2. Certificate access fees

202. No stipulation.

9.1.3. Revocation or status information access fees

203. FNMT-RCM offers OCSP certificate status information services free of charge.

9.1.4. Fees for other services

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

9.1.5. Refund policy

205. FNMT-RCM has a refund policy whereby a refund request may be made within the set withdrawal period, and accepts that this will result in automatic revocation of the certificate. The procedure is published at the FNMT-RCM website.

9.2. FINANCIAL RESPONSIBILITY

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

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.4. PRIVACY OF PERSONAL INFORMATION

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

9.5. INTELLECTUAL PROPERTY RIGHTS

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

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA representations and warranties

210. FNMT-RCM's representations and warranties as *Trust Service Provider* to the *Certificate Subscriber* and, as appropriate, users and relying parties, shall be mainly determined by the document containing the terms of use or the *Certificate* issuance agreement, and, secondarily, by this *Certification Policy and Practice Statement*.

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

212. Subject to the provisions of the law applicable to this type of *Certificates*, and the representations described in the relevant section of the *GCPS*, the *Trust Service Provider* agrees as follows:

213. Prior to *Certificate* issuance:

- To check the identity and personal circumstances of the *Applicant* for the *Certificate* and the *Subscriber* and/or the *Subscriber's Representative* and obtain a statement that the *Applicant* is authorised by the *Subscriber* to submit the application.

  The identification shall be made through qualified electronic signature *Certificates* admitted in FNMT-RCM processes.

- In processing registration, to check the *Subscriber's* legal personality data and the *Representative's* authority. These checks will all be carried out as provided for in the *Specific Certification Practices* referred to herein and based on FNMT-RCM's registration protocols and procedures.

  In checking the above, FNMT-RCM may involve third parties with powers to attest or public or private registers.

- To verify that all the information contained in the *Certificate* application matches the information supplied by the *Applicant*.

- To check that the *Applicant* is in possession of the *Private Key* associated with the *Public Key* incorporated to the *Certificate* to be issued.

- To make sure that the procedures followed allow *TSU Certificate Private Key* generation with an assurance that they are not copied or stored by FNMT-RCM.

- Information will be delivered to the *Subscriber, Representative* and *Applicant* in such a way that it remains *Confidential*.

- To provide the *Applicant, Subscriber, Representative* and other interested parties (http://www.ceres.fnmt.es) with the *Certification Practice Statement* and all relevant information required to carry out the life-cycle procedures of the *Certificates* subject of this *Certification Policy* and *Specific Certification Practices* in accordance with the applicable laws.

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

9.6.2. RA representations and warranties

215. RA activities will be exclusively carried out by FNMT-RCM through its Registration Area.

216. The RA, through FNMT-RCM's Registration Area, has the following obligations:

- Generally, to follow the procedures established by FNMT-RCM in the *Certification Policy and Practices* applicable to the performance of its *Certificate* management, issuance and revocation duties and not to alter that policy framework.
- In particular, to check the identity and any personal circumstances relevant to the intended purpose, of the *Certificate Applicants*, *Subscribers* and *Representatives*, using any means permitted by Law and in accordance with the general provisions of the *GCPS* and the specific provisions of this *SPPS*.
- To retain for fifteen (15) years all information and documentation relating to the application for and renewal or revocation of *Certificates* managed thereby.
- To receive and manage the *Certificate* issuance applications and agreements (pdf form) with the *Certificate Subscriber*.
- To dutifully check the grounds for revocation that could affect *Certificate* validity.

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

9.6.3. Subscriber representations and warranties

218. The exclusive use of associated *Private keys* must be ensured for *TSU Certificates*.

219. The *Applicant* for and *Subscriber* of *Certificates* issued under this *PPS* have the following obligations:

- Not to use the *Certificate* beyond the limits specified in this specific *Certification Policy and Practices*.
- Not to use the *Certificate* if the *Trust Service Provider* has discontinued its activity as *Certificate* Issuer issuing the certificate in question, particularly where the provider's *Seal Creation Data* may be compromised, and so it has been advised.
- To supply truthful information in the *Certificate* application and keep that information up to date, entering into the agreements through a duly authorised person.
- Not to apply on behalf of the *Subject* of the certificate for distinctive signs, names or intellectual property rights other than where it is the proprietor, licensee or has proof of consent to use the same.
- To use its best efforts to safely hold and store the *Signature / Seal Creation Data* or any other sensitive information such as *Keys*, *Certificate* activation codes, passwords, personal identification numbers, etc., and *Certificate* media, which in any case includes non-disclosure of any such data.
- To become acquainted with, accept and comply with the terms of use of the *Certificates* provided for in the terms and conditions of use and in the *Certification Practice Statement* and in particular, the restrictions on *Certificate* use.

- To become acquainted and comply with any amendments to the *Certification Practice Statement*.
- To request revocation of the relevant *Certificate*, using the procedure described herein, duly notifying FNMT-RCM of the circumstances for revocation or suspected loss of *Confidentiality*, disclosure, modification or unauthorised use of the associated *Private keys*.
- To check the information contained in the *Certificate* and notify FNMT-RCM of any error or inaccuracy.
- Before relying on the *Certificates,* to verify the advanced *Electronic signature* or the *Electronic seal* of the *Trust Service Provider* issuing the *Certificate.*
- To duly notify FNMT-RCM of any change to the information supplied on applying for the *Certificate*, consequently requesting revocation of the *Certificate* where appropriate.

220. The *Subscriber* will be responsible for properly using the *Certificate* and keeping it securely based on the purpose and function for which it is issued, and for informing FNMT-RCM of any change of status or information with respect to what is recorded in the *Certificate*, in order for the *Certificate* to be revoked and re-issued.

221. In addition, the *Subscriber* shall in any case be liable to FNMT-RCM, *User entities* and, as appropriate, third parties, for *Certificate* misuse or for misrepresentations or inaccuracies therein contained, or acts or omissions resulting in damages and losses for FNMT-RCM or third parties.

222. The *Subscriber* will be responsible and will therefore be required not to use the *Certificate* if the *Trust Service Provider* has discontinued its activity as *Certificate* Issuer during the course of which it issued the *Certificate* in question and no substitution shall have occurred as provided for by Law. In any case, the *Subscriber* shall not use the *Certificate* where the *Provider's Signature creation data* may be under threat and/or compromised, and the *Subscriber* has been so advised by the Provider or, as appropriate, learned of these circumstances.

223. To request revocation of the *TSU Certificate* issued under this policy where any information relating to the *Subscriber* is incorrect, inaccurate or has changed with respect to that contained in the *Certificate,* or does not relate to the owner and contact persons established in the relevant databases for management and administration of the email address included in the revoked *Certificate*.

224. Relations between FNMT-RCM and the *Subscriber* shall be mainly governed, insofar as how the *Certificates* are to be used, by the document containing the terms of use or, as the case may be, the *Certificate* issuance agreement, and with reference to the agreements, arrangements or document governing the relationship between FNMT-RCM and the relevant Public Entity.

9.6.4. Relying party representations and warranties

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

9.6.5. Representations and warranties of other participants

226. No stipulation.

9.7. DISCLAIMER OF WARRANTIES

227. No stipulation.

9.8. LIMITATIONS OF LIABILITY

228. In relation to *TSU Certificates* belonging to third-party Time Stamping Authorities, it is noted that FNMT-RCM shall have no liability and will provide no warranty whatsoever with respect to any aspect of the Time Stamping Service offered by the entities owning such *Certificates* and Time Stamping Authorities. In particular, the exemption from liability shall extend to management of any aspects relating to the information systems used by those *Certificates* or Authorities, and the validity of the time sources, or synchronicity, used in the service.

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

9.9. INDEMNITIES

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

9.10. TERM AND TERMINATION

9.10.1. Term

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

9.10.2. Termination

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

9.10.3. Effect of termination and survival

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

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12. AMENDMENTS

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

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

9.12.3. Circumstances under which OID must be changed

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

9.13. DISPUTE RESOLUTION PROVISIONS

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

9.14. GOVERNING LAW

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

9.15. COMPLIANCE WITH APPLICABLE LAW

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

9.16. MISCELLANEOUS PROVISIONS

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

9.17. OTHER PROVISIONS

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