Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERTIFICATION PRACTICES AND POLICIES STATEMENT ON WEBSITE AUTHENTICATION CERTIFICATES

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

Version	Date	Description
1.0	5/03/2019	Certification Practices and Policies Statement on website authentication certificates, under the hierarchy of the FNMT Root AC Raíz Servidores Seguros
1.1	30/05/2019	Update domain validation methods according to CA / Browser Forum Baseline Requeriments.
1.2	12/12/2019	General review and improvement update
1.3	16/06/2020	General review in accordance to Mozilla Root Store Policy v.2.7., Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.7.0. and EV Guidelines v.1.7.2
1.4	31/08/2020	Reduction of the validity period of OV SSL certificates to 12 months. Improvements in several sections
1.5	01/10/2020	Incorporation of the EKU "Client Authentication" to the website authentication certificates.
1.6	26/11/2020	Incorporation of information from the DGPC for greater clarity. General review in accordance with Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.7.3. and EV Guidelines v.1.7.4
1.7	18/02/2021	Inclusion of the URL where the list of Incorporating Agencies or Registration Agencies was published. Compliance review to Law 6/2020. Reference to the maximum period between revisions of the Information Security Policy is documented
1.8	28/04/2021	General review and Mozilla Policy review v2.7.1. - Information is included in relation to the methods to communicate a compromise of keys.

Reference: DPC/DPCASW_0108/SGPSC/2021

Document classified as: *Public*

Table of contents

Index of tables

1. INTRODUCTION

1. The Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (*The National Currency and Stamp Factory – Spanish Royal Mint*), hereinafter the FNMT-RCM, bearer of tax identification number Q2826004-J, is a public business corporation regulated by Act 40/2015 (1 October) on the Public Sector Legal Regime. As a public body, the FNMT-RCM has a separate public legal personality, its own assets and treasury, and is managed independently in the terms of the said law.

2. It is attached to the Ministry of Finance, which, through the Under-Secretary's Office for Finance, will be responsible for strategic management and control of the FNMT-RCM's efficiency in the terms of the aforementioned Act 40/2015.

3. The FNMT-RCM has been engaged in its industrial activities, backed by the State, for a long period of time. Since Article 81 of Act 66/1997 (30 December) on Tax, Administrative and Labour Matters and its amendments came into force, the FNMT-RCM's authorised services have been expanded and it has achieved recognition in the provision of trust services.

4. Similarly, the FNMT-RCM, through the CERES (Spanish Certification) Department, has been given the status of Qualified Trust Service Provider, 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, through an independent entity and within the framework of a certification scheme, in compliance with the European standard ETSI EN 319 401 "General Policy Requirements for Trust Service Providers".

1.1. PURPOSE

5. The purpose of this document is to provide public information on the conditions and features of the trust services offered to users of *Website authentication certificates* provided by the FNMT-RCM as a *Trust Service Provider,* specifically the obligations the FNMT-RCM must fulfil in connection with:

   - the management of the said *Certificates,* the conditions applicable to the application, issuance, use and cancellation of the validity thereof, and
   - the provision of the *Certificate* validity checking service, as well as the conditions applicable to the use of the service and guarantees offered.

1.2. DOCUMENT NAME AND IDENTIFICATION

6. This document is called "*Statement of Practices and Policies for Certification of Web Site Authentication Certificate*s", and will hereafter be cited in this document and with the scope described therein as *"Certification Practice or Policy Statement*" or by its acronym "*CPS*".

   Version: 1.8

   Issue date: 28/04/2021

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

7. A *Website authentication certificate* is a type of certificate aimed at ensuring that the domain name of the website to which Internet users are connected is authentic, by using protocols that provide data encryption and authentication between applications and servers (TLS/SSL).

8. Within the scope of this CPS, the FNMT-RCM issues the following types of *Website authentication certificates,* the description of which is found in the section "1.6.1 Definitions" of this document:

- *Website authentication certificates* which are considered to have the condition of qualified[1]:

Type of *Certificate*	Policy Reference/OID [2]
Electronic Venue certificate EV	1.3.6.1.4.1.5734.3.16.1.1
EV Certificate	1.3.6.1.4.1.5734.3.16.1.2
EV SAN Certificate:	1.3.6.1.4.1.5734.3.16.1.3

This qualified certificates have the following associated policies:

Extended Validation Certificate Policy (EVCP) OID: 0.4.0.2042.1.4

Extended Validation (EV) guidelines certificate policy OID: 2.23.140.1.1

QCP-w: certificate policy for European Union (EU) qualified website authentication certificates OID: 0.4.0.194112.1.4

- *Website authentication certificates,* under Organisation Validation Policies (OV):

Type of *Certificate*	Reference / Policy OID
OV Certificate	1.3.6.1.4.1.5734.3.16.2.1
OV Wildcard Certificate	1.3.6.1.4.1.5734.3.16.2.2
OV SAN Certificate	1.3.6.1.4.1.5734.3.16.2.3

These OV certificates have the following associated policies:

[1]Issued in accordance with requirements established under Annex IV of 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.

[2] *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 certain type of *Certificate* to the *Electronic Community* and/or Application class with the same security requirements.

Organizational Validation Certificate Policy (OVCP) OID: 0.4.0.2042.1.7

Organization identity Validation OID: 2.23.140.1.2.2

1.3. PKI PARTICIPANTS

9. The following parties are involved in the management and use of the *Trust Services* described in this *Policies and Practices Statement*:

1. Certification Authority
2. Registration Authority
3. *Certificate* subscribers or holders
4. Trusting parties
5. Other participants

1.3.1. Certification Authority

10. The FNMT-RCM is the *Certification Authority* that issues the electronic Certificates included in the present CPS. *Certification Authorities* are as follows:

a) Root Certification Authority. This authority exclusively issues *Certificates* for Subordinate Certification Authorities. This CA's root certificate is identified by the following information:

Table 1 - AC RAIZ FNMT-RCM SERVIDORES SEGUROS Certificate

AC RAIZ FNMT-RCM SERVIDORES SEGUROS Certificate	
Subject	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Issuer	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Serial number (hex)	62:F6:32:6C:E5:C4:E3:68:5C:1B:62:DD:9C:2E:9D:95
Validity	Not before: 20 December 2018 Not after: 20 December 2043
Public key length	ECC P-384 bits
Signature algorithm	Sha384ECDSA

AC RAIZ FNMT-RCM SERVIDORES SEGUROS Certificate	
Key identifier	01 B9 2F EF BF 11 86 60 F2 4F D0 41 6E AB 73 1F E7 D2 6E 49

b) Subordinate Certification Authorities: Issue the end entity *Certificates* covered by this *CPS.* The certificates of these Authorities are identified by the following information:

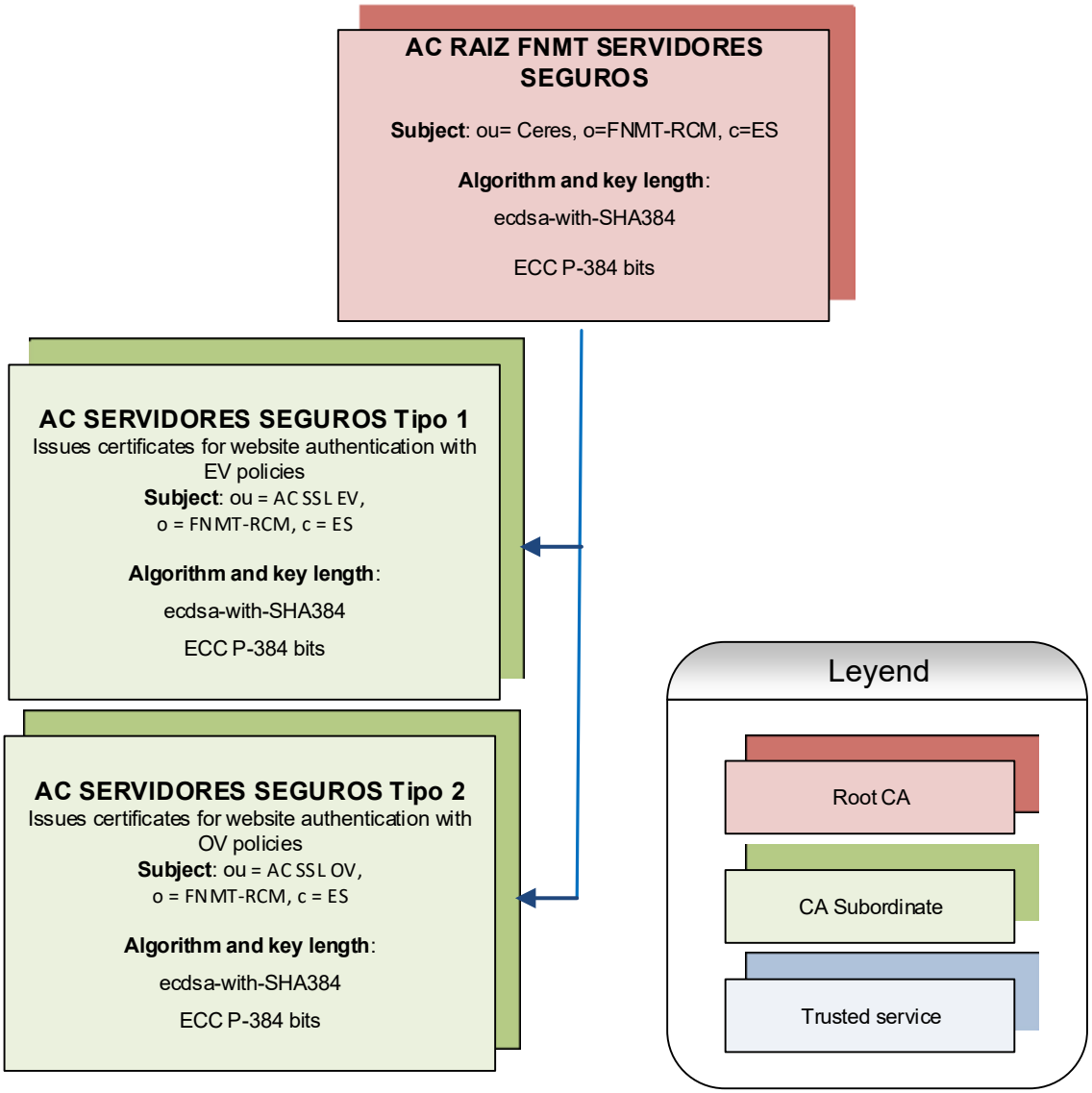
Table 2 - Subordinate AC SERVIDORES SEGUROS TIPO1 Certificate (EV certificates)

Subordinate AC SERVIDORES SEGUROS TIPO1 Certificate (EV certificates)	
Subject	CN = AC SERVIDORES SEGUROS TIPO1, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Issuer	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Serial number (hex)	50:89:86:CD:B4:17:0E:FE:5C:1B:6B:D5:C8:24:EB:5B
Validity	Not before: 20 December 2018 Not after: 20 December 2033
Public key length	ECC P-384 bits
Signature algorithm	Sha384ECDSA
Key identifier	8C 42 32 40 F9 79 3F 6B 13 C1 75 C6 5D EE 86 22 44 39 6F 77

Table 3 - Subordinate AC SERVIDORES SEGUROS TIPO2 Certificate (OV certificates)

Subordinate AC SERVIDORES SEGUROS TIPO2 Certificate (OV certificates)	
Subject	CN = AC SERVIDORES SEGUROS TIPO2, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES

Subordinate AC SERVIDORES SEGUROS TIPO2 Certificate (OV certificates)	
Issuer	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Serial number (hex)	13:8E:6B:BE:DF:20:F5:94:5C:1B:6C:F6:29:B4:2F:4A
Validity	Not before: 20 December 2018 Not after: 20 December 2033
Public key length	ECC P-384 bits
Signature algorithm	Sha384ECDSA
Key identifier	C5 F2 05 4E F4 37 72 E4 EA 4F 02 57 03 FD 86 96 05 AE 50 8F



1.3.2. Registration Authority

11. The FNMT-RCM is the only *Registry Authority* that acts in the process of issuing these types of *Certificates.* It performs identification and verification tasks, with the main purpose of ensuring that the *Certificate* is issued to the *Subscriber* with control of the domain name that is incorporated into the *Certificate.* None of the verifications on identity or domain validation will be delegated.

1.3.3. Subscribers

12. *Subscribers* are the legal entities to whom this type of *Certificate* is issued and who are legally bound by an agreement that describes the terms of use of the *Certificate.*

13. For *Electronic Venue certificates,* the *Subscriber* would be the public administration, group, public body or legal public entity that has control of the domain name of the *Electronic Venue*.

1.3.4. Relying parties

14. Trusting parties are those Internet users who establish connections to websites through the use of TLS/SSL protocols that incorporate these types of *Certificates* and decide to trust them.

1.3.5. Other participants

15. Not stipulated.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate certificate Uses

16. Certificates issued under this *Certification Policy* are considered valid as a means by which the person who visits a website is guaranteed of the fact that exists an authentic and legitimate entity, the FNMT-RCM, that supports the existence of said website.

17. Additionally, *Electronic Venue certificates* are a subset of *Website authentication certificates*, which are issued as identification systems for *Electronic Venues* and that guarantees secure communication with it, under the terms defined in Act 40/2015 of 1 October, of Legal Regime of the Public Sector and in Act 18/2011, of 5 July, governing the use of information and the communication technologies in the Department of Justice.

18. All *Website authentication certificates* with Extended Validation (EV) policies issued under this *Certification Policy* are considered to be *Qualified Certificates* in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 2014 relating to electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 (eIDAS Regulation) and in accordance with the requirements established in the European standards ETSI EN 319 411-2 “Requirements for trust service providers issuing EU certificates” and ETSI EN 319 412-4 “Certificate profile for web site certificates”.

1.4.2. Prohibited certificate uses

19. If a *User Entity* or a third party wishes to rely on these *Certificates* without accessing the *Information and consultation service* regarding the validity status of the certificates issued under this *Certification Policy,* coverage of these *Particular Certification Practices and Policies* shall not apply, and there will be no grounds to make any type of claim or take legal action against the FNMT-RCM for damages, loss, or conflicts arising from the use of or reliance on a *Certificate.*

20. The FNMT-RCM prohibits the use of the *Certificates* issued under this CPS for the illegal interception or decryption of encrypted communications (MITM), deep packet inspection (DPI), etc.

21. These types of *Certificates* may not be used to:

- Sign a different *Certificate*, unless specific prior authorisation is obtained.
- Sign software or components.
- Generate *time stamps* for *electronic dating* procedures.
- Provide services for free or for consideration, unless specific prior authorisation is obtained, that include but are not limited to:
    - Provision of *OCSP* services.
    - Generation of *Revocation Lists*.
    - Provision of 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, bearer of tax identification number Q2826004-J, is the *Certification Authority* issuing the certificates to which this *Statement of Certification Practices and Policies* applies*, and is* responsible for its maintenance

1.5.2. Contact person

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

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

Directorate of Information Systems - CERES Department

C/ Jorge Juan, 106

28071 – MADRID

E-mail: ceres@fnmt.es

Telephone: 902 181 696

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

1.5.3. Person determining General Statement suitability for the policy

25. The FNMT-RCM's Management has capacity to specify, revise and approve the review and maintenance procedures both for the Specific Certification Practices and the relevant Certification Policy.

1.5.4. General Statement approval procedure

26. The FNMT-RCM manages its certification services and issues certificates in accordance with the latest version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", established by the CA/Browser forum, which can be viewed at the following address: https://cabforum.org/baseline-requirements-documents.

27. The FNMT-RCM reviews its certification policies and practices and annually update this Statement of Certificates Policy in order to keep it in line with the latest version of those requirements, increasing the version number and adding a dated change log entry, even if no other changes were made to the document.

28. Updates to CP or CPS documents are made available by publishing new versions at https://https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

29. For the purposes of this *CPS*, when the terms begin with a capital letter and are in italics, the definitions in the following section shall be taken into account:

- *CAA records:* Certification Authority Authorisation (CAA) Domain Name System (DNS) resource record. This allows a DNS domain name holder to specify the Certification Authorities (CA) authorised to issue certificates for that domain. The publication of the CAA resource records allows a domain name holder to implement additional controls in order to reduce the risk of unauthorised issuance of a *Website Authentication Certificate* for their domain name.
- *Certificate Transparency (CT):* this is an open framework for the supervision of *Website authentication certificates*, so that when one of these *Certificates* is issued, it is published in CT registry, thus enabling domain owners to monitor the issuance of them for their domains and detect erroneously issued *Certificates.*
- *Certification Practices Statement (DPC):* Declaration made available to the public in an easily accessible form, electronically and free of charge by the FNMT-RCM. This is considered a security document in which, within the eIDAS framework, the obligations that *Trust Service Providers* undertake to comply with in relation to the management of the *Signature creation and verification data* and the *Electronic certificates* are detailed, as well as conditions applicable to the application, issuance, use and termination of the validity of the Certificates, the technical and organizational security measures, the profiles and the information mechanisms on the validity of the *Certificates.*
- *Certificate Problem Report (CPR)*: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
- *Electronic Venue: Website* available to citizens through telecommunication networks, whose ownership corresponds to a Public Administration, or to one or several public bodies or entities of Public Law in the exercise of the powers granted to them.

- *Electronic Venue certificate EV:* EV certificate that identifies an Electronic Venue, guaranteeing secure communication with it under the terms defined in Act 40/2015 of 1 October, on the Legal Regime of the Public Sector.
- *EV Certificate: Website authentication certificate* that contains validated information of its *Holder* in accordance with the procedure of exhaustive validation as outlined in the requirements of the "Guide for the issuance and management of Extended Validation Certificates" established by the CA/Browser Forum entity, and that can be found at the following address https://cabforum.org/extended-validation/
- *EV SAN Certificate: EV certificate* that incorporates a set of domains independent of each other.
- *OV Certificate: Certificate of web site authentication* issued according to the Organisation Validation Policy (OVCP), reasonably guaranteeing to users of Internet browsers that the owner of the website that they are accessing matches with the Organisation identified by the *OV Certificate.* This *Certificate* complies with the requirements of the European standard ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- *OV SAN Certificate: OV certificate* that incorporates a set of domains independent from each other.
- *OV Wildcard Certificate: OV Certificate* that incorporates a set of unlimited subdomains, starting from the third level, with a unique *Website Authentication Certificate.*
- *Representative of the Registry Office (only applicable for Electronic Venue certificates):* Individual appointed by the representative of the Public Administration, public body or public legal entity, under whose responsibility the tasks assigned to the *Registry Office* are performed with the obligations and responsibilities assigned in these *Special Certification Policies and Practices*.
- *Representative of the Subscriber*: the legal person, or person authorised by the Subscriber, of the *Subscriber* organisation of the *Website Authentication Certificate,* for the request and use of said *Certificate.*
- *Certification Practices and Policies Statement (CPS):* Private CPS that applies to the issuance of a specific set of *Certificates* issued by the FNMT-RCM under the particular conditions included in said Declaration, and that are subject the particular Policies defined therein.
- *Supervisory body*: body designated by a Member State as being responsible for supervisory functions in the provision of trust services, in accordance with the provisions contained in Article 17 of the eIDAS Regulation. In Spain, this is currently the Ministry of Energy, Tourism and Digital Affairs.
- *Staff serving the Public Administration:* Officials, staff, statutory staff and authorised personnel, at the service of the Public Administration, group, public body or legal public entity.
- *Subscriber:* Legal entity, group or public body that is the recipient of the activities of the FNMT-RCM as Trust Service Provider, which subscribes to the terms and conditions of the service. Under the current *Certification Policies*, this service consists of the issuance of *Website authentication certificates.* The *Subscriber* is referenced in the *Subject* field of the

Certificate and is the owner and responsible for its use, and maintains exclusive control and the decision-making capacity over it.

- *Website Authentication Certificate:* This is a Certificate that allows for the authentication of a website and links it with the individual or legal entity to whom the *Certificate* has been issued.

1.6.2. Acronyms

30. For the purposes of the provisions contained in this CPS, the following acronyms shall be applicable, with meaning is in accordance with the 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

DPC: Certification Practices 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.

EV: Extended validation

ETSI: European Telecommunications Standards Institute

HSM: Hardware security module This is a security device that generates and protects cryptographic keys.

OCSP: Online Certificate Status Protocol

OID: Object Identifier

OV: Organisational validation

PDS: PKI disclosure statement

PIN: Personal identification number

PKCS: Public key cryptography standards

TLS/SSL: Transport Layer Security/Secure Socket Layer protocol TSP:

UTC: Coordinated Universal Time

2. PUBLICATION AND REPOSITORIES RESPONSIBILITIES

2.1. REPOSITORY

31. The FNMT-RCM, as a *Trust Service Provider*, has a repository of public information available 24x7, every day of the year, with the characteristics indicated in the following sections and with access using the address:

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

2.2. PUBLICATION OF INFORMATION

32. The information regarding the issuance of electronic *Certificates* subject to this CPS which is accessible through https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion, includes the following information:

- Certification Practices and Policies Statement
- *Certificate profiles* and *Revocation lists*.
- PKI Informative statements (PDS).
- The terms and conditions of use of the *Certificates*, as a legally binding instrument.

33. In addition, it is possible to download of the Root Certificates and subordinate CAs of the FNMT-RCM, as well as additional information, at the following address:

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

2.3. TIME OF FREQUENCY OF PUBLICATION

34. The FNMT-RCM will review its certification policies and practices and annually review and update the present *CPS*, following the guidelines established in section "1.5.4. DPC Approval Procedure" of this *CPS* document.

35. Any amendment to the *Certification Policies and Practices* will be immediately published in the URL where they may be accessed.

2.4. ACCESS CONTROLS ON REPOSITORIES

36. All the above-mentioned repositories are freely accessible for information consultation and, if applicable, download purposes. Moreover, the FNMT-RCM has put in place controls to prevent unauthorised persons from adding, altering or deleting information included in its repositories and to protect the authenticity and integrity of the information.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

37. The coding of *Certificates* follows the RFC 5280 standard "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All the fields defined in the profile of the *Certificates* profile in the *Special Certification Policies and Practices* use UTF8String coding, except in fields that specifically express otherwise.

38. In addition, for EV Certificates, the FNMT-RCM shall meet the requirements of Section 9.2 of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

3.1.1. Types of names

39. End-user electronic *Certificates* as covered in this *CPS* contain a distinguished name (DN) in the Subject Name field, composed in accordance with the information relating to the Certificate profile (section 7.1 of this document). FNMT-RCM complies with X.500, RFC 5280 and CA/Browser Forum requirements for naming.

40. The Common Name field specifies the holder of the *Certificate.*

3.1.2. Need for names to be meaningful

41. All distinguished names (DN) of the Subject Name field are denotative. The description of the attributes associated with the *Certificate Subscriber* is provided in human-readable form (see section 7.1.4 Name format of this document).

42. The Subject Distinguished Name fields are also subject to the requirements of Section 9.2 of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates. Wildcard Certificates are not allowed for EV Certificates

3.1.3. Anonymity or pseudonymity of subscribers

43. The FNMT - RCM does not permit the use of pseudonyms under this *Certification Policy.*

3.1.4. Rules used to interpreting various name forms

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

3.1.5. Uniqueness of names

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

3.1.6. Recognition, authentication, and role of trademark

46. Subscribers may not request Certificates with any content that infringes the intellectual property rights of a third party.

47. The FNMT–RCM makes no commitment whatsoever regarding the use of distinctive signs, whether registered or otherwise, in the issuance of *Certificates. Certificates* including distinctive signs may only be requested when the *Holder* owns the right of use or is authorised to use the sign. The FNMT–RCM is not obligated to previously verify the ownership or registration of the distinctive signs before issuing the *Certificates,* even if they are entered in public registers.

3.2. INITIAL IDENTITY VALIDATION

48. The FNMT-RCM performs the validation process on the information included in the *Website authentication certificate* in accordance with the "Baseline Requirements for the Issuance and

Management of Publicly-Trusted Certificates", established by the CA/Browser forum, which may be viewed at the following address: https://cabforum.org/baseline-requirements-documents.

49. In addition, the FNMT-RCM, before issuing an *EV Certificate, SAN EV Certificate* or *Electronic Venue certificate*, ensures that all information included in these types of *Certificates* relative to the *Subscriber,* is in accordance with (and is verified according to) the requirements defined by the entity CA/Browser forum in its "guide for the issuance and management of Extended Validation Certificates", (section 11) and that can be consulted at the address https://cabforum.org/extended-validation/

50. The FNMT-RCM records all confirmations performed in this section for both internal an independent audits processes.

3.2.1. Methods to prove possession of the private key

51. The FNMT-RCM receives a C*ertificate* request, in PKCS #10 format, digitally signed by the *Private key* generated by the *Subscriber's Representative* in its environment. Prior to proceeding with the issuance of the *Certificate*, the FNMT-RCM verifies this signature, guaranteeing that the *Public key* included in the request corresponds to the *Private key* generated by the *Party responsible for the certificate.*

3.2.2. Authentication of Organization and domain identity

3.2.2.1 Identity

52. The FNMT-RCM verifies the legal existence, address and identity of the Certificate's subscribing organisation through different methods, depending on the type of organisation (private, public or business).

53. In cases where the *Subscriber* is a private entity, its identity and address, which is legally recognised, active at that moment, and formally registered, will be verified by direct consultation by the RA of the FNMT-RCM using service that the Mercantile Registry provides for this purpose.

54. For cases of public entities, such verifications will be carried out by direct consultation of the RA of the FNMT-RCM of the inventory of public sector entities contained at the General Intervention Board of the State Administration, under the Ministry of Finance, or in the corresponding Official Gazette.

55. If the nature of the *Subscriber* is different from the two previous examples, verifications related to its legal capacity, identity and address will be made by direct consultation with the corresponding official registry.

56. The list of Incorporating Agencies or Registration Agencies is published in the Legal Repository on FNMT-RCM's website (https://www.cert.fnmt.es/registro/utilidades).

57. The FNMT-RCM does not issue *Website authentication certificates* for *Subscribers* who are individuals.

58. The FNMT-RCM verifies that the name, address and tax identification number of the subscribing organisation of the *Certificate* included in the request matches with the name,

address and tax identification number formally registered in the records consulted as described in the previous sections.

59. If an *Applicant* requests an *Extended Validation* (EV), the FNMT-RCM shall conform to the CAB Forum's respective EV Guidelines.

3.2.2.2 DBA/Tradename

60. If the Subject Identity information includes a DBA or tradename, the FNMT-RCM will use the same verification procedures and criteria as in Section 3.2.2.1 to verify the Applicant's right to use the DBA/tradename.

61. For *EV Certificate* requests extensive identity verification as defined in the CAB Forum's EV Guidelines section 11.3 are required.

3.2.2.3 Verification of country

62. The countryName is verified using any method in Section 3.2.2.1

3.2.2.4 Validation of Domain Authorization or Control

63. In order validate *Website authentication certificate* domains, the FNMT-RCM uses one of the following methods described in the CA/Browser Forum's Baseline Requirements document: "3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact", "3.2.2.4.4 Constructed Email to Domain Contact" or "3.2.2.4.7 DNS Change ". For each method FNMT-RCM will follow a documented process and maintain records noting the method(s) used for each issuance. The rest of methods described in the CA/Browser Forum's Baseline Requirements document are not used.

- 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact:

  Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value must be sent to an email address identified as a Domain Contact.

  Each email may confirm control of multiple Authorization Domain Names.

  FNMT-RCM may send the email identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email.

  The Random Value shall be unique in each email.

  FNMT-RCM may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

  The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

- 3.2.2.4.4 Constructed Email to Domain Contact:

  Confirm the Applicant's control over the requested FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster',

or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value shall be unique in each email.

The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipients shall remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

- 3.2.2.4.7 DNS Change:

  Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value in a DNS TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

  FNMT-RCM shall provide a Random Value unique to the certificate request and shall not use the Random Value after (i) 30 days.

64. The FNMT-RCM confirms that the *Subscriber's Representative* has control over the full domain names, or FQDN (Fully Qualified Domain Name) that are incorporated into the *Website authentication certificates* that it issues. For such purpose, the FNMT-RCM consults the identity of the *Subscriber's Representativ*e and the name of the aforementioned FQDN, through the program that registers the applications of these Certificates. Next, it is verified that the request originates from the contact with control over said domain (according to the methods defined in the previous section), or has received authorisation from it. Additionally, it is verified that the request for the *Certificate* has been made subsequent to its registration in the corresponding registries.

65. Furthermore, before issuing a *Website authentication certificate*, it is verified that the domain to be included in the *Certificate* is public (i.e. it is not an internal domain) and public records are consulted to verify that it is not a high risk domain (for example, the Google registry created for this purpose, or the Safe Browsing site status).

3.2.2.5 Authentication for an IP address

66. *Certificates* that identify IP addresses are not issued under these policies.

3.2.2.6 Wildcard domain validation

67. The entire Domain Namespace in wildcard *Certificates* must be rightfully controlled by the *Subscriber*

68. If a wildcard *Certificate* would fall within the label immediately to the left of a registry-controlled or public suffix, the FNMT-RCM will refuse issuance unless the applicant proves

its rightful control of the entire Domain Namespace. To perform such verification, the AR will use the public list of suffixes available in https://publicsuffix.org/ which will be retrieved regularly.

3.2.2.7 Data source accuracy

69. Prior to using any data source as a Reliable Data Source, the RA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

3.2.2.8 CAA records

70. FNMT-RCM checks to confirm that there is a CAA Record for each domain name that it includes in any Website authentication certificate, in accordance with the procedure established under the terms of RFC 8659 and following the processing instructions set forth in RFC 8659 for any record may be found. In the event that such CAA Record exists, no Certificate will be issued unless it is determined that the Certificate request is consistent with the applicable CAA resource record group. The domain identifier recognized for the certification authority of the FNMT is "fnmt.es".

3.2.3. Authentication of the individual identity

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

3.2.4. Non-verified subscriber information

72. All the information incorporated into the electronic *Certificate* is verified by the *Registration Authority,* therefore, it does not include unverified information in the “Subject” field of the certificates issued.

3.2.5. Validation of Authority

73. The RA of the FNMT-RCM verifies that the *Applicant* has been granted sufficient representation capacity through the electronic signature of the application form, as described in section 3.2.3 of this *CPS*, accepting the use of a qualified *Certificate* of sole or joint administrator representative of the subscribing legal person or a qualified *Certificate* of *Personnel at the service of the Public Administration*, for whose issuance the capacity of representation has been accredited.

74. When the aforementioned form is signed by a qualified *Certificate* different from those mentioned in the previous section, the RA of the FNMT-RCM is able to verify the power of representation of the signatory of the request by consulting official records (Commercial Registry, Official Gazettes, etc., depending on the nature of the representation). In the event that the results of these consultations do not provide sufficient evidence of representation, the RA of the FNMT-RCM will contact the *Subscriber* to collect such evidence.

75. For Extended Validation requests, FNMT-RCM shall verify this authority using the procedures described in the EV Guidelines. (sections 11.8 y 11.11)

3.2.6. Criteria for interoperation or certification

76. There are no interoperational relationships with Certification Authorities external to FNMT-RCM.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and authentication for routine re-key

77. *Certificate* Subscribers should request any corresponding re-key prior to the expiration of their period of validity. The authentication conditions for renewal requests are covered in the section of this *CPS* corresponding to *Certificate* renewal processes (see section 4.6 of this document).

3.3.2. Identification and authentication for re-key after revocation

78. The FNMTRCM do not renew Certificates that have been revoked. The process for the re-key of a *Certificate* after its revocation is the same as that which is followed in the initial issuance of said *Certificate.*

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

79. The conditions for authentication of a revocation request are covered in the section of this *CPS* corresponding to the *Certificate* revocation process (see section 4.9 of this document).

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who can submit a certificate application

80. Only *Subscriber* representatives *or* individual duly authorized to request *Certificates* on behalf of the applicant, who have demonstrated control over the name of the domain to be included in the *Certificate* are able to request *Website authentication certificates.* The aforementioned control over the domain name will be verified by the FNMT-RCM as described in section "3.2 Initial Validation of Identity" contained in this *CPS.*

81. In addition, for EV Certificates, the FNMT-RCM shall meet the requirements of Section 11 of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates

4.1.2. Enrolment process and responsibilities

82. The FNMT-RCM require each Applicant to submit a Certificate request and application information prior to issuing a Certificate. The FNMT-RCM authenticates all communication from an Applicant and protects communication from modification.

83. The enrollment process includes:

- Submitting a complete Certificate application and agreeing to the applicable subscription agreement. By executing the subscription agreement, *Subscribers* warrant that all of the information contained in the Certificate request is correct.
- Generating a key pair,
- Delivering the public key of the key pair to the CA and
- Paying any applicable fees.

84. The RA of the FNMT-RCM performs the verification of the identity of the subscribing Organisation and of the *Subscriber Representative*, and verifies that the application for the Certificate is both correct and duly authorised, in accordance with the requirements contained in section "3.2 Initial Validation of identity" of this document. The FNMT-RCM may carry out additional verification on the validation processes described in the aforementioned section.

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

86. Section 9.6 "Representation and warranties" of this document establishes the responsibilities of the parties involved in this process.

4.2. CERTIFICATION APPLICATION PROCESSING

4.2.1. Performing identification and authentication functions

87. The *Subscriber Representative* sends a form to the RA of the FNMT-RCM, electronically signed with a qualified electronic *Certificate*, which contains all of the information to be included in the *Website authentication certificate.* Based on this information, the RA of the FNMT-RCM performs all of the checks described in the section "3.2 Initial Validation of Identity," of this *CPS.*

88. The FNMT-RCM will verify the accuracy of the data included in the application and, if applicable, the capacity of the *Representative* by means of the corresponding verifications and by providing the appropriate evidence.

89. The electronic signature generated to sign contract will be verified by the FNMT-RCM.

90. Reuse of previous validation data or documentation obtained from a source specified under section 3.2 may be used no more than 12 months after such data or documentation was validated.

4.2.2. Approval or rejection of certificate applications

91. The RA that acts in the process of issuing *Website authentication certificates* is shall always be that of the FNMT-RCM itself, and, therefore, the validation of domains will never be delegated to any other AR.

92. The RA of the FNMT-RM performs all checks related to proof of possession of the *Private key* by the *Subscriber Representative*, authentication of the identity of the Organisation and of the person requesting the *Certificate,* as well as the validation of the domain, as described in the section "3.2 Initial Validation of Identity" of this *CPS*, which will then result in the approval or rejection of the request in question.

93. The FNMT-RCM maintains an internal database of all revoked *Certificates* and all requests for *Certificates* that were previously rejected due to suspected phishing or other forms of fraudulent use. This information is then taken into account to identify subsequent requests for suspicious certificates before proceeding with the approval of the issuance thereof.

94. In addition, the FNMT-RCM also drafts, maintains, and implements documented procedures that identify and require additional verification activity for applications for high-risk Certificates prior to approval of the issuance of a *Certificate*, to the extent that is reasonably necessary to ensure that such requests are properly verified, in accordance with these requirements.

95. If it is not possible confirm any of these validations, the FNMT-RCM will deny the Certificate request, reserving the right not to disclose the reasons for such denial. The *Subscriber Representative* whose request has been denied may appear to present their request in the future.

96. Both OV and EV certificate requests shall be processed by FNMT-RCM Trusted Role personnel. The approval system for issuing *EV Certificates* requires the action of at least two Trusted Role personnel belonging to the RA of the FNMT-RCM, one with the role of validating and the other with the role for approving the requests.

97. In addition, the FNMT-RCM checks to confirm that there is a CAA Record for each domain name that it includes in any *Website authentication certificate,* in accordance with the procedure established under the terms of RFC 8659 and following the processing instructions set forth in RFC 8659 for any record may be found. In the event that such *CAA Record* exists, no Certificate will be issued unless it is determined that the Certificate request is consistent with the applicable CAA resource record group. The domain identifier recognized for the certification authority of the FNMT is "fnmt.es".

4.2.3. Time to process certificate applications

98. The amount of time spent processing a Certificate application depends to a large extent on the *Subscriber Representative* providing all necessary information and documentation in the manner specified in the procedures approved by the FNMT-RCM for this purpose. However, this Entity will make all necessary efforts so that the validation process resulting in the acceptance or denial of the request does not exceed a total of two (2) business days.

99. This time period may occasionally be exceeded for reasons beyond the control of the FNMT-RCM. In these cases, the best option is to contact the *Subscriber Representative* who made the request and inquire as to the causes of such delays.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA actions during certificate issuance

100. Once the application for the *Certificate* has been approved by the RA of the FNMT-RCM's, the system then performs pre-issuance linting to check compliance with RFC 5280 and CA/Browser Forum (BRs and EVGs). Only where no errors are found, FNMT-RCM proceeds to issue the *Certificate* according to the profile approved for each corresponding type of *Certificate.*

101. Likewise, the FNMT-RCM periodically monitors possible deviations in the certificates issued.

102. The processes related to the issuance of electronic *Certificates* guarantee that all the accounts that interact with them include multi-factor authentication.

4.3.2. Notification of certificate issuance

103. Once the *Certificate* is issued, the FNMT-RCM sends a notice to the e-mail address recorded on the request form signed by the *Subscriber Representative*, stating that the *Certificate* is available for download.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct constituting certificate acceptance

104. In the process of requesting the *Certificate,* the *Subscriber Representative* accepts the conditions of use and expresses their willingness to obtain the *Certificate* as mandatory requirements for its generation.

4.4.2. Publication of certificate by the CA

105. All *Certificates* drafted are stored in a safe FNMT-RCM storage facility.

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

106. Prior to the issuance of *Website authentication certificates* a “pre-certificate” is sent for the records of the *Certificate Transparency* service used by those providers with whom the FNMT-RCM maintains an agreement for this purpose.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber's private key and certificate usage

107. The FNMT-RCM does not generate or store any *Private Keys* associated with the *Certificates* that are issued under this *Certification Policy.* The condition of custody and control of the *Certificate* keys correspond to the *Head of Registry Operations* in the case of the *Electronic Venue certificate* and, for the rest of the *Website authentication certificates*, to the *Subscriber's Representative*s that have demonstrated that they hold control over the name of the domain to be included in the *Certificate.* Therefore, the *Private Key* associated with the *Public Key* will be kept under the responsibility of said custodian, who will act as representative of the Entity with rights to ownership, management and administration of the corresponding electronic address.

4.5.2. Relaying party public key and certificate usage.

108. Users and relying parties must use software that is compatible with applicable standards for the use of electronic *Certificates* (X.509, IETF, RFCs ...). In the event that any connection to the website requires additional insurance measures, these measures must be obtained by the user entities.

109. Third parties that rely on the establishment of a secure connection guaranteed by a *Website authentication certificate* must make sure that such connection was created during the period of validity of the *Certificate*, that said *Certificate* is being used for the purpose for which it was issued, in accordance with this *CPS,* as well as to verify that the *Certificate* is active at that time, by checking its revocation status in the form and conditions that are expressed in section "4.10 Information services for the status of certificates" of the present document.

4.6. CERTIFICATE RENEWAL

110. The renewal of a *Certificate* involves the issuance of a new Certificate without changing any information regarding the *Signatory, Public Key* or any other information that appears in it.

111. Under these *Certification Policies*, the FNMT-RCM does not renew *Certificates* keeping the same *Public key,* but, rather, the renewal of Certificates is performed by renewing the *Cryptographic keys*, as defined in section of this document titled "4.7 Renewal with regeneration of the certificate keys".

4.6.1. Circumstances for certificate renewal

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

4.6.2. Who may request renewal

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

4.6.3. Processing certificate renewal requests

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

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

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

4.6.6. Publication of the renewal certificate by the CA

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

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

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

4.7. CERTIFICATE RE-KEYS

119. Renewal of *Website authentication certificates* with key regeneration is always done by issuing new public and private keys, following the same process as described for the issuance of a new *Certificate.*

4.7.1. Circumstances for certificate re-key

120. *Certificates* shall be re-keyed in the following events:

- Where the current keys will expire soon, upon request by the renewal requestor.
- Due to key compromise or any other circumstance set out in section "*4.9 Certificate revocation and suspension"* of this *CPS.*

4.7.2. Who may request re-key

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

4.7.3. Processing certificate re-keying requests

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

4.7.4. Notification of certificate re-key

123. 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

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

4.7.6. Publication of the re-keyed certificate

125. 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

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

4.8. CERTIFICATE MODIFICATION

127. No amendments may be made to *Certificates* issued. Consequently, a new *Certificate* must be issued in order for changes to be made.

4.8.1. Circumstance for certificate modification

128. The modification is not stipulated.

4.8.2. Who may request certificate modification

129. The modification is not stipulated.

4.8.3. Processing certificate modification requests

130. The modification is not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

131. The modification is not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

132. The modification is not stipulated.

4.8.6. Publication of the modified certificate by the CA

133. The modification is not stipulated.

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

134. The modification is not stipulated.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

135. *Website Authentication certificate*s issued by the FNMT-RCM will cease to be valid in the following cases:

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

b) Discontinuance of the FNMT-RCM's activities as a *Trust Service Provider* unless, upon express previous consent of the *Subscriber*, the *Certificates* issued by the FNMT-RCM are transferred to a different *Trust Service Provider.*

In these two cases [a) and b)], the loss of the *Certificate*'s effectiveness will occur as soon as the circumstances arise.

c) Revocation of the *Certificate* due to any of the causes stipulated in this document.

136. The revocation of the *Certificate*, i.e. the termination of its validity, will take effect as of the date on which the FNMT-RCM is in possession of certain knowledge of any of the determining events, and such events are recorded by its *Certificate status information and consultation service.*

137. The FNMT-RCM makes trusting third parties, software suppliers, and third parties available to Subscribers by means of communication through the electronic headquarters of the FNMT-RCM https://www.sede.fnmt.gob.es/ with clear instructions, to allow them to report any matter related to this type of Certificates, regarding a supposed compromise of a Private Key, improper use of the Certificates or other types of fraud, compromise, misuse or inappropriate behavior.

138. The FNMT-RCM, as a Trust Service Provider, reserves the right not to issue or to revoke these type of *Certificates* in the event that *Subscribers* with control of the domain name of the website included in the *Certificate* do not make proper use thereof, violating industrial or intellectual property rights of third parties with regard to applications, websites or *Electronic Venues* that are to be protected with such *Certificates*, or in cases where their use is deceptive or confusing as to the ownership of such applications, websites or *Electronic Venues* and, Therefore, of its contents. In particular, such reservation of rights may be carried out by the FNMT-RCM in cases where the use of such *Certificates* is contrary to the following principles:

a) The safeguarding of public order, criminal investigation, public security and national defence.

b) The protection of public health or of individuals who have the status of consumers or users, even when acting as investors.

c) Respect for the dignity of the individual and the principle of non-discrimination based on race, sex, religion, opinion, nationality, disability or any other personal or social circumstance, and

d) Protection of children and youth

139. The FNMT-RCM will be kept harmless by the holders of or those responsible for any equipment, applications, websites or *Electronic Venues* that fail to comply with the provisions

of this section and that are related to the *Certificate*, and shall be considered as exempt from any claim or complaint arising from the improper use of such Certificates.

4.9.1. Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

140. In addition to these provisions, the following will be causes for revocation of a *Website authentication certificate:*

a) The request for revocation by authorised individuals. The following may give rise to this request:

- Loss of support of the *Certificate.*
- Use of the *Private Key* associated with the *Certificate* by a third party.
- Any violation or endangerment of the details of the *Private Key* associated with the *Certificate.*
- The non-acceptance of new conditions that may imply the issuance of new *Certification Practices Statement*, during the period of one month subsequent to its publication.

b) Judicial or administrative resolution ordering such request.

c) Termination, deletion, or closure of the website identified by the *Certificate.*

d) Extinction or dissolution fo the legal personality of the *Subscriber.*

e) Termination of the form of representation of the *Certificate Subscriber* representative.

f) Total or partial supervening lack of capacity of the *Subscriber's* representative.

g) Inaccuracies in the data provided by the *Subscriber's Representative* in order to obtain the *Certificate*, or alteration of any of the data provided to obtain the *Certificate,* or modification of the verified information relating to the issuance of the *Certificate,* so that it is no longer in accordance with reality.

h) Violation of a subst*antial obligation of this Certification Practices Statement by the Subscriber, the Subscriber Representative* or a *Registry Office*, in the event that, in the latter case, this might have potentially affected the procedure for issuing the *Certificate.*

i) Use the Certificate with the purpose of generating doubt for users regarding the origin of the products or services offered, indicating that their origin is different from the one actually offered. To do this, the criteria will be followed related to activity in violation of the rules on consumers and users, trade, competition and advertising.

j) Termination of the contract entered into between the *Subscriber* or their *Representative*, and the FNMT-RCM, or any non-payment for services rendered.

k) Violation or endangerment of the secrecy of the FNMT-RCM *Signature/Seal Creation Data*, with which it signs/seals the *Certificates* it issues.

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

141. Under no circumstances may it be understood that the FNMT-RCM assumes any obligation whatsoever to verify the factors mentioned in letters c) to i) of this section.

142. The FNMT-RCM shall only be responsible for consequences arising from failure to revoke a Certificate in the following cases:

- That the revocation has been requested by the *Subscriber's Representative* following the procedure established for these types of *Certificates*.
- That the revocation should have been performed due to the termination of the contract entered into with the *Subscriber.*
- That the revocation request or the cause that gives rise to it has been notified by judicial or administrative resolution.
- That these facts are convincingly demonstrated in causes c) to g) of this section, prior to identification of the revocation *Applicant.*

143. Any acts constituting a crime, or the lack thereof, of which FNMT-RCM has no knowledge of, committed involving the data contained in a *Certificate, any* inaccuracies regarding the data, or lack of diligence in its communication to the FNMT-RCM, shall result the FNMT-RCM being exempted from any liability.

144. All requests for revocation of end entity *Certificates*, are processed within a maximum period of 24 hours from receipt of the application.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

145. The Issuing CA shall revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

a) The Subordinate CA requests revocation in writing;

b) The Subordinate CA notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization;

c) The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of sections 6.1.5 and sections 6.1.6,

d) The Issuing CA obtains evidence that the Certificate was misused;

e) The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the Baseline Requirements, EV Guidelines, Minimum Requirements for Code Signing or this CPS;

f) The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

g) The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

h) The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or

i) Revocation is required by the Issuing CA's CPS.

4.9.2. Who can request revocation

146. *CAs, RAs* and *Subscribers* may initiate revocation.

147. Revocation of a *Website authentication certificate* may only be requested by the person with powers of representation of the *Subscriber* to whom the *Certificate* has been issued.

148. In the case of an *Electronic Venue certificate*, the FNMT-RCM shall accept the authority and capacity of the *Applicant* when this corresponds to the *Registry Operations Manager.* In addition, the following shall be considered qualified to request the revocation of said *Certificate:*

- The governing body, body or public entity *Subscriber* of the *Certificate,* or the individual delegated for such purpose.
- The *Registry Office*, through its representative designated for this purpose, either by the Administration, public entity or body, *Subscriber* of the *Certificate* to be revoked, in such event that it detects that any of the data included in the *Certificate*
    - is incorrect, or that there is a discrepancy between it and that pertaining to the *Certificate,* or
    - the individual acting as holder of the *Certificate* does not correspond with the responsible party or that designated for the management and administration of the e-mail address contained in the *Certificate* object of the revocation.

  always within the framework of the terms and conditions applicable to the revocation of these types of *Certificates.*

149. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate

150. Nevertheless, the FNMT-RCM may officially revoke *Website authentication certificates* in cases included in this *Certification Practices and Policies Statement.*

4.9.3. Procedure for revocation request

151. There is a 24/7 service available at phone number 902 200 616, to which applications for the revocation of *Website authentication certificates* can be addressed. The communication will be recorded and registered, to be used as support and guarantee of the acceptance of the requested revocation request.

152. Additionally, it is possible to submit the revocation request to the Registration Area of the FNMT-RCM, adhering to the following procedure:

1. *Subscriber* request

   The *Subscriber's Representative* will submit the revocation request form the FNMT-RCM, completed and electronically signed with any of the *Certificates* admitted for the application and by the electronic channels enabled by this Entity.

2. Processing of the request by the FNMT-RCM

   The registrar of the FNMT-RCM will receive the revocation contract, and will carry out the same checks regarding the identity and capacity of the *Subscriber's Representative* as would be performed for cases of issuance requests and, if approved, will process the revocation of the *Certificate.*

153. For cases of *Electronic Venue certificate EV,* the FNMT-RCM will always accept the actions and report made by the *Registry Office* designated to request the revocation of these types of Certificates by the Administration, whose procedure is as follows:

1. *Applicant's* identity contained at a *Registry Office.*

   In order to revoke the *Certificate*, the *Applicant* with sufficient capacity and competence, will appear before a *Registry Office* designated for that purpose by the body, group or entity *Subscriber* of the *Certificate* to be revoked, or, otherwise, it will be performed directly by the Registry Operations Manager.

2. Appearance and documentation.

   The *Applicant* will provide all data required, and which demonstrate:

   - their personal identity
   - its status as Personnel at the service of the *Public Administration, Subscriber* of the *Certificate* and holder of the e-mail address through which the *Website* covered by the *Certificate* or status as *Registry Operations Manager* is accessed.
   - their status as individual designated for the management of the e-mail address through which the *Website c*overed by *Certificate* to be revoked is accessed, or of personnel assigned to the *Registry Office* designated by the body or entity Subscriber of the Certificate to revoke or this purpose.

   In the event that the above points are not demonstrated, the *Registry Office* will not proceed with the request for revocation of the *Certificate.*

3. Submission of the request for revocation to the FNMT-RCM and its processing.

   In the absence of evident causes of lack of authorisation of the *Registry Operations Manager* and/or once the identity of the *Applicant* has been confirmed, validity of the conditions demanded of the latter and the revocation request document subscribed, the *Registry Office* will proceed to validate the data and send it FNMT-RCM for the effective revocation of the *Certificate.* The personal data and its treatment shall be subject to specific legislation governing this matter.

Said submission will only occur in the event that the *Registry Office* has the power to act as such on behalf of the body, group or Public Administration entity acting as *Subscriber* of the *Certificate,* and if the latter is the holder of the e-mail address through which the Website covered by the *Certificate* is accessed.

This transmission of information to the FNMT-RCM will be carried out through secure communications established for such purpose between the *Registry Office* and the FNMT-RCM.

154. Once the FNMT-RCM has proceeded with the revocation of the *Website authentication certificate*, the corresponding *List of Revoked Certificates* will be published in the secure *Directory,* containing the serial number of the revoked *Certificate,* in addition to the date, time, and cause of revocation. The *Subscriber's Representative* will receive notification of the change of the validity status of the *Certificate* through the e-mail address included in the request.

4.9.4. Revocation request grace period

155. There is no grace period associated with this process, since revocation is immediate upon verified receipt of the revocation application.

4.9.5. Time within which CA must process the revocation request

156. Within 24 hours after receiving a *CPR*, the CA will investigate the facts and circumstances related to the *CPR* and provide a preliminary report to both the Subscriber and the entity who filed the *CPR*.

157. After reviewing the facts and circumstances, the CA will work with the Subscriber and any entity reporting the *CPR* or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date which the CA will revoke the Certificate. The period from receipt of the *CPR* or revocation-related notice to published revocation will not exceed the timeframe set forth in section 4.9.1.1.

158. The date selected by the CA will consider the following criteria:

1. The nature of the alleged problem(scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of CPRs received about a particular Certificate or Subscriber;
4. The entity making the complaint; and
5. Relevant legislation.

159. The FNMT – RCM proceeds with the immediate revocation of the Website authentication certificate at the time of performing the checks described above or, where applicable, once the veracity of the request resulting from judicial or administrative resolution has been verified.

4.9.6. Revocation checking requirement for relying parties

160. Third parties that place their trust in and accept the use of *Certificates* issued by the FNMT-RCM are obligated to verify:

- the *Advanced Electronic Signature or Advanced Electronic Stamp of the Trust Service Provider* that issues the *Certificate;*
- that the Certificate is still valid and active;
- the status of *Certificates* included in the *Certification Chain*.

4.9.7. CRL issuance frequency

161. *Revocation lists (CRLs)* for end-entity Certificates are issued at least every 12 hours, or whenever there is a revocation; they have a 24-hour validity period. *CRLs* of *Authority* certificates are issued at least every six months, or whenever there is a revocation by a *Certification Authority*; they have a 6-month validity period.

4.9.8. Maximum latency for CRLs

162. *Revocation lists* are published at the time they are generated, so the latency period between CRL generation and publication is zero.

4.9.9. On-line revocation/Status checking availability

163. Information on the status of certificates will be available online 24 hours a day, seven days a week. In the event of system failure, the business continuity plan will be implemented to resolve the incident as soon as possible.

4.9.10. Online revocation checking requirements

164. On-line verification of the revocation status of the *Website Authentication Certificate* may be performed through the *Certificate status information service,* which is provided through OCSP as described in section 4.10 of this document. Persons wishing to use this service must:

- verify the address contained in the *Certificate*'s AIA (Authority Information Access) extension.
- check that the OCSP response is signed/stamped.

4.9.11. Other forms of revocation advertisements available

165. Not defined.

4.9.12. Special requirements related to key compromise

166. The FNMT-RCM will use reasonable means of communication to inform *Subscribers* that their private key may have been compromised. Whenever a compromise of the key is confirmed, the FNMT-RCM will revoke the affected *Certificates* as described in section 4.9

of this *DGPC* and, where appropriate, the *Specific Certification Policy Statements* dependent on it.

167. The communication to the FNMT-RCM about the compromise of a private key through the contact information indicated in section 1.5.2, must in any case include proof of said compromise and indicate in the subject of the email "Key compromise". To demonstrate this, the parties may use the following methods:

• Submission of the private key compromised or a challenge response signed by the private key and verifiable by the public key, as well as the public key itself.

• Providing references to vulnerabilities and / or sources of security incidents from which the key compromise is verifiable.

168. The FNMT-RCM may accept other types of evidences that adequately prove the compromise of keys.

4.9.13. Circumstances for suspension

169. The suspension of certificates is not provided.

4.9.14. Who can request suspension

170. The suspension of certificates is not provided.

4.9.15. Procedure for suspension request

171. The suspension of certificates is not provided.

4.9.16. Limits on the suspension period

172. The suspension of certificates is not provided.

4.10. CERTIFICATE STATUS SERVICES

173. The *Certification status information and consultation service* works as follows: the OCSP server receives an OCSP request made by an OCSP Client and checks the validity status of the Certificates included in it. If the request is valid, an OCSP response will be issued on the status at that moment of the *Certificates* included in the request. This OCSP response is signed/stamped using the *Signature/Stamp Creation Data* of the FNMT-RCM, thus guaranteeing the integrity and authenticity of the information supplied on the revocation status of Certificates consulted.

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

175. The FNMT-RCM operates and maintains the maintenance capabilities of its CRLs and OCSP service with sufficient resources to provide a maximum response time of ten seconds under normal operating conditions.

176. Access to these information services:

a. Certificate Revocation Lists:

AC RAIZ FNMT-RCM "SERVIDORES SEGUROS":

http://www.cert.fnmt.es/crls/ARLSERVIDORESSEGUROS.crl

Subordinate CA "SERVIDORES SEGUROS TIPO 1" (*EV Certificates)*:

http://www.cert.fnmt.es/crlsservseguros/CRLT1.crl

Subordinate CA "SERVIDORES SEGUROS TIPO 2" (*OV Certificates)*:

http://www.cert.fnmt.es/crlsservseguros/CRLT2.crl

b. Certificate status verification service (OCSP):

AC RAIZ FNMT-RCM "SERVIDORES SEGUROS".

http://ocspfnmtssr.cert.fnmt.es/ocspssr/OcspResponder

Subordinate CA "SERVIDORES SEGUROS TIPO 1" (*EV Certificates)*.

http://ocspfnmtss1.cert.fnmt.es/ocspss1/OcspResponder

Subordinate CA "SERVIDORES SEGUROS TIPO 2" (*OV Certificates)*. Access:

http://ocspfnmtss2.cert.fnmt.es/ocspss2/OcspResponder

4.10.1. Operational characteristics

177. The *Certification status information and consultation service* works as follows: the FNMT-RCM's OCSP server receives an OCSP request made by an OCSP Client and checks the status of the *Certificates* included in it. If the request is valid, an OCSP response will be issued on the status at that moment of the *Certificates* included in the request. This OCSP response is signed using the *Signature/Seal Creation Data* associated with the OCSP server specific to each CA, thus guaranteeing the integrity and authenticity of the information supplied on the revocation status of *Certificates* consulted.

178. The OCSP supports the GET Method for retrieval of validation information for *Certificates* issued, in accordance with RFC 6960 and the requirements established by CA/Browser Forum (https://cabforum.org/baseline-requirements-documents/). FNMT-RCM OCSP responses have validity interval of 8 hours and the information provided via OCSP updates constantly by acceding directly to the database of each AC. The OCSP responder that receives a request for status of a certificate which has not been issued, shall not respond with a "good" status.

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

4.10.2. Service availability

180. The FNMT-RCM guarantees access to this service, 24/7, for all Certificate users, holders and trusting parties, securely, quickly and free of charge.

181. In the event that the service is unavailable as a result of maintenance operations, the FNMT-RCM will post a notification stating this at http://www.ceres.fnmt.es at least forty-eight (48)

hours in advance, if possible, and will attempt to resolve the issue within twenty-four (24) hours.

4.10.3. Optional features

182. No stipulation.

4.11. END OF SUBSCRIPTION

183. The subscription will at the time of expiration of the validity of the *Website authentication certificate*, either as a result of expiration of the validity period or by revocation thereof

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policies and practices

184. Since the FNMT-RCM does not generate the P*rivate keys* of the *Website authentication certificates,* it does not maintain them, and is not able to recover them.

4.12.2. Session key encapsulation and recovery policies and practices

185. Not stipulated.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

186. The FNMT-RCM, as a *Trust Service Provider*, maintains all critical assets used in trusted services in secure zones, physically, logically and functionally protected.

187. Likewise, it has segmented networks for the administration of its systems and for the operation of trusted services. The systems used for the administration of the implementation of the security policy are not used for other purposes. Production systems for trusted services are separated from the systems used in development and testing.

188. The FNMT-RCM has physical, logical, personnel and operating control procedures in place to guarantee the necessary security in the management of the systems under its control and involved in the provision of trust services. The FNMT-RCM will also log all events related to its services that could be relevant so as to check that all the internal procedures required to perform the activities comply with applicable legislation in order to be able to determine the causes of anomalies detected.

189. All the controls implemented by the FNMT-RCM as a *Trust Service Provider* are listed below, using as work models the document *RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* and the European standards *ETSI* EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 411 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates" and ETSI EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", excluding confidential and secret controls that are not disclosed for security reasons.

5.1. PHYSICAL SECURITY CONTROLS

190. The FNMT-RCM guarantees that it complies with legislation applicable to all aspects of physical security, which are described in this chapter.

191. Security perimeters are in place around critical or sensitive activities, including security barriers and appropriate entry controls equipped with security control mechanisms to reduce the risk of unauthorised entry or damage to IT resources.

5.1.1. Site location and construction

192. The building in which the *Trust Service Provider*'s infrastructure is located is equipped with access control security measures so that the activities and services may be carried out with sufficient guarantees of *Confidentiality* and security.

5.1.1.1 Data Processing Centre location

193. The *Trust Service Provider*'s data centre has been built taking into account the following physical requirements:

- In an apartment, away from exhaust ducts to avoid any damage in the event of a fire in the stories above.
- Absence of windows providing access from outside the building.
- Intrusion detectors and surveillance cameras in the restricted access areas during time periods in which the systems are unattended.
- Access control based on a card and a password.
- Fire protection and prevention systems: fire detectors, extinguishers, fire-fighting training for operators, etc.
- Transparent partitions separating zones and allowing rooms to be observed from access corridors so as to detect intrusion or illicit activities inside the Data Centre.
- All cabling will be protected against damage, electromagnetic interception and interception of data transfers and telephone calls.

194. The facilities employed to provide trust services are located in a high-security environment, separate from the Entity's other activities.

5.1.2. Physical access

5.1.2.1 Physical security perimeter

195. Once the security areas in which the FNMT-RCM's activities as a *Trust Service Provider* are conducted have been defined, suitable physical access control measures are put in place, without forgetting that the FNMT-RCM's premises have an advanced physical perimeter security system comprising various rings equipped with the appropriate technical and human resources, protection and surveillance by State security forces and corps, and specialised security services.

196. In addition to the access controls, there are various internal control mechanisms in rooms and facilities, such as access control using card readers, video surveillance cameras, intrusion detectors, fire detectors, etc., as well as human resources controlling access outside and inside the premises.

5.1.2.2 Physical entry controls

197. There is a comprehensive system of physical controls for people entering and leaving the premises, in a number of security rings.

198. All the *Trust Service Provider*'s critical operations are carried out inside physically secure premises with various levels of security controlling access to critical machines and applications.

199. These systems will be physically separate from other FNMT-RCM systems so that only the Department's authorised personnel may access them, thus guaranteeing independence from other general-purpose networks.

5.1.2.3 Work in secure areas

200. Work in secure areas is protected by access controls and, when required, is monitored by the FNMT-RCM's Security Department. Unless specifically authorised by Management, photographic, video, audio or other recording devices are not permitted in these areas.

5.1.2.4 Visits

201. Access by non-FNMT-RCM personnel to the facilities must previously be communicated to the Security Department and authorised by Ceres Department management. Visitors must wear a visible identification card and be accompanied at all times by FNMT-RCM personnel.

5.1.2.5 Separate loading and unloading areas

202. Loading and unloading are carried out in separate areas under permanent technical and human surveillance.

5.1.3. Power and air conditioning

203. The rooms housing the *Trust Service Provider*'s infrastructure machines has an adequate electricity supply and air-conditioning to create a favourable operating environment. This production infrastructure is protected against power outages or any anomaly in the power supply by means of an independent auxiliary power line from the main supply centre, as well as an autonomous power generator.

204. Mechanisms are also in place to keep heat and humidity at suitable levels for the *Trust Service Provider'*s system.

205. Where necessary, the systems have uninterruptible power supply units, a dual power supply and a generator.

5.1.3.1 Cabling security

206. Cabling is located in false ceilings or floors and is adequately protected by fire detectors in the floor and ceiling, and humidity sensors for fast leak protection.

5.1.4. Water exposures

207. The necessary steps have been taken to prevent water exposure in relation to equipment and cabling.

5.1.5. Fire prevention and protection

208. The rooms are suitably equipped (detectors) to protect their content against fire.

5.1.6. Media storage

209. The FNMT-RCM, as a *Trust Service Provider*, has the necessary procedures in place to back up all the information in its production infrastructure. All media are handled securely in accordance with requirements of the information classification scheme as described by the Standard of "Classification and control of information resources" developed by the Information Security Policy of the FNMT-RCM. Media containing sensitive data are securely disposed of when no longer required.

5.1.6.1 Information recovery

210. The FNMT-RCM has backup plans covering all sensitive information and data deemed to be necessary for the Department's business to continue. There are various preparation and recovery procedures depending on the sensitivity of the information and of the installed media.

5.1.7. Waste disposal

211. A waste management policy is in place to guarantee the destruction of any material that may contain information, as well as a policy for the management of removable media.

5.1.8. Off-site backup

212. Backups applicable to the FNMT-RCM as a *Trust Service Provider* are not made outside its facilities.

5.2. PROCEDURE CONTROLS

213. The FNMT-RCM possess an Information Security Policy, approved by its Director General, ratified by the Information Security Committee and the Management Committee, and is subject to a process of periodic review and permanent updating, in order to guarantee its adaptation to the needs of the organization, current legislation and continuous technological advances. The maximum period between revisions of the Information Security Policy is one year. The participation of a member of the TSP Management Committee in the Information

Security Committee guarantees the adequacy of the provision of trust services to said Policy and participation in the aforementioned process of updating it.

214. The FNMT-RCM seeks to assure that all management of both operating and administrative procedures is carried out in a trustworthy manner as stipulated in this document; audits are performed to avoid any defect that could lead to a loss of trust (see the section 8 "Compliance audits").

- Audits are carried out to verify the fulfilment of security measures and technical and administrative requirements.
- Functions are segregated to avoid the same person obtaining control over the entire infrastructure. To this end, multiple profiles are defined and assigned to infrastructure personnel to distribute tasks and responsibilities.

215. The FNMT-RCM outsources certain activities, such as the *Certificate* user service unit. These activities are carried out as stipulated in the FNMT-RCM's *Certification Policies and Practices* and in contracts and agreements with the relevant entities. In these cases, third-party access to information owned by the FNMT-RCM is subject to the protocol defined in the Security Policy as regards the identification of risks, establishment of security controls to protect access to information, the relevant confidentiality agreements and, if applicable, an agreement on personal data processing in compliance with prevailing legislation.

216. The FNMT-RCM will implement supervision and control programmes to assure that the entities that carry out delegated functions related to the provision of certification services comply with the FNMT-RCM's policies and procedures.

217. The FNMT-RCM has an up-to-date inventory of all the information and system assets employed to process information, detailing their owner or person responsible, nature, classification and any other relevant data to prevent and react to incidents. Information processing systems are categorised to put in place security controls in accordance with the National Security Scheme.

218. The FNMT-RCM, through its Code of Conduct Review Committee, oversees compliance with the Code to avoid situations that could result in a conflict of interest. Additionally, the specific regulations[3] that apply to trust roles, as civil servants, guarantee the impartiality of the operations in the activity of the FNMT-RCM, in its activity as Trust Services Provider.

5.2.1. Trusted Roles

219. People who perform "Trusted roles" are suitably trained and have the knowledge and experience necessary to execute the work related to each role. Where necessary, the FNMT-RCM has provided suitable technical and security training for personnel involved in the management of its trustworthy systems.

[3] Royal Legislative Decree 5/2015, of October 30, approving the revised text of the Basic Employee Statute Law.

5.2.2. Number of Individuals Required per Task

220. The tasks assigned, depending on the trusted role, are set out in the internal document of the FNMT-RCM's Information Systems Department entitled "Trusted roles and security profiles".

221. The FNMTs Private Key are backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

5.2.3. Identification and Authentication for Trusted Roles

222. Trusted roles, tasks assigned and security profiles are identified in the internal document of the FNMT-RCM's Information Systems Department entitled "Trusted roles and security profiles".

5.2.4. Roles Requiring Separation of Duties

223. The following trusted roles are defined: Security Officer, System Administrator, System Operator, System Auditor and Validation Specialist. People are selected for these roles applying the principle of least privilege and taking into account training, experience and the Personnel Security controls described below. The people holding these roles will be designated by the CSP's Management Committee.

5.3. PERSONNEL CONTROLS

224. The FNMT-RCM has internal procedures establishing all the controls necessary to identify the activities performed by users in critical information systems that affect the provision of Trust Services so as to log incidents and assure traceability. There is an auditable log for each access or failed access attempt in both the system and the system assets. All activities relating to security functions are logged.

225. There is a policy on the management of access privileges for information and information systems, as well as user password management. Privileges granted in the system to each user are reviewed periodically by the person responsible for each information system or asset. Consequently, the FNMT-RCM administers access for system operators, administrators and auditors, with sufficient logical security controls to guarantee the separation of the trusted roles identified in its trust service practices, such that privileges related to access to critical applications in the *Trust Service Provider*'s infrastructure are afforded special treatment, previously identifying and authenticating personnel authorised to access and equipping them with electronic certificates in cryptographic cards.

226. In the course of their work for the FNMT-RCM, or whenever they use the FNMT-RCM's media and/or materials, its employees, in accordance with their employment contracts and/or applicable legislation, exclusively assign to the FNMT-RCM all exploitation rights that may be applicable to intellectual property, to the fullest extent and for the maximum duration envisaged in the Law, worldwide and, in particular, for illustrative, non-restrictive purposes, rights of reproduction, distribution, transformation and public communication, as well as other industrial property rights or semiconductor topography rights, and rights to projects, works, inventions and creations that they may originate and/or develop. The employees, as a

result of the exclusive assignment of the said rights to projects, works, inventions and creations prepared or created as a result of their employment relationship with the FNMT-RCM or as a result of the use of the FNMT-RCM's material and/or technical resources, will not be entitled to exploit the said works and/or creations in any way, even if this would not harm the exploitation or use of the same by the FNMT-RCM.

227. In order to comply with the FNMT-RCM's internal rules, applicable laws and regulations, and assure its employees' security, the FNMT-RCM reserves the right to inspect, at any time, and monitor all the FNMT-RCM's computer systems.

228. The computer systems subject to inspection include, but are not limited to, e-mail archives, personal computer hard drive archives, voice mail archives, print queues, fax machine documents, desk draws and storage areas. These inspections will be carried out after having been approved by the Security and Legal Affairs Departments, following the procedures laid down in applicable legislation and involving trade union representatives, if appropriate. The FNMT-RCM reserves the right to remove from its computer systems any material that it considers to be offensive or potentially illegal or fraudulent.

229. The FNMT-RCM's management reserves the right to revoke the system privileges of any user at any time. No conduct will be permitted that interferes with the normal and adequate functioning of the FNMT-RCM's computer systems, prevents others from using the systems or is dangerous or offensive.

230. The FNMT-RCM will not be responsible for opinions, acts, transactions and/or underlying businesses that the users may express or carry out using the FNMT-RCM's certification systems, all without affecting the FNMT-RCM's obligation to report any matter to the competent authority, if applicable.

231. Unless the relevant authorisation is granted by the FNMT-RCM's Information Systems Department, the FNMT-RCM's employees must not acquire, possess, trade or use hardware or software tools that could be employed to evaluate or compromise the IT security systems. Some examples of such tools are those that ignore software protection against unauthorised copies, detect secret passwords, identify vulnerable security points and decode archives. Moreover, employees are prohibited, without suitable permission, from using trackers or other types of hardware or software that detects traffic in a networked system or a computer's activity, barring cases in which their use is necessary to conduct system testing and after informing the head of the department in question.

232. Users must not verify or try to compromise the security measures in place in a communication machine or system unless this action has previously been approved in writing by the FNMT-RCM's Information Systems Management. Incidents related to computer piracy, password discovery, archive decoding, unauthorised copying of software, personal data protection and other activities representing a threat to the security measures, or which are illegal, will be deemed serious infringements of the FNMT-RCM's internal rules. The use of bypass systems to avoid protection measures and other archives that may compromise protection systems or resources is also absolutely forbidden.

233. All these infringement of regulations, system intrusions, malicious software infections and other conditions that jeopardise the FNMT-RCM's information or computer systems must be immediately reported to Information Systems Management.

5.3.1. Qualifications, Experience, and Clearance Requirements

234. All the personnel involved in the activity of the FNMT-RCM, as a Trusted Service Provider, and especially the managerial staff, possess necessary experience and knowledge to manage said activity. These requirements are guaranteed by the corresponding criteria in the personnel selection processes, verifying the identity and trustworthiness of such person and that the employee's professional profile is as appropriate as possible to the characteristics of the tasks to be developed. The trustworthiness and suitability of the assigned trusted roles are reviewed periodically.

235. Procedures followed to manage infrastructure personnel will promote competence and know-how, as well as the fulfilment of their obligations.

236. Trusted positions within the scope of this document will be those that entail access to or control of components that could directly affect the management of systems that implement the services related to *Certificates* and information on the status of *Certificates.*

5.3.2. Background Check Procedures

237. The terms and conditions of the employment relationship are included in both the relevant contract and in the Collective Agreement on work relations between the FNMT-RCM and its employees, as well as in legislation applicable by virtue of the Statute.

5.3.3. Training Requirements and Procedures

238. The FNMT-RCM manages the Annual Training Plan, through its Training Centre attached to the Human Resources Department, on the basis of the Entity's general needs and each department's specific needs. All employees, whether on the payroll or subcontracted, who have access to or control of the trustworthy systems on which the trusted third-party services are based are covered by the annual Training Plan focused on information security training and awareness building needs, as laid down in the internal document “Information security training and awareness raising standard”.

239. For the personnel performing information verification duties the annual training covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the FNMT’s Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” and the “EV SSL Certificate Guidelines” established by the entity CA/Browser forum.

240. The FNMT-RCM maintains records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

241. The FNMT-RCM documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

242. The FNMT-RCM requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

5.3.4. Retraining Frequency and Requirements

243. The FNMT-RCM implements ongoing training plans, paying particular attention to substantial modifications of *Trust Service* infrastructure operations. The FNMT-RCM review these requirements at least once a year.

5.3.5. Job Rotation Frequency and Sequence

244. Not stipulated.

5.3.6. Sanctions for Unauthorized Actions

245. Security is included among employees' responsibilities but does not require additional references since the FNMT-RCM's main purpose is security, which is therefore the objective and responsibility of all the organisation's members.

246. In any event, without prejudice to the relevant public legislation, provisions of the Criminal Code that are directly applicable and clauses of certain senior management contracts, Chapter XVII "Disciplinary regime", Article 63. Infringements and Penalties of the above-mentioned Collective Agreement specifically states:

> *"The following shall be serious infringements:*
>
> *...*
>
> *13. The undue use or disclosure of data or matters known by reason of the work carried out in the Organisation.*
>
> *...*
>
> *The following shall be very serious infringements:*
>
> *...*
>
> *9. The use of the FNMT-RCM's internal information for the employee's own benefit or for the benefit of companies competing with the FNMT-RCM.*
>
> *..."*

247. The penalty may entail dismissal, irrespective of any infringement of general legislation and the corresponding penalty or sentence that may be imposed by a court.

248. Additionally, where required, personal confidentiality agreements may be arranged at the request of the FNMT-RCM and/or third parties.

5.3.7. Independent Contractor Controls

249. Personnel recruitment and policies are included in the Collective Agreement regulating work relationships between the FNMT-RCM and its employees, as well as in legislation applicable to the civil service and the related Statute (Royal Decree 1114/1999 of 25 June adapting the Spanish Mint to Law 6/1997 of 14 April on the Organisation and Functioning of the General State Administration, approving its Statute and agreeing on the name *Fábrica Nacional de*

Moneda y Timbre-Real Casa de la Moneda and its status as a State-owned enterprise attached to the Ministry of Economy and Finance (now Ministry of Finance)).

250. Definitions of work posts and responsibilities, including security positions, are included in the Collective Agreement regulating work relationships between the FNMT-RCM and its employees, as well as applicable regulations governing the civil service.

251. In the case that an independent contractor is assigned to perform a Trusted Role for the certification service, the FNMT-RCM will verify that the personnel involved meet the training and skills requirements of section 5.3.3 and the document retention and event logging requirements of section 5.4.1

5.3.7.1 Third-party contracting requirements

252. The contracting of third parties by the FNMT-RCM is subject to the Law 9/2017, of November 8, on Contracts of the Public Sector, by which the Directives of the European Parliament and Council 2014/23 / EU and 2014/24 / EU, of February 26, are transposed into the Spanish legal system (*LCSP*). In this context, the Entity is an "awarding authority" and is therefore subject to the above-mentioned law, i.e. to the "harmonised regulation" of contracting. For cases in which the *LCSP* is not applicable, the FNMT-RCM will employ its Internal Contracting Instructions (*IIC*).

5.3.8. Documentation Supplied to Personnel

253. All employees who have access to or control of the trustworthy systems in which trusted third-party services are based are provided with access to the department's knowledge database, which contains documentation on security regulations, *Certification Practices and Policies*, functions entrusted to personnel, the quality and security plan, business continuity policy and plans and, in particular, they are provided with the documentation required to carry out their respective tasks.

254. Personnel assigned permanently or temporarily to these posts will be duly accredited and identified by the FNMT-RCM. A periodic assurance process is completed to verify that they are still trusted by the FNMT-RCM to perform their confidential duties.

255. Relations between third parties and the FNMT-RCM are protected by the relevant confidentiality agreement if sensitive information must be exchanged in the course of the relationship.

256. The FNMT-RCM's personnel, under the Collective Agreement, do not require specific personal confidentiality agreements, without affecting exceptional cases in which there may be personal confidentiality agreements, normally due to third-party requests or the FNMT-RCM's own decisions.

5.4. AUDIT PROCEDURES

257. The FNMT-RCM has a system for monitoring and logging events that is independent from the production infrastructure. It functions uninterruptedly (24x7), compiling security information and events for all the Certification Authority's sensitive and trust-related elements for subsequent processing and correlation.

258. The relevant reports are extracted from this monitoring system in order to oversee infrastructure security. Rules and policies are in place to provide real-time alarms in the event of anomalous behaviour in the Certification Authority's systems or signs of a security incident.

5.4.1. Types of Events Recorded

259. The FNMT-RCM will log all significant events so as to verify that all the internal procedures necessary to carry out its activities are executed as stipulated in this document, in applicable legislation and in the Internal Security Plan and Quality and Security Procedures, allowing the causes of any anomalies to be identified. These logged events will be made available, if necessary, so as to provide evidence of the proper functioning of the services for the purposes of court proceedings.

260. The events logged will include all operations carried out during the management of keys, *Certificates*, *Electronic time stamp* issuance, *Certificate* status information, publication, filing, recovery, directory, event logs and user logs. All events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA. The registration information (identity accreditation), such as the unique identification data, the signed subscriber agreement, the identity of the entity to which the Registration Office belongs, etc., will also be part of the recorded events, as specified in the corresponding documents of Registration Procedures. The FNMT-RCM will archive all the most important events logged and will keep them accessible for a period of not less than 15 years.

261. All events logged may be audited and will include the date and time of record, the identity of the person making the journal record and a description of the record.

262. The FNMT-RCM will make available to the competent authorities the evidences related to the registered events that are in its possession, by judicial request or the corresponding legal procedure, upon written request made to the contact data described in section "1.5. 2. Contact details".

263. In addition to the events mentioned, all logs specified by the ISO 9001 and SR10 standards will be kept in the manner stated in the FNMT-RCM's general quality procedures, for a period of not less than three years.

264. FNMT:RCM will record at least the following events:

a) CA certificate and key lifecycle events, including:

1. Key generation, backup, storage, recovery, archival, and destruction;
2. Certificate requests, renewal, and re-key requests, and revocation;
3. Approval and rejection of certificate requests;
4. Cryptographic device lifecycle management events;
5. Generation of Certificate Revocation Lists and OCSP entries;
6. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

b) Subscriber Certificate lifecycle management events, including:

1. Certificate requests, renewal, and re-key requests, and revocation;

2. All verification activities stipulated in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and the CA's Certification Practice Statement;
3. Approval and rejection of certificate requests;
4. Issuance of Certificates; and
5. Generation of Certificate Revocation Lists and OCSP entries.

c) Security events, including:

1. Successful and unsuccessful PKI system access attempts;
2. PKI and security system actions performed;
3. Security profile changes;
4. Installation, update and removal of software on a Certificate System;
5. System crashes, hardware failures, and other anomalies;
6. Firewall and router activities; and
7. Entries to and exits from the CA facility.

5.4.2. Frequency for Processing and Archiving Audit Logs

265. Logs are analysed continuously, although they may be audited manually where necessary. For example, this will occur in the event of a system alert caused by an incident, no frequency having been stipulated for this process.

5.4.3. Retention Period for Audit Logs

266. FNMT-RCM shall retain, for at least 15 years:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 after the later occurrence of:
   a. the destruction of the CA Private Key; or
   b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the CA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 after the revocation or expiration of the Subscriber Certificate;
3. Any security event records (as set forth in Section 5.4.1) after the event occurred.

5.4.4. Protection of Audit Log

267. Once entered in the systems, logs cannot be modified or deleted and will remain archived in their original condition.

268. Logs will only have read access and will be restricted to people authorised by the FNMT-RCM.

269. Logs will be recorded automatically by specific software implemented by the FNMT-RCM as deemed fit, so as to prevent manipulation.

270. The audit log will be protected against any contingency, modification, loss or data disclosure during recording on external media, change of external media and storage, in addition to the security measures in place for recording and subsequent verification.

5.4.5. Audit Log Backup Procedures

271. The FNMT-RCM, in its activities as a *Trust Service Provider* using a high-security system, guarantees that backups will be made of all audit logs.

5.4.6. Audit Log Accumulation System (internal vs. external)

272. The significant events generated by the CAs and by the RAs are duly stored in the FNMT-RCM's internal systems.

5.4.7. Notification to Event-Causing Subject

273. Not envisaged.

5.4.8. Vulnerability Assessments

274. The FNMT-RCM carries out quarterly vulnerability analyses in its systems. An annual penetration test is also performed.

5.5. LOG ARCHIVING

5.5.1. Types of Records Archived

275. The FNMT-RCM will archive and keep accessible all relevant information on the data issued and received, particularly for use as evidence in legal proceedings and to guarantee the continuity of its Trust Services.

276. The following will be logged:

- Issuance, revocation and other relevant events related to the *Certificates*, as well as operations related to the management of the *Trust Service Provider*'s keys and *Certificates*.
- *Signatures* and other relevant events related to *Revocation Lists* (CRLs).
- All operations to access the *Certificate* archive.
- All operations to access the *Certificate status information service*.
- Relevant events relating to the generation of random and pseudo-random number pairs for *Key* generation.

- Relevant events relating to the generation of own *Key* pairs or *Key* pairs for authentication support. The numbers themselves or any data facilitating the prediction of the numbers will not be included in any event.
- All operations in the *Key* filing service and access to the expired own *Key* archive.
- All operations related to activities as a trusted third party.
- Relevant events in the *Time Stamping Authority*'s operations, particularly relating to clock synchronisation and synchronisation losses. The exact moment of occurrence will also be included.

277. In addition to these events, all related documentation is also archived, for example:

- Documentation related to the generation and conservation protocols of the *Keys* of the *Certification Authorities* and the *Time Stamping Service*.
- Requests for issuance and revocation of *Certificates*,
- Documentation related to the accreditation operations carried out by the registration offices.
- Events related to the provision of the server signature service

278. Declarations of *Certification Practices* and *Policies* and their history.

5.5.2. Retention Period for Archive

279. The retention period of the archived records shall not be less than 15 years after the expiration of the validity of the associated certificate.

5.5.3. Protection of Archive

280. Access to the logs will be limited to personnel authorised by the FNMT-RCM.

281. Third-party access to encrypted data by means of the data recovery service without user authorisation must always comply with the Law and, if applicable, with the relevant *Contracts, Commissions and Agreements*.

282. The FNMT-RCM guarantees that the archive of logged events meets the following requirements:

- It may not be modified through unauthorised means.
- Availability and reliability must be high.

283. The confidentiality of the information will be guaranteed and access will be traceable.

5.5.4. Archive Backup Procedures

284. All archives deemed to be critical to the FNMT-RCM's activities as a *Trust Service Provider* will be backed up at all times.

5.5.5. Requirements for Time-stamping of Records

285. All the events stored contain a time mark obtained from the UTC time reference (Spanish Navy Observatory). The Spanish Navy Observatory (*ROA*) is Spain's official timing centre. The FNMT-RCM and the *ROA* have an agreement to synchronise the time in their systems. The terms and conditions of the Synchronisation System are defined in the document "FNMT – ROA Synchronisation System".

5.5.6. Archive Collection System (internal or external)

286. The archive systems used by the FNMT-RCM to keep these audit logs will be the infrastructure's own internal systems and external media with storage capacity for long periods of time will also be employed. These media will provide sufficient guarantees to prevent any type of alteration of the logs.

287. The FNMT-RCM will make several copies that will be stored in different places equipped with all physical and logical security measures to avoid, where reasonably possibly, any alteration of the media stored and of the data contained in the media. Each copy will be stored in a different place in case of a disaster in any location.

5.5.7. Procedures to Obtain and Verify Archive Information

288. These archive systems have a high level of integrity, confidentiality and availability to avoid attempts to manipulate the *Certificates* and events stored.

5.6. CHANGE OF CA KEYS

289. Prior to the expiration of the validity period of the *Certificate* of a root *Certification Authority* or of a subordinate *Certification authority*, a new root or subordinate *Certification Authority* will be created by generating a new key pair. The old *Certification Authorities* and their associated private keys will only be used to sign CRLs while there are active Certificates issued by those CAs.

5.7. INCIDENT AND VULNERABILITY MANAGEMENT

5.7.1. Incident and Compromise Handling Procedures

290. The FNMT-RCM guarantees a coherent and effective approach to the management of information security incidents. The document "Information Security Management System - Security Manual" lays down incident management procedures and responsibilities, guaranteeing a fast, effective and orderly response to security incidents.

291. The FNMT-RCM obtains information on technical vulnerabilities affecting the information systems and the appropriate measures are taken. Responsibilities associated with the management of technical vulnerabilities are defined and established, maintaining the information resources up-to-date in the asset inventory so as to identify any such vulnerabilities. Additionally, procedures undertaken are audited periodically and the management of technical vulnerabilities is monitored and assessed on a regular basis.

292. The FNMT-RCM will address any unforeseen critical vulnerability within 48 hours of discovering it. Once the impact has been analysed, it will be documented and a decision will be taken to resolve the vulnerability by means of a mitigation plan, based on the resolution cost.

293. In the case of a security incident, the affected parties will be notified as described in the Security Policy and the related implementing rules, particularly the incident response plan. In the event of a high-impact incident, the FNMT-RCM will send notification in less than 24 hours following detection.

5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

294. This contingency is envisaged in the FNMT-RCM's Business Continuity Plan.

5.7.3. Recovery Procedures After Key Compromise

295. This contingency is envisaged in the FNMT-RCM's Business Continuity Plan, as is the procedure to be followed, described in the Crisis Management Plan as part of the Business Continuity Plan, including the following actions, among others:

1) Stop providing the affected service.
2) Revoke any certificates that might be affected.
3) Execute the Communication Plan to notify of the events affected parties and to the browsers in whose root programs the FNMT-RCM certificates are included.

296. Study the need to execute the Discontinuance of the CSP's Activities as per the Certification Practices Statement and prevailing legislation.

5.7.4. Business Continuity Capabilities after a Disaster

297. The FNMT-RCM has a business continuity plan describing the actions to be implemented in case of disaster. So, it has a backup system that stores in safe places the data necessary to resume CA operations in case of incident/disasters, even in the alternative support centre, in order to ensure that all essential information and software can be recovered following a disaster or media failure.

298. To guarantee business continuity after a contingency or disaster and following the provisions of the FNMT Business Continuity Plan Test Plan- RCM, backups are regularly tested by means of drills at least once a year.

299. In the case of a failure or disaster affecting the *Trust Service Provider*'s systems, a Disaster Recovery Plan will be launched, encompassing:

- Redundancy of the most critical components.
- Start-up of an alternative support centre.
- Full, periodic checking of backup copy services.
- Compromised *Signature creation data* of the *Trust Service Provider or algorithm compromise that leads a real threat, considering the current state of the art, identity impersonation*. In these cases, the FNMT-RCM will schedule the revocation of the

affected *Certificates* and will inform all members of the *Electronic Community* that all the *Certificates*, *Revocation Lists*, *Electronic time stamps* and any other data structure able to be signed are no longer valid due to the compromised data. The FNMT-RCM will restore the service as soon as possible and on the new terms applicable.

300. The FNMT-RCM will not be responsible for the lack of service or service anomalies, nor for any damage that may be caused directly or indirectly, when the failure or disaster is the result of force majeure causes, a terrorist attack, sabotage or wildcat strikes, all without affecting any actions necessary to correct and/or restore the service as soon as possible.

5.8. DISCONTINUANCE OF THE TRUST SERVICE PROVIDER'S ACTIVITIES

301. In the event of the discontinuance of the *Trust Service Provider* activities, the FNMT-RCM will be subject to the provisions of prevailing electronic signature legislation.

302. In any case, the FNMT-RCM:

- Will duly inform *Certificate Subscribers* and *Holders*, and the Users of the affected services, of its intention to discontinue *Trust Service Provider* activities at least two (2) months in advance.
- Any outsourcing of functions carried out in the FNMT-RCM's name relating to the service to be discontinued will be terminated.
- Once evidence that the *Subscribers* do not object has been obtained, *Certificate* that are still valid at the effective date of discontinuance may be transferred to a different *Trust Service Provider*. If such transfer is not possible, the *Certificates* will expire.
- Whatever the service discontinued, the FNMT-RCM will transfer the event and audit logs to a third party, as well as the *Certificates* and keys used to provide the service, for a sufficient period of time as stipulated in prevailing legislation.
- The *Supervisory body* will be informed of the discontinuance of the activity and the destination of the *Certificates*, specifying, if applicable, whether they are to be transferred or will expire. That body must be notified at least two (2) months in advance by means of a document signed by hand or electronically.

303. If discontinuance relates to the *Time Stamping Service*, the FNMT-RCM will:

- revoke the *Certificates* of the affected *Time Stamping Units*.
- destroy the *Private Keys* of the *Time Stamping Units* and related backups so that they cannot be recovered.

304. If discontinuance relates to the *Server signature service*, the FNMT-RCM will:

- revoke the certificates of the affected Certification Authorities, and
- destroy users' Private Keys and their backups, so that they cannot be recovered.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key pair generation

6.1.1.1 CA Key Pair Generation

305. The FNMT-RCM possess a procedure described in the document "Gestión del ciclo de vida de las claves de la FNMT-RCM como Prestador de Servicios de Certificación y Sellado", for conducting CA key pair generation for all CAs, whether root CAs or subordinate CAs that issue certificates to end users.

306. Following this procedure, the FNMT-RCM will prepare and follow a Key Generation Script, have a Qualified Auditor witness the CA Key Pair generation process, and have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

307. This procedure describes the following:

- roles participating in the ceremony;
- functions to be performed by every role and in which phases;
- responsibilities during and after the ceremony; and
- requirements of evidence to be collected of the ceremony.

308. The procedure of issuing, signing and distributing of new CA Certificate, specifying that before the expiration of the *Certificate* a new one is generated, thus avoiding possible interruptions in the operations from any entity that can trust the *Certificate*.

309. For reasons of security and quality, the *Keys* that the FNMT-RCM needs to carry out its activities as a *Trust Service Provider* will be generated by the Entity itself inside its own infrastructures, in a physically secure environment and by at least two authorised persons.

310. *Key* generation and *Private Key* protection are performed guaranteeing the necessary confidentiality measures, using secure, trusted hardware and software systems under the EESSI CWA14167-1 and CWA14167-2 standards, in addition to the necessary precautions to prevent loss, disclosure, modification or unauthorised use, in accordance with the security requirements specified in the EESSI standards applicable to *Trust Service Providers*.

311. *Key* algorithms and lengths employed are based on standards that are broadly recognised for the purpose for which they are generated.

312. The technical components necessary to create *Keys* are designed so that a *Key* is only generated once and so that a *Private Key* cannot be calculated using its *Public Key*.

6.1.1.2 RA Key Pair Generation

313. Not stipulated

6.1.1.3 Subscribers Key Pair Generation

314. The *Private keys for* the *Website authentication certificates* are generated and guarded by the *Subscriber* of the *Certificate.*

6.1.2. Private key delivery to subscriber

315. There is no generation or deliver of the *Private key* to the *Holder.*

6.1.3. Public key delivery to certificate issuer

316. The *Public key*, generated along with the *Private key* for the key generation and custody device, is submitted to the Certification Authority by sending a certification request using the PKCS #10 format.

6.1.4. CA public key delivery to relying parties

317. The FNMT-RCM distributes the *Public Keys*, both of the root CA and of the subordinate CAs that issue the *Website Authentication Certificates*, through various means, such as publication on its website (www.sede .fnmt.gob.es), or through public information contained in this document, in section "1.3.1. Certification Authority".

6.1.5. Key sizes and algorithms used

318. The algorithm used is ECDSA-with-SHA384.

319. The Key size, depending on each case, is:

- FNMT root CA Keys: ECC P-384 bits.
- CA Subordinate keys: ECC P-384 bits.
- *Website authentication certificate* keys: ECC P-384 bits.

6.1.6. Public key parameters generation and quality checking

320. The *Public keys* for the *Website authentication certificates* are encoded under RFC5280 and PKCS#1.

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

321. The FNMT *Certificates* include the Key Usage extension and, as applicable, the Extended Key Usage extension, indicating authorised uses of the *Keys*.

322. The root *Certificate* of the CA has enabled the uses of Keys to sign/stamp the *Certificates* of the Subordinated CAs and the ARLs. The *Certificates* of the Subordinate CAs that issue *Website Authentication Certificates* are exclusively authorised to sign/stamp end user *Certificates* (*Website authentication certificates*) and CRLs.

323. The *Website authentication certificate* is enabled for use of a digital signature. Additionally, these Certificates feature the Extended Key Use for server authentication and client authentication.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

324. FNMT-RCM shall protect its Private Key(s) in accordance with the provisions of this CPS and in a compliance with CA/Browser Forum's Baseline Requirements

6.2.1. Cryptographic Module Standards and Controls

325. The *Trust Service Provider*'s *Signature creation data* are protected by a cryptographic device that fulfils FIPS PUB 140-2 Level-3 security standards. Operations for the signing of *Certificates, Revocation lists* and data structures relating to the validity of *electronic Certificates* and *Time Stamps* are carried out inside the cryptographic device, which brings *Confidentiality* to the *Trust Service Provider*'s *Signature creation data*.

326. When the *Signature creation data* are outside the cryptographic device, the FNMT-RCM applies the appropriate technical and organisational measures to guarantee their *Confidentiality.*

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

327. Mechanisms to activate and use the *Certification Authorities' Private keys* are based on the segmentation of management and operation roles that the FNMT-RCM has implemented, including multi-person access based on cryptographic cards and related PINs in a simultaneous use M of N (2 of 5) system.

6.2.3. Private Key Escrow

328. Copy, backup or recovery operations relating to the *Signature creation data* are controlled exclusively by authorised personnel employing, at minimum, dual control in a secure environment.

329. The *Holders*' *Private Keys* are held, at a high level of trust, under the exclusive control of the *Holder*.

6.2.4. Private Key Backup

330. Backup copies of CA Private Keys shall be backed up by multiple persons in Trusted Role position sand only be stored in encrypted form on cryptographic modules that meet the requirements specified in Section 6.2.1

6.2.5. Private Key Archival

331. Only the FNMT-RCM may make a backup of the *Private keys,* guaranteeing that the security level of the copied data is at least equal to that of the original data and that the number of data duplicated does not exceed the minimum necessary to assure service continuity. The *Signature creation data* are not duplicated for any other purpose.

6.2.6. Private Key Transfer into or from a Cryptographic Module

332. The *Certification Authorities*' *Private keys* are generated as described in point "6.1 *Key* generation and installation". In the event that a Private Key is to be transported from one Cryptographic Module to another, the Private Key must be encrypted during transport. Private Keys must never exist in plain text form outside the Cryptographic Module boundary

6.2.7. Private Key Storage on Cryptographic Module

333. The FNMT-RCM has the necessary means to assure that the cryptographic hardware used to protect its *Keys* as a *Trust Service Provider:*

- Has not been manipulated during transportation, by means of an inspection of the material supplied which includes controls to detect authenticity and possible manipulation.
- Functions correctly, through continuous monitoring processes, periodic preventive maintenance and a software and firmware upgrade service.
- Remains in a physically secure environment from receipt to destruction, if applicable.

334. Root CA private keys of the FNMT-RCM are held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA *Certificates*.

335. Root CA private keys of the FNMT-RCM are generated and stored inside cryptographic modules which meet the requirements of 6.2.1 of this *CPS*

6.2.8. Activating Private Keys

336. The *Certification Authorities' Private keys* are generated and custodied by a cryptographic device that meets FIPS PUB 140-2 Level 3 security requirements.

6.2.9. Deactivating Private Keys

337. A person in an administrator's role may deactivate *the Certification Authorities' Key* by stopping the system. Reactivation will follow the steps described in point "6.2.8 Private key activation method".

6.2.10. Destroying Private Keys

338. The FNMT-RCM will destroy or store the *Trust Service Provider*'s *Keys* in an appropriate manner once the validity period has elapsed so as to avoid misuse.

6.2.11. Cryptographic Module Capabilities

339. The cryptographic modules fulfil the security requirements necessary to guarantee *Key* protection, as indicated in point "6.2.1 Cryptographic module standards" of this document.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

340. The *Certificates of authentication of websites* and, in turn, their associated *Public keys,* are kept by the FNMT-RCM during the period of time required by current legislation, which is currently specified as 15 years.

6.3.2. Certificate operational periods and key pair usage periods

341. *Certificate* and associated *Key* operating periods are as follows:

- Root CA *Certificate* and set of *Keys:* see section "1.3.1 Certification Authority" of this *CPS*.
- The certificate of the subordinate CA that issues the authentication certificates for websites and their set of *Keys*: see section "1.3.1. Certification Authority" of this *CPS*.
- The *Website authentication certificates* and their set of *Keys*: the maximum period of validity of the *OV Certificate, SAN OV Certificate, Wildcard OV Certificate*, *EV Certificates, SAN EV Certificates and Electronic Venue certificate EV* is 12 months.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

342. The activation data, both the FNMT root CA *Keys* and the *Keys* of the subordinate CAs that issue end-entity *Certificates*, are generated during the *Certification Authorities*' *Key* creation ceremony.

6.4.2. Activation data protection

343. The activation data for the Certification Authorities' *Private keys* are protected using the method described in paragraph "6.2.8 Private key activation method" of this document, including multi-person access based on cryptographic cards and related PINs in a simultaneous use M of N (2 of 5) system.

6.4.3. Other aspects of activation data

344. Not stipulated.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

345. When defining security for all the technical components used by the FNMT-RCM in the course of its *Trust Service Provider* activities and in its structure and procedures, all aspects of Information System security certification are taken into consideration, in accordance with the National Information System Security Certification Framework approved in Spain, in

particular those relating to EESSI published in the Official Journal of the European Union or in the relevant Spanish Official Journals. Information technology security evaluation under ISO 15408 (Common Criteria) is also taken into account in the design, development, evaluation and acquisition of IT products and systems for use by the *Trust Service Provider*, in addition to the EESSI regulations.

346. The FNMT-RCM shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

347. Infrastructure security management processes will be evaluated periodically.

6.5.1.1 Notification of security incidents

348. Incidents are reported to Management, irrespective of whether or not the appropriate corrective action is taken, through the Incident Management System in place in the Department to assure the fastest possible solution, as described in the "Incident Notification Procedure" and "Incident Management Procedure".

6.5.1.2 Notification of security weaknesses

349. Security weaknesses are classed as incidents and, as such, are resolved, giving rise to the appropriate corrective action, as described in the above-mentioned procedures.

6.5.1.3 Notification of software failures

350. Software failures are classed as incidents and, as such, are resolved, giving rise to the appropriate corrective action, as described in the aforementioned procedures.

6.5.1.4 Learning from incidents

351. The "Incident Notification Procedure" and "Incident Management Procedure" also include incident groups and classifications giving rise to the relevant corrective actions.

6.5.2. Computer Security Rating

352. Technical components supplied to users so as to enhance public trust in the FNMT's cryptographic methods include security evaluations of the products and services offered, applying open criteria accepted by the market.

353. Security levels of infrastructure components and procedures and components forming part of the activities of the *Trust Service Provider* will be evaluated in accordance with "Information Technology Security Evaluation Criteria" (ITSEC/ITSEM) and/or Common Criteria (ISO15408), and particularly the EESSI initiative.

354. Information security management is carried out in accordance with the UNE- ISO/IEC 27001 standard "Information Security Management Systems (ISMS). Requirements", regulations under which the FNMT-RCM has the corresponding certification in the field of systems involved in the provision of trust services.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System development controls

355. Before undertaking a software development project, the *Trust Service Provider* follows the "Guidelines for the establishment of security requirements for applications developed by Ceres". This guarantees that computer applications developed undergo a risk assessment process and an analysis of security requirements.

356. The *Trust Service Provider*'s computer applications are developed in accordance with the "Procedure for managing changes in applications developed by Ceres". This procedure allows identification of the need for emergency corrections or new versions of software, impact assessments, inclusion and documentation of approved changes, and verification that the product definition is consistent.

6.6.2. Security management controls

357. The integrity of the FNMT-RCM's information and systems, as a *Trust Service Provider,* is protected against viruses, malware and unauthorised access.

358. The FNMT-RCM has procedures guaranteeing the application of security patches in the shortest possible time once they are available, unless application will result in vulnerabilities or operating failures, in which case the reasons for non-application will be documented.

6.6.3. Life cycle security controls

359. The FNMT-RCM applies security controls throughout the system life cycles, among which includes the management of media, against obsolescence and deterioration of storage media, during the period of time required, in accordance with the provisions of the document "PECE 26026 Backup-Politicas-Restauracion-Arquitectura".

6.6.3.1 Algorithm update

360. The FNMT-RCM keeps permanently up to date with the evolution of cryptographic algorithms and undertakes to update the size of *keys* or cryptographic algorithms used by its *Certification Authorities* before reaching an insufficient level of security.

6.7. NETWORK SECURITY CONTROLS

361. The FNMT-RCM segments its systems in separated networks or zones taking into account the functional, logical and physical relationship between reliable systems and services.

362. For the correct provision of trust services, external access to them is required through the Internet and / or other networks (for example, Red SARA). Access to the Internet in the Main Data Centre is redundant and, in addition, a different operator provides Internet access to the Backup Centre. The mechanisms of commutation of operators are automatic. Access to Red SARA is also redundant in the Main Data Centre and there is a backup in the Backup Centre, so that, if necessary, it is activated from the Red SARA Operations Centre at the request of FNMT-RCM.

363. The means of communication through public networks employed by the FNMT-RCM in its activities are equipped with sufficient security mechanisms to avoid or adequately control any external aggression through these networks. This system is audited periodically to check that it functions correctly.

364. Similarly, the network infrastructure that provides certification services is equipped with the necessary security mechanisms currently known to guarantee a reliable and comprehensive service. This network is also audited regularly.

365. The FNMT-RCM submits to a penetration test the systems related to the provision of trust services, prior to putting it into production and after infrastructure or application upgrades or modifications considered significant. The penetration tests are carried out by the Security and Normalization Area of the FNMT-RCM, which guarantees its execution by qualified personnel who have the necessary skills, tools, proficiency, code of ethics and independence to provide a reliable report.

366. The FNMT-RCM submits to a penetration test the systems related to the provision of trust services, prior to putting them into production and after the updates or modifications of infrastructure or applications considered significant. The penetration tests and the management of the results are the responsibility of the Security and Normalization Area of the FNMT-RCM, which guarantees its execution by independent personnel, who have the necessary skills, tools, competence, code of ethics and independence to provide a reliable report.

367. The FNMT-RCM possess a procedure to carry out the tasks related to the periodic analysis of vulnerabilities and the annual penetration test, treating the results thereof, in terms of their assessment, subsequent elaboration of the corresponding plan of action for correction and, where appropriate, for the corresponding assumption of risks.

6.8. TIME-STAMPING

368. The FNMT-RCM employs as a time source a connection with the Spanish Navy Observatory (UTC time standard) under an agreement between the two institutions to synchronise the time in their systems. The Spanish Navy Observatory (*ROA*) is Spain's official timing centre.

7. CERTIFICATE, CRLS AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

369. *Website authentication certificates* are in accordance with the European standard ETSI EN 319 412-4 "Certificate profile for web site certificates".

370. *Certificates* issued with EV policies (*Electronic Venue certificate EV, EV Certificate and SAN EV Certificate*) contain the policy identifier 0.4.0.2042.1.4., 2.23.140.1.1 and 0.4.0.194112.1.4

371. *Certificates* issued with OV policies (OV *certificate, OV Wildcard Certificate and SAN OV Certificate*) contain the policy identifier 0.4.0.2042.1.7. and 2.23.140.1.2.2

7.1.1. Version number

372. *Website authentication certificates* are compliant with the X.509 version 3 standard.

7.1.2. Certificate content and extensions; application of RFC 5280

373. The extensions defined for the FNMT-RCM's X.509 v3 certificates provide methods for associating additional attributes with users or Public Keys and for managing the certification hierarchy. Each extension in a certificate is designated as either critical or non-critical.

374. Certificate extensions, their criticality, and cryptographic algorithm object identifiers, are provisioned according to the IETF RFC 5280 standards and/or comply with CAB Forum Baseline Requirements and EV Guidelines where appropriate.

375. The documents describing the profiles of the Website authentication certificates, including all extensions, are published at

AC SERVIDORES SEGUROS TIPO 1:

https://www.sede.fnmt.gob.es/documents/10445900/10575386/Perfiles_certificados_servidores_seguros_tipo1.pdf

AC SERVIDORES SEGUROS TIPO 2:

https://www.sede.fnmt.gob.es/documents/10445900/10575386/Perfiles_certificados_servidores_seguros_tipo2.pdf

7.1.3. Algorithm object identifiers

376. The object identifier (OID) relating to the cryptographic algorithm used (ecdsa-with-SHA384) is 1.2.840.10045.4.3.3.

7.1.4. Name formats

377. *Website authentication certificate* encoding follows the RFC 5280 recommendation "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All the fields defined in the *Certificate* profile, except where expressly stated in the relevant fields, use UTF8String encoding.

7.1.5. Name constraints

378. The subordinate CA certificates are not technically constrained.

7.1.6. Certificate policy object identifier

379. The object identifier (OID) of the *Website authentication certificate* policy is that which is defined in section "1.2 Document Name and Identification" of this document.

7.1.7. Usage of the policy constraints extension

380. The "Policy Constraints" extension of the CA's root *Certificate* is not used.

7.1.8. Policy qualifiers syntax and semantics

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

- CPS Pointer: contains the URL in which the *Certification Policies and Trust Service Practices* applicable to this service are published.
- User notice: contains text that may drop down on the *Certificate* user's screen during verification.

7.1.9. Processing semantic for the critical certificate policy extension

382. The "Certificate Policy" extension includes the policy OID field, which identifies the policy associated with the *Certificate* by the FNMT–RCM, as well as the two fields referred to in the previous point.

7.2. CRL PROFILE

7.2.1. Version number

383. The CRL profiles are in accordance with standard X.509 version 2.

7.2.2. CRL and CRL entry extensions

384. The CRL profile has the following structure:

Table 4 – CRL profile

Fields and extensions	Value
Version	V2
Signature algorithm	ecdsa-with-Sha384
CRL number	Incremental value
Issuer	Issuer DN
Issue date	UTC issuance time.
Date of next upgrade	Issue date + 24 hours (with the exception of the ARL, which is Issue date + 6 months)
Authority key identifier	Issuer key hash
ExpiredCertsOnCRL	NotBefore CA value

Fields and extensions	Value
Certificates revoked	List of certificates revoked, containing at least the serial number and revocation date for each entry

7.3. OCSP PROFILE

385. The profile for the Online Certificate Status Protocol (OCSP) messages issued by the FNMT-RCM conform to the specifications contained in the IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile.

7.3.1. Version number

386. *Certificates* used by the *Certificate validity status information and consultation service*, via OCSP, comply with the X.509 version 3 standard.

7.3.2. OCSP extensions

387. The OCSP responses of the *Certificate status information service* on the validity status of the certificates include, for requests that request it, the global extension "nonce", which is used to link a request with a response, so that it is can prevent repetition attacks.

388. Additionally, the extension "Extended Revoked Definition" is included in the cases in which is consulted the status of a *Certificate* that the CA acknowledges as not issued. In this way, the service responds to the query of certificates not issued by the CA as revoked *Certificate*.

8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS

389. The system for issuing *Website authentication certificates* is submitted to an audit process annually 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”.

390. In addition, the *Certificates* that are deemed to be *qualified Certificates* are therefore audited to ensure compliance with the requirements set in European standard ETSI IN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”.

391. Independent auditor annually assess the CA’s compliance to the stated requirements and practices of this CPS, and/or the CAB Forum’s Baseline Requirements and EV Guidelines.

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

- Audit of the Information Security Management System in accordance with UNE-ISO / IEC 27001 “Information Security Management Systems. Requirements”.

- Audit as ruled in the National Security Scheme (Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration).
- Audit of the Quality Management System according to ISO 9001.
- Audit of the Social Responsibility Management System in correspondence with IQNet SR10.
- Audit of the Business Continuity Plan according to ISO 22301.
- Audit in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/, and Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (RGPD / LOPD-GDD).

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

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

394. The ETSI audits detailed in the previous section are carried out annually. The corresponding audit plans will be prepared periodically.

395. For *Certificates* that are considered to be qualified (*Electronic Venue certificate EV, EV Certificate and SAN EV Certificate,* the audit additionally guarantees compliance with the requirements of the European standards ETSI EN 319 411-2 “Requirements for trust service providers issuing EU certificates” and ETSI EN 319 412- 4 “Certificate profile for web site certificates”.

396. The frequency of the rest of the additional audits will be in accordance with the provisions of the corresponding current regulations and with the CAB Forum’s Baseline Requirements and EV Guidelines.

8.2. IDENTITY / QUALIFICATIONS OF ASSESSOR

397. The auditor that verifies and checks the proper performance of the FNMT-RCM *Trust Service Provider* must be a person or professional with sufficient official qualifications and suitable experience in the matter to be audited, pursuant to legislation in force from time to time. The auditor must at least be accredited under the European standard ETSI EN 319 403.

398. The audit report issued will identify the auditors. The audit report will be signed by the auditors and the head of the entity audited.

8.3. ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

399. These audits may be entrusted to external Audit Firms, to qualified internal personnel (as per applicable legislation) or both. In the case of internal personnel and depending on the criticality of the area to be audited, the level of independence of the personnel involved and their experience will be specified in each case, based on functional independence parameters.

400. Where the audits are performed by personnel external to the FNMT-RCM, the necessary measures and controls are put in place to regulate audit requirements, scope, access to sensitive information and other agreements on *Confidentiality* and responsibility for assets.

401. In external audits, the auditor and the audit firm will never have any employment, commercial or other relationship of any kind with the FNMT-RCM or with the party requesting the audit. The requested audit must always be carried out by an independent professional.

8.4. TOPICS COVERED BY ASSESSMENT

402. The following controls will be carried out:

- Internal network security controls.
- Internal contingency plan controls and tests.
- Internal Quality and Security controls.
- Extraordinary controls: Where required in the circumstances, at the FNMT-RCM's discretion.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

403. All weaknesses detected in the audit will give rise to the relevant corrective actions. The corrective action plan will be drawn up as soon as possible and will be kept with the audit report for inspection and follow-up in subsequent audits.

404. Should the weakness entail a serious risk to system security, *Certificates* or *Revocation Lists*, *Signature creation or verification data* or any document or piece of data deemed to be *Confidential* in this document, of the *Subscribers* or of the *Trust Service Provider*, the FNMT-RCM will act as described in the *Continuity Plan* so as to safeguard security in all the infrastructure.

405. The FNMT-RCM will also act diligently to correct the error or defect detected as soon as possible.

8.6. COMMUNICATION OF RESULTS

406. The competent administrative authorities or courts of law may request the audit reports to verify the proper functioning of the *Trust Service Provider*.

407. The FNMT-RCM will make its Audit Report publicly available no later than three months after the end of the audit period.

8.7. SELF-AUDIT

408. Additionally, the FNMT-RCM performs internal audits to self-assess compliance with its *Certification Policies*, *Certification Practices Statement*, applicable regulations, and the requirements established by the CA / Browser forum and to control the quality of the provision of services. These internal audits are carried out at least quarterly, taking a randomly selected

sample of at least 3% of the *Certificates* issued during the period that begins immediately after the previous self-assessment sample.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

409. The FNMT-RCM will apply to the Public Administrations the fees approved by the relevant Under-Secretary's Office for the provision of certification services or, failing this, the fees stated in the specific management agreement or commission.

410. The fees applicable to the private sector are governed by the agreement for the provision of certification services. Additionally, the FNMT-RCM may determine the fees and payment methods deemed fit from time to time. The price and terms of payment may be consulted in the FNMT-RCM website or will be provided by the relevant commercial area in response to requests sent to the e-mail address comercial.ceres@fnmt.es.

9.1.1. Certificate issuance or renewal fees

411. Fees applicable to the issuance or renewal of *Certificates* will be determined as stipulated in paragraph "9.1 Fees" of this document.

9.1.2. Certificate access fees

412. Not stipulated.

9.1.3. Revocation or status information access fees

413. The FNMT-RCM provides Certificate status information services free of charge by means of the OCSP protocol.

9.1.4. Fees for other services

414. Fees applicable to other services will be determined as stipulated in paragraph "9.1 Fees" of this document.

9.1.5. Refund policy

415. The FNMT - RCM has a return policy that allows the refund request within the established termination period, accepting that this fact will lead to the automatic revocation of the certificate. The procedure is published at the Website of the FNMT – RCM.

9.2. FINANCIAL RESPONSIBILITY.

416. The FNMT-RCM has the necessary human, material and financial resources to reasonably cover the application requirements of each declared policy. As a governmental Entity attached to the Ministry of Finance, in patrimonial matters, Law 33/2003, of November 3, of the

Patrimony of Public Administrations and its Statute (currently approved by Royal Decree 1114 / 1999, of June 25), in terms of adequacy, sufficiency, effective application, identification and control of their assets to serve the public service to which they are intended. Additionally, although the national regulations on the provision of trust services establish the exemption of the FNMT-RCM, due to its governmental nature, about the constitution of a civil liability insurance to exercise as a qualified trust services provider, this Entity possess, voluntarily, said insurance, as defined in the following section.

9.2.1. Insurance coverage

417. The FNMT-RCM, as a *Trust Service Provider*, as well as a Spanish government body, has third-party liability insurance covering its *Trust Service Provider* activities, with a coverage limit of above €4,000,000.

9.2.2. Other assets

418. No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

419. No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of confidential information

420. The FNMT-RCM has internal regulations developing the Entity's "Information Security Management System", in which information classification and processing is defined.

9.3.2. Information not within the scope of confidential information

421. The following information is not deemed to be confidential:

- Information contained in documents classified as "Public".
- Information contained in *Certificates*.
- *Certificate* Revocation Lists (CRLs) and information contained in replies issued by the *Certificate validity status information and consultation service*.

422. Any information that must be published by law.

9.3.3. Responsibility to protect confidential information

423. Confidential information relating to the *Trust Service Provider*'s activities will be disclosed subject to prevailing legislation. Information on the activity relating to *Certificate* issuance and management may be disclosed, if requested, as evidence of certification in a court proceeding, even without the *Certificate Holder*'s consent, provided this complies with applicable legislation.

9.4. PRIVACY OF PERSONAL INFORMATION

424. The FNMT-RCM publishes the records of processing activities and the rest of the information related to personal data, for consultation by interested parties, at the following website:

425. http://www.fnmt.es/politica-privacidad

9.4.1. Privacy plan

426. The processing of personal data carried out by the FNMT-RCM aligns with the provisions of 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 (General Data Protection Regulation, hereinafter GDPR) as well as the requirements that are application by specific national regulations in this matter.

9.4.2. Information treated as private

427. The FNMT-RCM considers as private all personal information about natural persons using trust services not incorporated in the certificates and in the mechanisms used by the *Certificate status information and consultation service*.

428. In any case, all personal information collected in the processes of requesting, renewing and revoking electronic *Certificates* (with the exception indicated in the following section), private keys that are in possession of the Trust Service Provider, as well as all that clearly identified as such, is considered private information.

429. The FNMT-RCM applies the appropriate safeguards to protect private information.

9.4.3. Information not deemed private

430. The information incorporated into the electronic *Certificates*, the information regarding the status of the *Certificates*, the date of beginning of that state (active, revoked, expired ...), as well as the reason that caused the status change, is not considered private information. Therefore, electronic Certificates, Revocation Certificate Lists and any content thereof are not considered private information.

9.4.4. Responsibility to protect private information

431. The FNMT-RCM adopts the required security measures in accordance with the GDPR regarding the access and treatment it performs on the personal data of applicants and subscribers of the *Certificates*.

432. Technical and organizational measures shall be established taking into account the cost of the technique, the costs of application, as well as the nature, scope, context and purposes of the treatment and the risk to the rights and freedoms of individuals.

9.4.4.1 Data Protection Officer

433. The GDPR establishes the obligation to designate a Data Protection Officer (DPO) to any authority or body of the public sector that carries out the processing of personal data. The contact data of the DPO of the FNMT-RCM are published on the website referenced in the first point of this section "9.4 Personal data protection". These contact details include the email address to which the interested parties can address all questions relating to the processing of their personal data and the exercise of their rights, in accordance with article 38.4 of the GDPR.

9.4.4.2 Records of processing activities

434. The FNMT-RCM possess records of processing activities carried out under its responsibility, as the "management of the PKI", related to the activity carried out by this Entity as a Trust Services Provider. These records includes, for each processing identified, the following information:

a) Purpose
b) Responsible entity
c) Categories of personal data
d) Who provides the data
e) Who is affected by personal data
f) Who are the people in charge of the treatment
g) Data communications
h) International data transfers
i) Cancellation period
j) Security measures

435. The document of records of processing activities can be consulted on the website referenced in the first point of this section "9.4 Personal data protection".

9.4.4.3 Subject's rights

436. Subjects can exercise the right of access, the right to rectification, to erasure, to restriction of processing, to data portability as well as the right to object to processing and not to be subject to a decision based solely on automated processing, in accordance with the provisions of articles 15 to 22 of the GDPR, by contacting the person responsible for processing electronically, through of the electronic headquarters of the FNMT-RCM, or in person through the General Registry of this Entity.

9.4.4.4 Cooperation with the Authorities

437. The FNMT-RCM will cooperate with the Spanish Data Protection Agency when required.

9.4.4.5 Notification of personal data breach

438. The FNMT-RCM shall notify to the Spanish Data Protection Agency of any personal data breach, without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

439. In cases where the personal data breach result in a high risk to the rights or freedoms of data subjects, the notification to the Spanish Data Protection Agency will be complemented by a notification addressed to the subjects, in order to allow them to adopt measures to protect themselves from its consequences.

9.4.5. Notice and consent to use private information

440. The obtaining of private information from individuals in the processes linked to the life cycle of the *Certificates* (application, accreditation of identity, renewal, revocation ...) will be carried out, in any case, after obtaining the consent of the subject. unambiguously, that is, through a manifestation of the subject or through clear affirmative action.

9.4.6. Disclosure pursuant to judicial or administrative process

441. The FNMT-RCM shall not disclose personal data, unless requested by the administrative or judicial authorities.

9.4.7. Other information disclosure circumstances

442. No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

443. The FNMT-RCM has exclusive ownership of all rights, including exploitation rights, to the secure *Directory* of *Certificates*, *Revocation Lists*, *Certificate* status information services and *Time stamping* services, pursuant to the revised Intellectual Property Law introduced by Royal Decree-Law 1/1996 (12 April) (Intellectual Property Law), including the *sui generis* right recognised in Article 133 of that Law. Consequently, access to the secure *Certificate Directories* is permitted for authorised members of the *Electronic Community*, while any reproduction, public disclosure, distribution, transformation or reorganisation is prohibited, unless specifically authorised by the FNMT-RCM or by the Law. The extraction and/or reuse of all or a substantial part of the content, whether from a quantitative or qualitative perspective, is also prohibited, as is repeated or systematic extraction and/or reuse.

444. Access to the *Time stamping* services will be restricted as stipulated in the specific policies and practices governing those services.

445. The FNMT-RCM holds all rights, title and interest to all intellectual and industrial property and knowledge related to this document, the services provided and the computer programs or hardware used to provide them. Any other use other than viewing, including the reproduction, redistribution and / or modification of this document, is prohibited without the express authorization of the FNMT-RCM.

446. The *OID* used in the *Certificates* issued, in *Certificates* employed to provide the services, in *Electronic time stamps* and to store certain objects in the *Directory* are owned by the FNMT-RCM and have been registered at the IANA (Internet Assigned Number Authority), under iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA-Registered Private Enterprises), the number 1.3.6.1.4.1.5734 having been assigned (FABRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA). This may be consulted and verified at:

http://www.iana.org/assignments/enterprise-numbers

447. Unless a specific agreement is entered into with the FNMT-RCM, the total or partial use of any of the *OID*s assigned to the FNMT-RCM is prohibited, barring the specific needs for which they were included in the *Certificate* or in the *Directory*.

448. Reproduction or copying is prohibited, even for private use of information that may be deemed Software or Databases pursuant to prevailing intellectual property legislation, as well as public disclosure or disclosure to third parties.

449. All extraction and/or reuse of all or a substantial part of the content or databases made available by the FNMT-RCM to *Subscribers* or *User entities* is prohibited.

9.6. REPRESENTATION AND WARRANTIES

9.6.1. CA representations and warranties

450. The obligations and responsibilities of the FNMT-RCM, as a *Trust service provider*, of the *Certificate Subscriber,* and, as applicable, with trusting third parties, determined mainly by the document on the terms and conditions of use contained in the *Certificate* issuance agreement and, secondarily, by this *Certification Practices and Policies Statement.*

451. The FNMT – RCM complies with all requirements contained in the technical specifications of the ETSI EN 319 411 standard for the issuance of Certificates and undertakes to continue complying with said regulation or those that replace it.

452. The FNMT-RCM issues the *Website authentication certificate* in accordance with the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", established by the entity CA/Browser forum, which may be consulted at the following address: https://cabforum.org/ Likewise, it will adapt its issuance practices for these *Certificates* to the version of the aforementioned requirements currently in effect. In the event of any inconsistency between this *CPS* and the aforementioned version, said requirements shall prevail over those contained in this document.

453. In addition, the FNMT-RCM undertakes to comply, with regard to the issue of EV Certificates (*Electronic Venue certificate EV, EV Certificate and SAN EV Certificate),* all requirements established by the entity CA/Browser for these types of Certificates (EV SSL Certificate Guidelines), and which can be consulted at https://cabforum.org/extended-validation/. In the event of any inconsistency between this *CPS* and the aforementioned version, said requirements shall prevail over those contained in this document.

454. Without prejudice to any of the provisions contained in any the regulations applicable to these types of *Certificates*, as well as the obligations described in the corresponding section of this document, the *Trust Service Provider* undertakes to:

455. Prior to *Certificate* issuance

- Verify the identity and personal circumstances of the *Applicant* for the *Certificate* and of the *Subscriber* and/or their *Representative,* and collect their declaration that the *Applicant* is authorised by the *Subscriber* to make such request.

  The identification will be made through verified *Certificates* with electronic signature accepted during the FNMT-RCM processes.

- Verify all data related to the legal personality of the *Subscriber* and regarding legal capacity of the *Representative d*uring the registration process. All these checks will be carried out as per the provisions of the *Special Certification Practices Statement* expressed in this document, and in accordance with the registration protocols and procedures of the FNMT-RCM.

  The FNMT-RCM may perform verifications with the involvement of third parties holding notarised powers of representation, or public or private registries as a part of the processes undertaken to verify the aforementioned aspects.

- Verify that all the information contained in the *Certificate* application matches the information provided by the *Applicant*.

- Verify that the *Applicant* is in possession of the *Private Key* associated with the *Public Key* that is included in the Certificate to be issued.

- Ensure that the procedures followed guarantee that the *Private Keys* corresponding to the *Website authentication certificates* are generated without any copies being made, or any storage of them being performed by FNMT-RCM.

- Perform the communication of information to the *Subscriber*, *Representative* and *Applicant* in such a manner that its *Confidentiality* is protected.

- Make available to the *Applicant, Subscriber, Representative* and any other interested parties (http://www.ceres.fnmt.es) the *Declaration of Certification Practices* and how much information is relevant for the development of the procedures related to the life cycle of the *Certificates* object of this *Special Certification Policy and Practices Statement* in accordance with applicable regulations.

9.6.2. RA representations and warranties

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

457. The RA, through the Registry Area of the FNMT-RCM, has the following obligations:

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

- In particular, to verify the identity, and any personal data that may be relevant for the specified purpose, of *Applicants* for *Certificates*, *Subscribers* and their

Representatives, using any of the methods permitted under the Law, and in accordance, in general terms, with the provisions contained in this document.

- Verify that the ownership of the domain name corresponds to the identity of the *Subscriber* or, if applicable, obtain authorisation from the latter, which will be associated with the *Website authentication certificate*, by any means at its disposal that would reasonably allow it to believe such ownership, in accordance with the state of the art.
- Expressly obtain the statement of the *Subscriber* in relation to the ownership of the domain of the *Website authentication certificate*, stating that it has sole decision-making power over it.
- Preserve all information and documentation relating to *Certificates,* maintaining all application, renewal or revocation data for fifteen (15) years.
- Handle the receipt and management of applications and the issuance contracts (pdf form) sent to *Certificate Subscribers.*
- Diligently check the causes for revocation that could affect the validity of *Certificates*.

9.6.3. Subscriber representations and warranties

458. The Applicant will be answerable for the truth of the information submitted during Certificate application and for the Certificate application to be made from equipment or a device that he or she may use to a high degree of trust under his or her exclusive control.

459. The Applicant will hold the FNMT-RCM harmless from and undertake defence at its own cost against any action that may be initiated against the latter entity as a result of the falseness of the information supplied in the Certificate issuance procedure or from any damage that the FNMT-RCM may incur as a result of an act or omission by the Applicant.

460. The *Subscriber* must fulfil security regulations related to the custody and use of information guaranteeing access to his or her *Private keys*.

461. The FNMT-RCM, in its activities as a *Trust Service Provider*, where permitted, envisaged or required by prevailing legislation, may obtain the e-mail address, mobile telephone number for the receipt of text messages and address of the *Subscribers* in contracts submitted to *Applicants* for signing, before issuing a *Certificate* or contracting a specific service.

462. This information is included in order to provide the trust services of which the said *Subscribers* are users and/or to notify events of interest to the *Subscriber* related to the FNMT-RCM's services and the *Certificates*, particularly those related to the revocation and suspension of *Certificates* or the termination of any agreements between the FNMT-RCM and the *Subscribers*. Additionally, the said information will be used as a communication channel to cover any need in the event of a disaster contingency that might disable the FNMT-RCM.

463. The *Applicant* and, subsequently, the *Subscriber* will be responsible for keeping the information up to date and correct.*Subscribers* must have control of the website domain name

included in said *Certificates* and maintain all associated *Private keys* under their exclusive use.

464. The *Applicant* and the *Subscriber* of the *Certificates* issued under this *DPP* have the obligation to:

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

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

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

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

468. With regard to *Electronic Venue certificate EV*, public entity *Subscribers,* represented through various authorised bodies, acting through the *Registry Operations Manager* for the issuance of these types of Certificates, must:

- Not to register or process requests for *Electronic Venue certificate EV* by personnel who render their services in an entity other than that represented as the *Registry Office*, unless expressly authorised by another entity.
- Not to register or process requests for *Certificates* issued under this policy and whose *Subscriber* corresponds to a public entity over which it has no powers, or does not have powers to act as the *Registry Office.*
- Not perform registrations or process requests for *Certificates* issued under this policy and whose *Subscriber* does not correspond to the ownership of the e-mail address through which the *Website* contained in the *Certificate* that is the subject of the request will be accessed.
- Not to register or process requests for *Certificates* issued under this policy and whose *Applicant* corresponds to an individual who does not provide services at the entity of the *Subscriber* of the *Certificate* and/or has not been authorised by the person acting as representative of the Public Entity for the management and administration of the electronic address through which the *Website* which will identify the Certificate object of the application is accessed.
- Reliably verify the identification and authorisation data of the *Certificate Subscriber* (the Entity that owns the *Website* and the e-mail address, domain or URL through which such Site is accessed) and the *Applican*t (the individual with sufficient powers to request an *Electronic Venue certificate EV*) for the *Certificate,* and verify that it matches with the owner and all contacts contained in the corresponding databases, for the management and administration of the e-mail address through which the *Website* identified in the *Certificate* will be accessed.
- To request the revocation of the *Electronic Venue certificate EV* issued under this policy when any of the data referred to the Subscriber or to the electronic address included in the *Certificate* is incorrect, inaccurate, or has changed with respect to that which is recorded in the *Certificate*, or does not correspond to the owner and contacts established in the corresponding databases for the management and administration of the e-mail address referenced in the *Certificate* subject to the revocation.

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

9.6.4. Relying party representations and warranties

470. It will be the responsibility of the User Entity and of the trusting third parties who use the Certificates to verify and check the status of said Certificates, in no case acting to assume the validity of the Certificates without these verifications.

471. Should the circumstances require additional guarantees, the User entity must obtain them in order for trust to be reasonable.

472. Moreover, the User entity will be responsible for observing the provisions of the Certification Practices Statement and any future amendments to it, paying particular attention to the stipulated restrictions on the use of Certificates in this Certification Policy.

9.6.5. Representations and warranties of other participants

473. Not stipulated.

9.7. DISCLAIMERS OF WARRANTIES

474. Not stipulated.

9.8. LIMITATIONS OF LIABILITY

475. The FNMT-RCM will only be answerable for the correct personal identification of the *Applicant* and future *Holder*, and for including these data in a *Certificate*. In order for the guarantees, obligations and responsibilities to be applicable, the event must have taken place within the scope of the *Electronic Community*.

476. The FNMT-RCM will only be answerable for weaknesses in the procedures pertaining to its own activities as a *Trust Service Provider* and in accordance with these *Certification Policies* or the Law. It will not in any circumstances be liable for actions or losses that may be incurred by *Holders*, *Subscribers*, *User entities* or third parties which are not due to errors attributable to the FNMT-RCM in the above-mentioned *Certificate* issuance and/or management procedures.

477. The FNMT-RCM will not be liable for force majeure events, terrorist attacks, wildcat strikes or actions constituting offences or misdemeanours that affect its facilities in which the services are provided, unless the Entity is guilty of serious negligence. In any event, the FNMT-RCM may include disclaimers in the relevant contracts and/or agreements. In any case, the amount of damages that the FNMT-RCM would be required to pay to affected third parties and/or members of the *Electronic community* as a result of a court order, in the absence of specific provisions of contracts or agreements, is limited to a maximum of SIX THOUSAND EUROS (€6,000).

478. The FNMT-RCM will not be answerable to persons whose behaviour in the use of the *Certificates* has been negligent; for these purposes, and in any event, negligence will be regarded as the failure to comply with the provisions of this *Certification Practices and Policies Statement* and, in particular, the provisions of the sections that refer to the parties' obligations and liability.

479. The FNMT-RCM will not be liable for any software that it has not provided directly. Nonetheless, the FNMT-RCM will put in place adequate measures to protect its systems against *Malicious software (Malware)* and will diligently keep them up to date to cooperate with users in the avoidance of the damage that such software may cause.

480. The FNMT-RCM does not guarantee the cryptographic algorithms and will not be liable for damage caused by successful external attacks on the cryptographic algorithms used, provided it acted with due diligence based on the current state of technology and in accordance with this *Certification Practices and Policies Statement* and the Law.

481. The FNMT-RCM in the provision of its service as a Time Stamping Authority, shall not be held responsible for any damage or harm and/or defective operations that the Electronic Time Stamps that it issues cause as a result of the uses that are made of them, either due to the fault of interested parties or defects in the original data.

482. The FNMT-RCM in the provision of its service as a Time Stamping Authority, shall not be liable to anyone whose behaviour when using the Qualified Time Stamping Service and/or the Electronic Time Stamps themselves is negligent. For these purposes, and in all cases, failure to observe the provisions established in these Policies and Practices for the Qualified Time Stamping Service, in the [TSPS] and, in particular, the provisions in the sections relating to the obligations and responsibilities of the parties, shall be deemed to constitute negligence

483. The FNMT-RCM in the provision of its service as a Time Stamping Authority, shall not be liable in the event of unforeseen circumstances, force majeure, terrorist attacks, wildcat strikes, or in the case of events involving actions that constitute a crime or failure that affects the underlying infrastructure, except in the event that the entity itself committed a serious breach. In any case, in the corresponding contracts and/or agreements, the FNMT-RCM may establish additional liability limitation clauses to those reflected in this document.

484. The FNMT-RCM in the provision of its service as a Time Stamping Authority, shall not be responsible for any software that it has not supplied directly.

485. The FNMT-RCM does not guarantee the cryptographic algorithms and shall not be held liable for any damage caused by successful external attacks on the cryptographic algorithms used, provided it maintains due care over them, in accordance with the current status of the technique, and acts in accordance with the provisions of the applicable Policies and Practices for Trusted Services and Electronic Certifications and the Law.

9.9. INDEMNITIES

486. The FNMT-RCM may include indemnity clauses in the legal instruments linking it to the *Holder* for the infringement of the latter's obligations or of applicable legislation. In this respect, see also point "9.6 Obligations and guarantees" and "9.8. Limitations of liability".

9.9.1. CA indemnity

487. Not stipulated.

9.9.2. Subscribers indemnity

488. Not stipulated.

9.9.3. Relying parties indemnity

489. Not stipulated.

9.10. TERM AND TERMINATION

9.10.1. Term

490. This *Certification Practices and Policies Statement* will come into force when it is published.

9.10.2. Termination

491. This *Certification Practices and Policies Statement* will be terminated when a new version of the document is published. The new version will entirely supersede the previous document. The FNMT- RCM undertakes to subject the said Statement to an annual review process.

9.10.3. Effects of termination and survival

492. For valid *Certificates* issued under a previous *Certification Practices* and *Policies Statement*, the new version will prevail over the previous version in all matters that do not conflict.

9.11. INDIVIDUAL NOTICES AND COMMUNICATION WITH PARTICIPANTS

493. The FNMT-RCM, in its activities as a *Trust Service Provider*, where permitted, envisaged or required by prevailing legislation, may obtain the e-mail address, mobile telephone number for the receipt of text messages and/or address of the *Subscribers* during the application process and before issuing a *Certificate*.

494. This information is included in order to provide the trust services of which the said *Subscribers* are users and/or to notify events of interest related to the FNMT-RCM's services, particularly those related to the revocation *Certificates* or the termination of any agreements between the FNMT-RCM and the *Subscribers*. Additionally, the said information will be used as a communication channel to cover any need in the event of a disaster contingency that might disable the FNMT-RCM.

495. The *Applicant* and, subsequently, the *Subscribers* will be responsible for keeping the information up to date and correct.

9.12. AMENDMENTS

9.12.1. Procedure for amendment

496. Amendments to this *Certification Practices and Policies Statement* will be approved by Ceres Department management and will be reflected in the relevant minutes of the Provider's Management Committee meetings, pursuant to the internal procedure approved in the document "Review and maintenance procedure for certification policies and the trust service practices statement".

9.12.2. Notification mechanism and period

497. Any amendment to this *Certification Practices and Policies Statement* will be immediately published in the URL where it may be accessed.

498. Should the amendments not entail significant changes to the parties' obligations and responsibilities or the modification of the service provision policies, the FNMT-RCM will not previously inform users and will simply post a new version of the statement in question on its website.

9.12.3. Circumstances under which an OID must be changed

499. Significant amendments to the terms and conditions of the services, obligations and responsibilities, or restrictions on use may give rise to a change to the service policy and identification (OID), as well as a new link to the new service policy statement. In this case, the FNMT-RCM may establish a mechanism for providing information on the proposed changes and, if applicable, gathering opinions from the affected parties.

9.13. DISPUTE RESOLUTION PROVISION

500. The FNMT-RCM will respond to any request, complaint or claim from its customers or third parties that place their trust in its trust services, pursuant to the protocols approved by the Entity through the internal procedure "Protocol for the management of corrective, preventive and improvement actions", "Protocol for the management of suggestions, complaints and claims" and "Protocol for the management of incidents". The contact data for such complaints or claims are provided in point "1.5.2 Contact details for this document".

9.14. GOVERNING LAW

501. The provision of trust services by the FNMT-RCM will be governed by the laws of Spain.

502. The following legislation is applicable to these trust service practices:

- Law 6/2020 (11 November) regulating certain aspects of electronic trust services.
- Law 39/2015 (1 October) on the Common Administrative Procedure for Public Administrations.
- Law 40/2015 (1 October) on the Public Sector.

- Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights.
- 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.
- Royal Decree 366/2007, of March 16, which establishes the conditions of accessibility and non-discrimination of persons with disabilities in their relations with the General State Administration.
- Royal Decree 505/2007, of April 20, which approves the basic conditions of accessibility and non-discrimination of persons with disabilities for the access and use of urbanized public spaces and buildings.

503. Additionally, the practices of the trust services provided by the FNMT-RCM follow the following standards:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.

504. In general, the members of the *Electronic Community* and *Users* of the FNMT-RCM's trust services accept that any lawsuit, discrepancy, matter or claim arising from the enforcement or interpretation of the *Trust Service and Electronic Certification Practices Policies and/or Declarations* or related to them directly or indirectly will be resolved in accordance with the provisions of the relevant contracts, general terms and conditions and/or commissions or agreements, in the terms stated in the Entity's Statute introduced under RD 1114/1999 (25 June) (Official State Gazette no. 161 of 7 July).

505. In the event that the contracts, general terms and conditions and/or commissions or agreements do not specify any conflict resolution arrangement, all the parties submit to the exclusive jurisdiction of Spanish courts in the city of Madrid.

506. In addition, mediation or arbitration procedures may be agreed, subject to the approval of the competent bodies of the FNMT-RCM, in accordance with applicable legislation.

9.15. COMPLIANCE WITH APPLICABLE LAW

507. The FNMT-RCM expresses its commitment to comply with all regulations and the application requirements applicable for each type of *Website authentication certificate*, including the considerations established in section "1.5.4. DPC Approval Procedure" of this *CPS* document.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

508. The *Subscribers* and third parties placing their trust in the *Certificates* fully accept the content of this *Certification Practices and Policies Statement.*

9.16.2. Assignment

509. The FNMT-RCM will not be responsible for the lack of service or service anomalies, nor for any damage that may be caused directly or indirectly, when the failure or disaster is the result of force majeure causes, a terrorist attack, sabotage or wildcat strikes, all without affecting any actions necessary to correct and/or restore the service as soon as possible.

9.16.3. Severability

510. Not stipulated.

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

511. Not stipulated.

9.16.5. Force Majeure

512. Not stipulated.

9.17. OTHER PROVISIONS

513. The FNMT-RCM, as a *Trust Service Provider*, will provide services to all interested parties that request them on the terms stipulated in this document and the Policies, Practices and Issuance Laws applicable to the purpose of the application.

514. The FNMT-RCM's trust services, adequately used and combined, will allow *Users*, *Subscribers* and *Holders*, among others, to obtain information exchange security measures necessary for the identification, authentication, non-repudiation and confidentiality of the parties.

515. The FNMT-RCM manages its certification services and issues *Certificates* in accordance with the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", established by the entity CA/Browser forum, which may be consulted at the following address: https://cabforum.org/baseline-requirements-documents and in accordance with the latest version of the requirements defined by the entity CA / Browser forum in its "Guidelines for the Issuance and Management of Extended Validation Certificates" (which can be consulted at the address https://cabforum.org/extended-validation/).

516. The FNMT-RCM will review its certification policies and practices so that they remain in line with the said requirements. On publication of new versions of the requirements document and in the event of an inconsistency, the FNMT-RCM will act diligently to correct any departures or, if appropriate, include a notification in this document on infringements committed.

517. In case of loss of the QSCD certification of any of the qualified signature / seal creation devices used by FNMT-RCM, as a Trusted Service Provider, appropriate measures will be taken to reduce the possible impact. The supervisory body will be informed about this and FNMT-RCM will stop the issuance of *Certificates* on those devices.

518. The organizational structure of the FNMT-RCM guarantees that the units related to the *Certificate* generation and revocation management are independent of other units for its decisions relating to the establishing, provisioning and maintaining and suspension of services in conformance with the applicable certificate policies. The document "CERES - Organización del Departamento" defines this organizational structure. Additionally, the legal nature of the FNMT-RCM, as a governmental entity attached to the General State Administration, guarantees that its senior executive, senior staff and staff in trusted roles are free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

519. The FNMT-RCM applies the principles of equal opportunities, non-discrimination and universal accessibility to its services, processes and procedures. The measures adopted reasonably comply with the basic criteria and conditions of accessibility and non-discrimination in accordance with the applicable regulations (see section "9.14 Applicable legislation"), with the aim of guaranteeing that users of trust services, in no case, suffer discrimination in the exercise of their rights and faculties due to reasons based on disability or advanced age. Additionally, the websites of the FNMT-RCM are subject to analysis in terms of compliance with accessibility requirements, such as the Accessibility Observatory of the Ministry of Finance.

520. The FNMT-RCM allows third parties to check and test all types of certificates issued. For this, it has a set of test certificates that can be requested through the email address in the section "1.5.2 Contact details".

APPENDIX I: FNMT-RCM "SERVIDORES SEGUROS" ROOT CERTIFICATE PROFILE

Field		Content	Critical ext.
1. Version		2	
2. Serial Number		Certificate Serial number.	
3. Signature Algorithm		ecdsa-with-SHA384 Keys: ECC P-384 bits	
4. Issuer Distinguish Name		Issuer Certificate (CA root)	
	4.1. Country	C=ES	
	4.2 Organization	O=FNMT-RCM	
	4.3 Organization Unit	OU=Ceres	
	4.4 OrganizationIddentifier	VATES- Q2826004J	
	4.5 CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS	
5. Validity		25 years	
6. Subject			
	6.1. Country	C=ES	
	6.2. Organization	O=FNMT-RCM	
	6.3. Organization Unit	OU=Ceres	
	6.4. OrganizationIddentifier	VATES- Q2826004J	
	6.5. CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS	
7. Subject Public Key Info		ECC P-384 bits	
8. Subject Key Identifier		CA Key Identifier. Means to identify certificates that contain a particular public key and facilitates the construction of certification routes.	
9. Key Usage		Allowed use of certified keys.	yes
	9.1. Digital Signature	0	
	9.2. Content Commitment	0	
	9.3. Key Encipherment	0	
	9.4. Data Encipherment	0	
	9.5. Key Agreement	0	
	9.6. Key Certificate Signature	1	
	9.7. CRL Signature	1	

Field		Content	Critical ext.
10. Basic Constraints			yes
	10.1. cA	Value TRUE (CA)	
	10.2. pathLenConstraint	None	