Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CERTIFICATION PRACTICES AND POLICIES STATEMENT ON QUALIFIED ELECTRONIC VENUE 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 Policy Statement on Qualified Electronic Venue Certificates, under the FNMT CA Root hierarchy.
1.1	30/05/2019	Update domain validation methods according to CA / Browser Forum Baseline Requeriments.
1.2	18/11/2019	Inclusion of explicit indication of Issuer Domain Names that the CA recognises in CAA "issue"
1.3	12/12/2019	General review and improvement update
1.4	01/10/2020	Incorporation of the EKU "Client Authentication" to the website authentication certificates.
1.5	18/02/2021	Inclusion of the URL where the list of Incorporating Agencies or Registration Agencies was published
1.6	28/04/2021	Annual review and Mozilla Policy Review v2.7.1. - Information is included in relation to the methods to communicate a compromise of keys.

Reference: DPC/DPCsede_0106/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, 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 *Electronic 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.

6. This document also includes, either directly or with references to the *General Statement of Practice of Trust Services and Electronic Certification of the FNMT-RCM* on which this Statement depends, details concerning the liability regime applicable to the users of and/or persons that place their trust in the services referred to in the previous paragraph, security controls applied to procedures and facilities, where they may be disclosed without harming their effectiveness, and secrecy and confidentiality rules, as well as matters related to the ownership of goods and assets, personal data protection and other informative aspects that should be made available to the general public.

1.2. DOCUMENT NAME AND IDENTIFICATION

7. This document is called "*Certification Practices and Policies Statement on Qualified Electronic Venue Authentication Certificates*", and will hereafter be cited in this document and with the scope described therein as *"Special Certification Practices and Policies Statement*" or by its acronym "DPPP".

8. These *Certification Policies and Special Certification Practices* form part of the *Certification Practices Statement* and shall take priority over the provisions of the *General Statement of Trust Services Practices and Electronic Certification.*

9. In the event that there is any contradiction between this document and the provisions of the *General Statement of Trusts and Electronic Certification Practice*s, preference shall be given to that which is included here.

10. This *Certification Policy* has the following identification:

Type of policy indicated: QCP-web. OID: 0.4.0.194112.1.4

Version: 1.6

Issue date: 28/04/2021

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

Relate DPC: General Statement on FNMT-RCM Practices of Trust Services and Electronic Certification

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

11. 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). When said website is an *Electronic Venue*, said *Website authentication certificate* is called the *Electronic Venue certificate.*

12. Within the scope of this DPPP, the FNMT-RCM issues the following types of *Website Authentication Certificates*, considered to be qualified certificates[1], whose description of which is found in section "1.6.1 Definitions" of this document:

[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.

Type of *Certificate*	**Policy Reference/OID** [2]
Electronic Venue certificate	1.3.6.1.4.1.5734.3.3.12.1

1.3. PARTIES

13. 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

14. The FNMT-RCM is the *Certification Authority* that issues the electronic Certificates object of the present DPPP. *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 - FNMT-RCM CA ROOT Certificate

FNMT-RCM CA ROOT Certificate	
Subject	OU = AC ROOT FNMT-RCM, O = FNMT-RCM, C = ES
Issuer	OU = AC ROOT FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07

[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.

FNMT-RCM CA ROOT Certificate	
Validity	Not before: 29 October 2008. Not after: 1 January 2030
Public key length	RSA 4096 bits
Signature algorithm	RSA – SHA256
Key identifier	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

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

Table 2 – "Public Administration" subordinate CA certificate

"Public Administration" subordinate CA certificate	
Subject	CN = CA Public Administration, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES
Issuer	OU = AC ROOT FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	02
Validity	Not before: 21 May 2010. Not after: 21 May 2022
Public key length	RSA 2048 bits
Signature algorithm	RSA – SHA256
Key identifier	14 11 E2 B5 2B B9 8C 98 AD 68 D3 31 54 40 E4 58 5F 03 1B 7D

15. The subordinate Certification authority "Public Administration CA" issues, the *Electronic Venue certificate* under these DPPPs.

1.3.2. Registration Authority

16. 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.*

1.3.3. Certificate subscribers

17. *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.*

18. For *Electronic Venue certificates,* the *Subscriber* is always a government administration or organisation, public body or state-owned entity that has control of the domain name of the *Electronic Venue*.

1.3.4. Trusting parties

19. 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

20. Not stipulated.

1.4. USE OF CERTIFICATES

1.4.1. Permitted uses of certificates

21. 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.

22. 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.

23. All Certificates 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 July 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 set out in the European standards ETSI EN 319 411-2 “Requirements for trust service providers issuing EU-certified certificates” and ETSI EN 319 412-4 “Certificate profile for web site certificates”.

1.4.2. Restrictions on the use of certificates

24. 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 *Special 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.*

25. 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. Responsible entity

26. 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.*

1.5.2. Contact details

27. 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

28. 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. Parties responsible for adapting the General Statement

29. 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

30. 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.

31. The FNMT-RCM will review 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.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

32. For the purposes of this *DPPP*, when the terms begin with a capital letter and are in italics, the definitions expressed in the DGPC and, in particular, the following section shall be taken into account in general:

- *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*: 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: Website authentication 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 System of the Public Sector.
- *Registry Operations Manager:* Individual appointed by the representative of the Public Administration, public body or law entity, to process the requests for *Electronic Venue certificates*.
- *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.*
- *Special Practices and Policies Statement (DPPP):* Private DPC 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.
- *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.
- *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. Currently, in Spain, this is the Ministry of the Economy and Business.
- *Trust Services Practices and Electronic Certification General Statement* (*DGPC*): A statement made available to the general public through electronic means and free of charge by the FNMT-RCM as a *Trust Service Provider*, in compliance 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.
- *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.

(The terms indicated in italics are defined in this document or in the General Statement of Trust Services Practices and Electronic Certification)

1.6.2. Acronyms

33. For the purposes of the provisions contained in this DPPP, 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

2.1. REPOSITORY

34. 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 CERTIFICATION INFORMATION

35. The information regarding the issuance of electronic *Certificates* subject to this DPPP 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.

36. 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. PUBLICATION FREQUENCY

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

38. Any amendment to the *Trust Services Practices and Electronic Certification General Statement* or to the *Specific Certification Policies and Practices* will be immediately published in the URL where they may be accessed.

39. The frequency of publication of CRLs is defined in paragraph "4.9.7. CRL generation frequency" of the DGPC.

2.4. REPOSITORY ACCESS CONTROL

40. 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. DENOMINATION

41. 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.

3.1.1. Name types

42. End-user electronic *Certificates* as covered in this *DPPP* 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).

3.1.2. Meaning of names

43. 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).

3.1.3. Pseudonyms

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

3.1.4. Rules used to interpret various name formats

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

3.1.5. Name uniqueness

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

3.1.6. Registered trademark recognition and authentication

47. Subscribers may not request Certificates with any content that infringes the intellectual property rights of a third party. Please see the corresponding section of the *DGPC.*

3.2. INITIAL VALIDATION OF IDENTITY

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 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/).

3.2.1. Methods to prove possession of the private key

49. 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 the organisation's identity

3.2.2.1 Identity

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

51. S*ubscribers* of the *Certificates* issued under these *DPPP's* are always spanish public entities in all cases. Therefore, the verification of its existence, of being legally recognised, active at the time of issuance of the *Certificate,* and formally registered, will be made by direct consultation of the RA of the FNMT-RCM of the records of public sector entities of the General Auditor of the State Administration, under the Ministry of Finance, or the records of the State Agency for Tax Administration.

52. 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).

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

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

3.2.2.2 DBA/Tradename

55. 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.

3.2.2.3 Verification of country

56. All *Certificates* issued under these *DPPPs* are issued to *Subscribers* who are Spanish public entities. The countryName is verified using any method in Section 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

57. 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".

58. 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. In order to do this, the FNMT-RCM consults the identity of the Subscriber's Representative 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.

59. 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

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

3.2.2.6 Wildcard domain validation

61. *Certificates* for wildcard domains are not issued under these policies

3.2.2.7 Data source accuracy

62. 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

63. 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 6844 and following the processing instructions set forth in RFC 6844 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 applicant's identity

64. The RA of the FNMT-RCM verifies that the *Subscriber's Representative* matches with the individual requesting a *Website authentication certificate*, by means of the electronic signature of the application form. The use of a qualified electronic signature *Certificate* guarantees the authenticity of your identity.

3.2.4. Non-verified subscriber information

65. 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. Verification of Authority

66. The RA of the FNMT-RCM verifies that the *Applicant* has sufficient representation capacity using the electronic signature of the application form, as described in section 3.2.3 of this DPPP, and also accepts the use of a qualified *Certificate,* further demonstrating that it has sufficient representation capacity to perform the request for the *Certificate.*

67. The validity of the evidence obtained as a result of the consultations carried out for the authentication of the identity of the Organisation and/or the authentication of the identity of the requesting natural person, according to sections 3.2.2 and 3.2.3 of this document, will be the validity of the *Certificate* to be issued, at a maximum. Therefore, if there is an active *Certificate* and the issuance of another *Certificate* of the same type and for the same *Subscriber* and domain name(s) is requested, it will not be necessary to obtain the aforementioned identification evidence from the subscribing organisation of the Certificate and/or of the identity of the requesting individual. For these purposes, it is emphasised that the maximum period of validity of the *Certificates* issued under these policies is 1 year.

3.2.6. Interoperation criteria

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

3.3. IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS

3.3.1. Identification and authentication for routine re-key

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

3.3.2. Identification and authentication for Re-key after revocation

70. The FNMTRCM do not renew Certificates that have been revoked. The process for the renewal 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

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

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATES APPLICATION

4.1.1. Who can submit a certificate applicacation

72. 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 *DPPP*.

4.1.2. Enrolment process and responsibilities

73. 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.

74. 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.

75. 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.

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

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

4.2. CERTIFICATION APPLICATION PROCEDURE

4.2.1. Performing identification and authentication functions

78. 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 *DPPP*.

79. 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.

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

81. 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 application

82. 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.

83. 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 *DPPP*, which will then result in the approval or rejection of the request in question.

84. 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.

85. 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.

86. 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.

87. The approval system for issuing *Website authentication certificates* requires the action of at least two individuals belonging to the RA of the FNMT-RCM with sufficient authorisation.

88. 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 6844 and following the processing instructions set forth in RFC 6844 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

89. 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.

90. 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

91. Once the application for the *Certificate* has been approved by the RA of the FNMT-RCM's, the system then performs certain checks, such as the size of the *Public key* generated, and proceeds to issue the *Certificate* according to the profile approved for each corresponding type of *Certificate.*

92. 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

93. 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

94. 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

95. 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

96. 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

97. The FNMT-RCM does not generate or store any *Private Keys* associated with the *Certificates* that are issued under this *Certification Policy.* The role of custodian and the holder of the keys of the *Certificate* corresponds to the *Registry Operations Manager.* 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. Relying party public key and certificate usage.

98. 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.

99. 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 *DPPP,* 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

100. 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. Under these *Certification Policies,* the FNMT-RCM does not renew *Certificates* keeping the same *Public key.*

4.7. CERTIFICATE RE-KEYS

101. The FNMT does not perform renewals of *Electronic Venue certificates.* 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

4.8. CERTIFICATE AMENDMENT

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

4.9. REVOCATION AND SUSPENSION OF CERTIFICATE

103. *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.

104. 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.*

105. 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 commitment of a *Private Key,* improper use of the *Certificates* or other types of fraud, compromise, misuse or inappropriate behaviour.

106. 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

107. 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

108. In addition to these provisions contained, in relation to the application for a *Certificate,* in cases where there is another in force in favour of the same domain and same *Subscriber*, 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 of 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 *DPPP* 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.*

109. 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.

110. 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.*

111. 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.

4.9.1.1 Reasons for Revoking a Subordinate CA Certificate

112. 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

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

114. In the case of an *Electronic site certificate*, the FNMT-RCM shall accept the authority and capacity of the *Applicant* for revocation 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.*

115. 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

116. 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

117. 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.

118. Additionally, the FNMT-RCM will revoke *Electronic Venue certificates* when the revocation request originates from a Registry Office designated by the Administration, using the following procedure:

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 *Electronic Venue* 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 *Electronic Venue 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 tot he 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 Electronic Venue 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.

119. 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

120. 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

121. All revocation requests for end entity Certificates, are processed within a maximum of 24 hours of receipt.

122. 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

123. 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 Seal 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

124. *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 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

125. *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 checking requirements

126. 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

127. 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/sealed.

4.9.11. Other forms of advertisements available

128. Not defined.

4.9.12. Special requirements related to key compromises

129. Please see the corresponding section of the DGPC.

4.9.13. Circumstances for suspension

130. The suspension of certificates is not covered.

4.9.14. Who can request suspension

131. The suspension of certificates is not covered.

4.9.15. Procedure for requesting suspension

132. The suspension of certificates is not covered.

4.9.16. Limits on the suspension period

133. The suspension of certificates is not covered.

4.10. CERTIFICATE STATUS SERVICES

134. 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/sealed using the *Signature/Seal Creation Data* of the FNMT-RCM, thus guaranteeing the integrity and authenticity of the information supplied on the revocation status of Certificates consulted.

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

136. 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.

4.10.1. Operational characteristics

137. Information regarding the validation of the electronic *Certificates* covered by this DPPP is accessible through the means described in the DGPC.

4.10.2. Service availability

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

139. 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

140. No stipulation.

4.11. END OF SUBSCRIPTION

141. 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

142. 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

143. Not stipulated.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

144. Please see the corresponding section of the DGPC.

5.1. PHYSICAL SECURITY CONTROLS

145. Please see the corresponding section of the DGPC.

5.1.1. Site location and construction

146. Please see the corresponding section of the DGPC.

5.1.2. Physical access

147. Please see the corresponding section of the DGPC.

5.1.3. Power and air conditioning

148. Please see the corresponding section of the DGPC.

5.1.4. Water exposures

149. Please see the corresponding section of the DGPC.

5.1.5. Fire prevention and protection

150. Please see the corresponding section of the DGPC.

5.1.6. Media storage

151. Please see the corresponding section of the DGPC.

5.1.7. Waste disposal

152. Please see the corresponding section of the DGPC.

5.1.8. Off-site backup

153. Please see the corresponding section of the DGPC.

5.2. PROCEDURE CONTROLS

154. Please see the corresponding section of the DGPC.

5.2.1. Trusted Roles

155. Please see the corresponding section of the DGPC.

5.2.2. Number of Individuals Required per Task

156. Please see the corresponding section of the DGPC.

5.2.3. Identification and Authentication for Trusted Roles

157. Please see the corresponding section of the DGPC.

5.2.4. Roles Requiring Separation of Duties

158. Please see the corresponding section of the DGPC.

5.3. PERSONNEL CONTROLS

159. Please see the corresponding section of the DGPC.

5.3.1. Qualifications, Experience, and Clearance Requirements

160. Please see the corresponding section of the DGPC.

5.3.2. Background Check Procedures

161. Please see the corresponding section of the DGPC.

5.3.3. Training Requirements and Procedures

162. Please see the corresponding section of the DGPC.

5.3.4. Retraining Frequency and Requirements

163. Please see the corresponding section of the DGPC.

5.3.5. Job Rotation Frequency and Sequence

164. Please see the corresponding section of the DGPC.

5.3.6. Sanctions for Unauthorized Actions

165. Please see the corresponding section of the DGPC.

5.3.7. Independent Contractor Controls

166. Please see the corresponding section of the DGPC.

5.3.8. Documentation Supplied to Personnel

167. Please see the corresponding section of the DGPC.

5.4. AUDIT PROCEDURES

168. Please see the corresponding section of the DGPC.

5.4.1. Types of Events Recorded

169. Please see the corresponding section of the DGPC.

5.4.2. Frequency for Processing and Archiving Audit Logs

170. Please see the corresponding section of the DGPC.

5.4.3. Retention Period for Audit Logs

171. Please see the corresponding section of the DGPC.

5.4.4. Protection of Audit Log

172. Please see the corresponding section of the DGPC.

5.4.5. Audit Log Backup Procedures

173. Please see the corresponding section of the DGPC.

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

174. Please see the corresponding section of the DGPC.

5.4.7. Notification to Event-Causing Subject

175. Please see the corresponding section of the DGPC.

5.4.8. Vulnerability Assessments

176. Please see the corresponding section of the DGPC.

5.5. LOG ARCHIVING

177. Please see the corresponding section of the DGPC.

5.5.1. Types of Records Archived

178. Please see the corresponding section of the DGPC.

5.5.2. Retention Period for Archive

179. Please see the corresponding section of the DGPC.

5.5.3. Protection of Archive

180. Please see the corresponding section of the DGPC.

5.5.4. Archive Backup Procedures

181. Please see the corresponding section of the DGPC.

5.5.5. Requirements for Time-stamping of Records

182. Please see the corresponding section of the DGPC.

5.5.6. Archive Collection System (internal or external)

183. Please see the corresponding section of the DGPC.

5.5.7. Procedures to Obtain and Verify Archive Information

184. Please see the corresponding section of the DGPC.

5.6. CHANGE OF CA KEYS

185. Please see the corresponding section of the DGPC.

5.7. INCIDENT AND VULNERABILITY MANAGEMENT

186. Please see the corresponding section of the DGPC.

5.7.1. Incident and Compromise Handling Procedures

187. Please see the corresponding section of the DGPC.

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

188. Please see the corresponding section of the DGPC.

5.7.3. Recovery Procedures After Key Compromise

189. Please see the corresponding section of the DGPC.

5.7.4. Business Continuity Capabilities after a Disaster

190. Please see the corresponding section of the DGPC.

5.8. DISCONTINUANCE OF THE TRUST SERVICE PROVIDER'S ACTIVITIES

191. Please see the corresponding section of the DGPC.

6. TECHNICAL SECURITY CONTROLS

192. Please see the corresponding section of the DGPC.

6.1. KEY GENERATION AND INSTALLATION

6.1.1. Key pair generation

6.1.1.1 CA Key Pair Generation

193. For more information regarding the *Keys* that the FNMT-RCM requires for the development of its activity as a *Trust Service Provider,* please see the corresponding section in the DGPC.

6.1.1.2 RA Key Pair Generation

194. No stipulation

6.1.1.3 Subscriber Key Pair Generation

195. 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

196. There is no generation nor deliver of the *Private key* to the *Holder.*

6.1.3. Public key delivery to to certificate issuer

197. 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's public key delivery to relying parties

198. 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

199. The algorithm and the key size used are the following:

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

- AC root FNMT: RSA 4096 bits.
- Subordinate CAs: RSA 2048 bits.
- *Website authentication certificate:* RSA 2048 bits.

6.1.6. Public key parameters generation and quality checking

201. 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)

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

203. The root *Certificate* of the CA has enabled the uses of Keys to sign/seal 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/seal end user *Certificates* (*Website authentication certificates*) and CRLs.

204. 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

205. Please see the corresponding section of the DGPC.

6.2.1. Cryptographic Module Standards and Controls

206. Please see the corresponding section of the DGPC.

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

207. Please see the corresponding section of the DGPC.

6.2.3. Private Key Escrow

208. Please see the corresponding section of the DGPC.

6.2.4. Private Key Backup

209. Please see the corresponding section of the DGPC.

6.2.5. Private Key Archival

210. Please see the corresponding section of the DGPC.

6.2.6. Private Key Transfer into or from a Cryptographic Module

211. Please see the corresponding section of the DGPC.

6.2.7. Private Key Storage on Cryptographic Module

212. Please see the corresponding section of the DGPC.

6.2.8. Activating Private Keys

213. Please see the corresponding section of the DGPC.

6.2.9. Deactivating Private Keys

214. Please see the corresponding section of the DGPC.

6.2.10. Destroying Private Keys

215. Please see the corresponding section of the DGPC.

6.2.11. Cryptographic Module Capabilities

216. Please see the corresponding section of the DGPC.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

217. 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

218. *Certificate* and associated *Key* operating periods are as indicated in section "1.3.1 Certification Authority" of this DPPP.

6.4. ACTIVATION DATA

219. Please see the corresponding section of the DGPC.

6.4.1. Activation data generation and installation

220. Please see the corresponding section of the DGPC.

6.4.2. Activation data protection

221. Please see the corresponding section of the DGPC.

6.4.3. Other aspects of activation data

222. Please see the corresponding section of the DGPC.

6.5. COMPUTER SECURITY CONTROLS

223. Please see the corresponding section of the *DGPC.*

6.5.1. Specific Computer Security Technical Requirements

224. Please see the corresponding section of the *DGPC.*

6.5.2. Computer Security Rating

225. Please see the corresponding section of the *DGPC.*

6.6. LIFE CYCLE TECHNICAL CONTROLS

226. Please see the corresponding section of the *DGPC.*

6.6.1. System development controls

227. Please see the corresponding section of the *DGPC.*

6.6.2. Security management controls

228. Please see the corresponding section of the *DGPC.*

6.6.3. Life cycle security controls

229. Please see the corresponding section of the *DGPC.*

6.7. NETWORK SECURITY CONTROLS

230. Please see the corresponding section of the *DGPC.*

6.8. TIME-STAMPING SOURCE

231. Please see the corresponding section of the *DGPC.*

7. CERTIFICATE, CRLS AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

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

233. The *Electronic Venue Certificate* contains the policy identifier EV 0.4.0.2042.1.4.

7.1.1. Version number

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

7.1.2. Certificate content and extensions; application of RFC 5280

235. The document describing the profiles of the *Website authentication certificates*, including all extensions, is published at http://www.cert.fnmt.es/dpcs/.

7.1.3. Algorithm object identifiers

236. The object identifier (OID) relating to the cryptographic algorithm used (Sha256withRsaEncryption) is 1.2.840.113549.1.1.11.

7.1.4. Name formats

237. *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

238. The subordinate CA certificates are not technically constrained.

7.1.6. Certificate policy object identifier

239. 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

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

7.1.8. Policy qualifiers syntax and semantics

241. 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

242. 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

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

7.2.2. CRL and CRL entry extensions

244. The CRL profile has the following structure:

Table 3 – CRL profile

Fields and extensions	Value
Version	V2
Signature algorithm	Sha256WithRSAEncryption

Fields and extensions	Value
CRL number	Incremental value
Issuer	Issuer DN
Issue date	UTC issuance time.
Date of next upgrade	Issuance date + 24 hours
Authority key identifier	Issuer key hash
ExpiredCertsOnCRL	NotBefore de la CA
Distribution point	URLs of distribution point & CRL scope
Certificates revoked	List of certificates revoked, containing at least the serial number and revocation date for each entry

7.3. OCSP PROFILE

245. *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

246. *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

247. Please see the corresponding section of the *DGPC.*

8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS

248. 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”.

249. In addition, these *Certificates* are considered to be qualified, so 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".

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

250. The audits detailed in the previous section are carried out annually.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

251. Please see the corresponding section of the *DGPC.*

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

252. Please see the corresponding section of the *DGPC.*

8.4. TOPICS COVERED BY ASSESSMENT

253. Please see the corresponding section of the *DGPC.*

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

254. Please see the corresponding section of the *DGPC.*

8.6. COMMUNICATION OF RESULTS

255. Please see the corresponding section of the *DGPC.*

8.7. SELF-AUDIT

256. Please see the corresponding section of the *DGPC.*

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

257. Please see the corresponding section of the *DGPC.*

9.1.1. Certificate issuance or renewal fees

258. 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

259. Not stipulated.

9.1.3. Revocation or status information access fees

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

9.1.4. Fees for other services

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

9.1.5. Refund policy

262. 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 *Electronic Venue* of the FNMT – RCM.

9.2. FINANCIAL RESPONSIBILITY.

263. Please see the corresponding section of the *DGPC.*

9.2.1. Insurance coverage

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

9.2.2. Other assets

265. See the relevant section in the *DGPC*.

9.2.3. Insurance or warranty coverage for end-entities

266. See the relevant section in the *DGPC*.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

267. Please see the corresponding section of the *DGPC.*

9.3.1. Scope of confidential information

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

9.3.2. Information not within the scope of confidential information

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

9.3.3. Responsibility to protect confidential information

270. See the relevant section in the *DGPC*.

9.4. PRIVACY OF PERSONAL INFORMATION

271. Please see the corresponding section of the *DGPC.*

9.4.1. Privacy plan

272. See the relevant section in the *DGPC*.

9.4.2. Information treated as private

273. See the relevant section in the *DGPC*.

9.4.3. Information not deemed private

274. See the relevant section in the *DGPC*.

9.4.4. Responsibility to protect private information

275. See the relevant section in the *DGPC*.

9.4.5. Notice and consent to use private information

276. See the relevant section in the *DGPC*.

9.4.6. Disclosure pursuant to judicial or administrative process

277. See the relevant section in the *DGPC*.

9.4.7. Other information disclosure circumstances

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

9.5. INTELLECTUAL PROPERTY RIGHTS

279. Please see the corresponding section of the *DGPC.*.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA representations and warranties

280. 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.*

281. 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.

282. The FNMT-RCM issues the *Electronic Venue 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 *DPPP* and the aforementioned version, said requirements shall prevail over those contained in this document.

283. In addition, the FNMT-RCM undertakes to comply, in relation to the issuance of the *Electronic Venue Certificates* issued under this policy, 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 DPPP and the aforementioned version, said requirements shall prevail over those contained in this document.

284. 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 the *DGPC,* the *Trust Service Provider* undertakes to:

285. 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

286. Please see the corresponding section of the *DGPC.*

287. All activities related to the RA will be carried out exclusively by the FNMT-RCM, through its Registration Area, for all *Website authentication certificates.*

288. 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 the *DGPC,* and, in particular, in this *DPP.*
- 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

289. Please see the corresponding section of the *DGPC.*

290. With regard to *Website authentication certificates*, *Subscribers* must have control of the website domain name included in said *Certificates* and maintain all associated *Private keys* under their exclusive use.

291. 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 *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.

292. 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.

293. 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.

294. 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.

295. With regard to Electronic Venue certificates, 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 certificates 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 Electronic Venue 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 Electronic Venue 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 Electronic Venue and the e-mail address, domain or URL through which such Site is accessed) and the Applicant (the individual with sufficient powers to request a Electronic Venue Certificate) 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 Electronic Venue identified in the Certificate will be accessed.
- To request the revocation of the Electronic Venue Certificate 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.

296. 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

297. Please see the corresponding section of the *DGPC.*

298. 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.

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

300. 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

301. Not stipulated.

9.7. DISCLAIMERS OF WARRANTIES

302. Not stipulated.

9.8. LIMITATIONS OF LIABILITY

303. Please see the corresponding section of the *DGPC.*

9.9. INDEMNITIES

304. Please see the corresponding section of the *DGPC.*

9.9.1. CA indemnity

305. See the relevant section in the GCPS.

9.9.2. Subscribers indemnity

306. See the relevant section in the GCPS.

9.9.3. Relying parties indemnity

307. See the relevant section in the GCPS.

9.10. TERM AND TERMINATION

9.10.1. Term

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

9.10.2. Termination

309. 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

310. 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

311. Please see the corresponding section of the *DGPC.*

9.12. AMENDMENTS

9.12.1. Procedure for amendment

312. 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

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

314. 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

315. 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 PROVISIONS

316. Please see the corresponding section of the *DGPC*.

9.14. GOVERNING LAW

317. Please see the corresponding section of the *DGPC*.

9.15. COMPLIANCE WITH APPLICABLE LAW

318. 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 *DPPP* document.

9.16. MISCELLANEOUS PROVISIONS

319. Please see the corresponding section of the *DGPC*.

9.16.1. Entire Agreement

320. Please see the corresponding section of the *DGPC*.

9.16.2. Assignment

321. Please see the corresponding section of the *DGPC*.

9.16.3. Severability

322. Please see the corresponding section of the *DGPC*.

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

323. Please see the corresponding section of the *DGPC*.

9.16.5. Force Majeure

324. Please see the corresponding section of the *DGPC*.

9.17. OTHER PROVISIONS

325. Please see the corresponding section of the *DGPC*.