Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

TRUST SERVICES PRACTICES AND ELECTRONIC CERTIFICATION GENERAL STATEMENT

	NAME	DATE
Prepared by:	FNMT-RCM	10/02/2021
Reviewed by:	FNMT-RCM	11/02/2021
Approved by:	FNMT-RCM	18/02/2021

DOCUMENT HISTORY			
Version	**Date**	**Description**	**Author**
		Certification Practices Statement (on all the FNMT-RCM's certification policies)	FNMT-RCM
3.0	05/05/2009	Document creation	FNMT-RCM
3.1	04/01/2010	Update of aspects relating to the time stamping service	FNMT-RCM
3.2	22/06/2010	A new chain of trust is created for the provision of certification services to public administrations. It includes new security controls to enhance guarantees and trust in the services. A specific section is added to identify the FNMT-RCM as the Certification Service Provider.	FNMT-RCM
3.3	19/12/2011	A specific section is included on the management of *Certification Policies*	FNMT-RCM
3.4	20/01/2012	A new wording of paragraph 12.1 is included, describing terms and conditions for the reselling of services.	FNMT-RCM
3.5	02/07/2013	A one-year frequency is included for the performance of audits under the ETSI 101-456 standard. Prohibition on the issuance of CA *Certificates* to entities other than the FNMT-RCM.	FNMT-RCM

		Maximum 3-year limit on the validity of end-entity certificates. Reorganisation to include policy-related aspects in a single section. Removal of references to Mobile Signature CA due to having discontinued the service. Inclusion of IT Components CA in the Root CA certification chain.	
4.0	17/06/2014	References to the appendices that were eliminated from version 3.5 are removed. The definitions of holder and signatory are aligned with respect to the Electronic Signature Law ("*LFE*"). Some links to the new Ceres website are updated. Audit review in accordance with WebTrust and ETSI. Extension of the maximum validity of certificates to five years, pursuant to the LFE amendment.	FNMT-RCM
4.1	16/02/2015	Inclusion of the commitment to the baseline requirements defined by the CA/Browser forum.	FNMT-RCM
4.2	14/07/2015	Inclusion of the commitment to the requirements defined by the ETSI 101 456 standard.	FNMT-RCM
4.3	12/04/2016	Inclusion of references to User CAs and Representation and elimination of APE CA and ISA CA.	FNMT-RCM
5.0	24/06/2016	Compliance with ETSI 101456 requirements and update of definitions pursuant to Regulation (EU) No. 910/2014 (eIDAS).	FNMT-RCM
5.1	03/01/2017	Upgrade to Regulation eIDAS (ETSI 319 401).	FNMT-RCM
5.2	09/10/2017	Content reorganisation and inclusion of new baseline requirements defined by the CA/Browser forum.	FNMT-RCM
5.3	13/06/2018	Inclusion of requirements defined by the ETSI standards and GDPR.	FNMT-RCM

5.4	05/03/2019	Inclusion of the new CA root "Servidores seguros" Certificate	FNMT-RCM
5.5	05/11/2019	Inclusion of the new CA root " AC Sector Público" Certificate and the new CA root "AC Unidades de Sellado de Tiempo" Certificate. General review and clarifying updates	FNMT-RCM
5.6	06/02/2020	Inclusion of information related to the online service on the status of certificates and information regarding the server signature service	FNMT-RCM
5.7	16/06/2020	General review	FNMT-RCM
5.8	29/09/2020	Inclusion of information related to the online service on the status of certificates and intellectual property rights	FNMT-RCM
5.9	18/02/2021	Compliance review to Law 6/2020. Reference to the maximum period between revisions of the Information Security Policy is documented.	FNMT-RCM

Reference: DPC/DGPC0509/SGPSC/2021

Document classified as: *Public*

Content

1. INTRODUCTION

1. The Spanish Mint ("Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda"), hereinafter the FNMT-RCM, holding tax code Q2826004-J, is a public corporation regulated by the Law 40/2015 (October 1) of Legal Regime of the Public Sector. As a public body, the Mint has its own public legal personality, 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 of Finance, will be responsible for strategic management and control of the FNMT-RCM's effectiveness in the terms of the aforementioned Law 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 Law 66/1997 (30 December) on Tax, Administrative and Social Measures came into force, together with related amendments, the FNMT-RCM's authorised services have been extended. The FNMT-RCM now plays a leading role in the provision of trust services.

4. The FNMT-RCM, through the CERES (Spanish Certification) Department, in order to provide secure electronic transactions through the Web, has built the necessary infrastructure since 1996 to provide electronic certification services with maximum guarantees.

5. The FNMT-RCM is a *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 (eIDAS Regulation).

6. The FNMT-RCM's objective, through its CERES Department, is to provide a *Public Key Infrastructure* and a full catalogue of services to support the services of administrations and companies, providing security and legal validity in a way that is simple and convenient for the general public. The FNMT-RCM will seek to achieve these goals mainly by means of encryption (to assure the confidentiality of information) and electronic signature techniques, which guarantee the signer's identity and the integrity of the information exchanged. The system employed is consistent with the mentioned eIDAS Regulation, with domestic legislation and with the FNMT-RCM's own specific regulations.

7. The FNMT-RCM has been making high-security and particularly sensitive products such as coins and notes for over a century. But it also makes other security products such as national ID cards, passports, stamps, paper for official contracts, registers, intelligent cards and secure labels, etc. for the domestic and international markets.

8. The FNMT-RCM thus continues to perform its traditional role of providing Spanish society with public security guarantees, although now also from the perspective of the Internet and new technologies, adapting to the new times and taking a qualitative leap from physical documents to *Electronic Documents,* as in the case of the electronic ID card ("DNIe") and electronic passport.

1.1. PURPOSE

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

- management of *Signature creation and verification data* and *Certificates*, conditions applicable to the request, issuance, use, suspension and expiration of *Certificates* and, if applicable, the existence of procedures for coordination with the relevant Public Registries that allow the immediate and confidential exchange of information on the validity of the powers stated in the *Certificates*, which must mandatorily be entered in such registers.
- provision of the service allowing the consultation of the validity of *Certificates*, whether those issued by the FNMT-RCM itself or by third parties, stating the specific aspects of each case and the conditions applicable to the use of the service and guarantees provided.
- management of requests for *Electronic time stamps* offered as part of the *Time stamping service*.

10. This document also includes details of 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

11. This document is named "*FNMT-RCM Trust Services Practices and Electronic Certification General Statement*" and will be referred to internally as "*Trust Services Practices and Electronic Certification General Statement*" or using the acronym "*DGPC*".

12. This document does not address the specific aspects of each of the *Practices and Policies for Certification, the the server signature service or Time stamping* that are employed by the FNMT-RCM when providing trust services. These specific aspects are addressed in the relevant documents under the general application framework of this *DGPC*.

13. The specific *Certification Policies and Practices* will prevail over the content of this *DGPC* for specific aspects relating to the types of *Certificate* and/or service addressed.

14. The Information Security Committee of the FNMT-RCM regularly reviews the risks to which the Organization is exposed and approves the necessary treatment plans to guarantee the security of the services defined in each of the Certification Policies.

15. The terms and conditions of use, restrictions, liabilities, properties and any other information deemed specific to each type of certificate will be set out in the Specific Certification Statements relating to this *DGPC*.

16. This *DGPC* is referenced *OID* 1.3.6.1.4.1.5734.4 and the latest version in force may be found at the address: http://www.cert.fnmt.es/dpcs

17. These procedures are based mainly on the standards of the *European Telecommunications Standards Institute* (ETSI).

1.3. PARTIES

18. The following parties are involved in the management and use of the *Trust service*s described in this *DGPC*:

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

1.3.1. Certification Authorities

19. The FNMT-RCM is the *Certification Authority* that issues electronic *Certificates* in accordance with this *DGPC*, which will be addressed in Specific Certification Policy Statements. Certification Authorities are as follows:

a) Root Certification Authorities. These authorities exclusively issue *Certificates* for Subordinate Certification Authorities. These CA's root certificates are identified by the following information:

Table 1 – CA FNMT-RCM root certificate

CA FNMT-RCM root certificate	
Subject	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Issuer	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Serial number (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07
Validity	Not before: 29 October 2008. Not after: 1 January 2030
Public key length	RSA 4096 bits
Signature algorithm	RSA – SHA256

CA FNMT-RCM root certificate	
Key identifier	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

Table 2 – CA FNMT-RCM "SERVIDORES SEGUROS" root certificate

CA FNMT-RCM "SERVIDORES SEGUROS" root certificate	
Subject	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Issuer	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Serial number (hex)	62:F6:32:6C:E5:C4:E3:68:5C:1B:62:DD:9C:2E:9D:95
Validity	Not before: 20 December 2018. Not after: 20 December 2043
Public key length	ECC P-384 bits
Signature algorithm	Sha384ECDSA
Key identifier	01 B9 2F EF BF 11 86 60 F2 4F D0 41 6E AB 73 1F E7 D2 6E 49

b) Subordinate Certification Authorities: issue end-entity *Certificates*, which will be addressed in Specific Certification Policy Statements.

20. The *Certification Chains* employed by the FNMT-RCM as a *Trust Service Provider*, signature algorithms and related parameters are as follows:

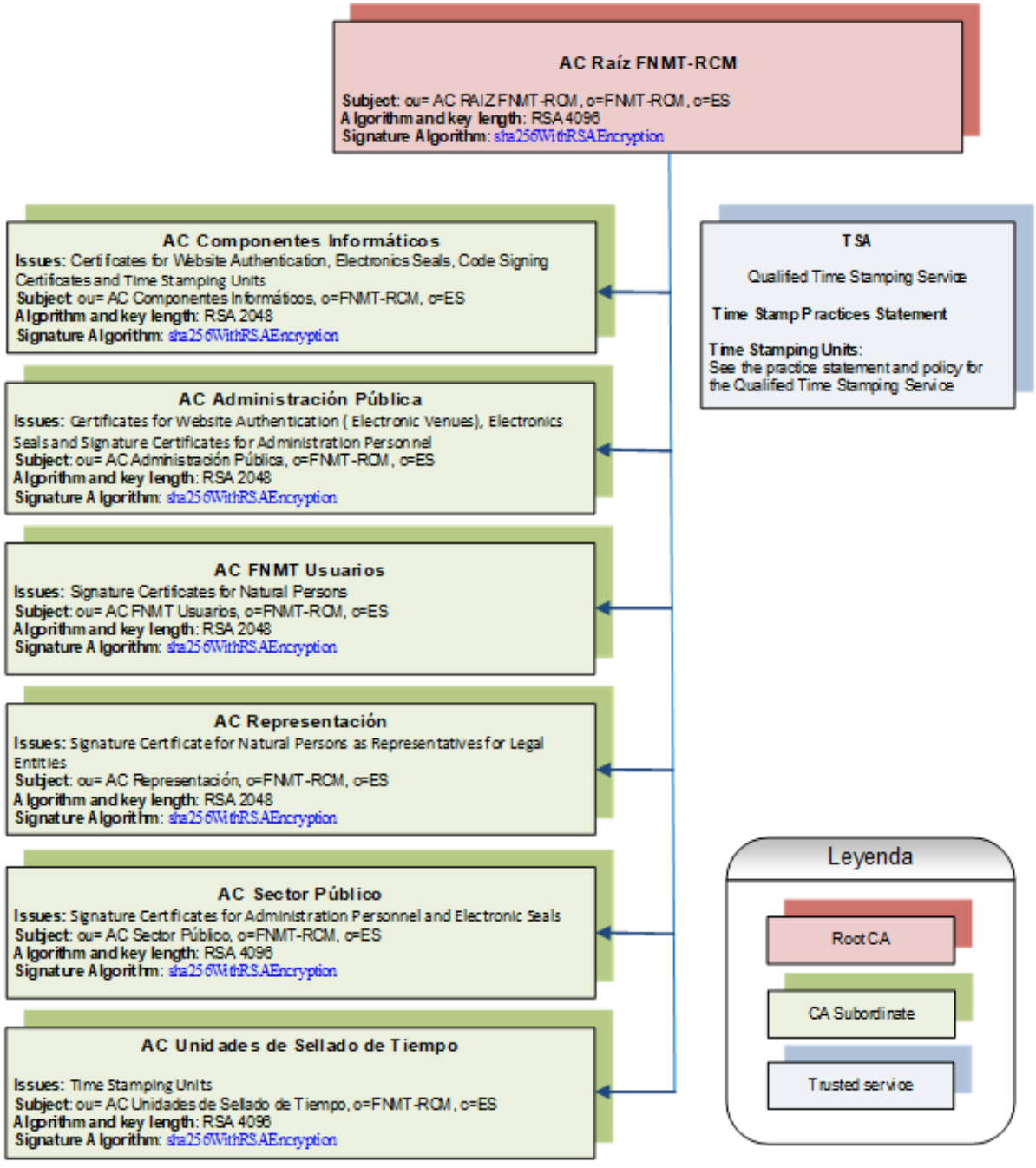

Illustration -1: CA FNMT-RCM hierarchy

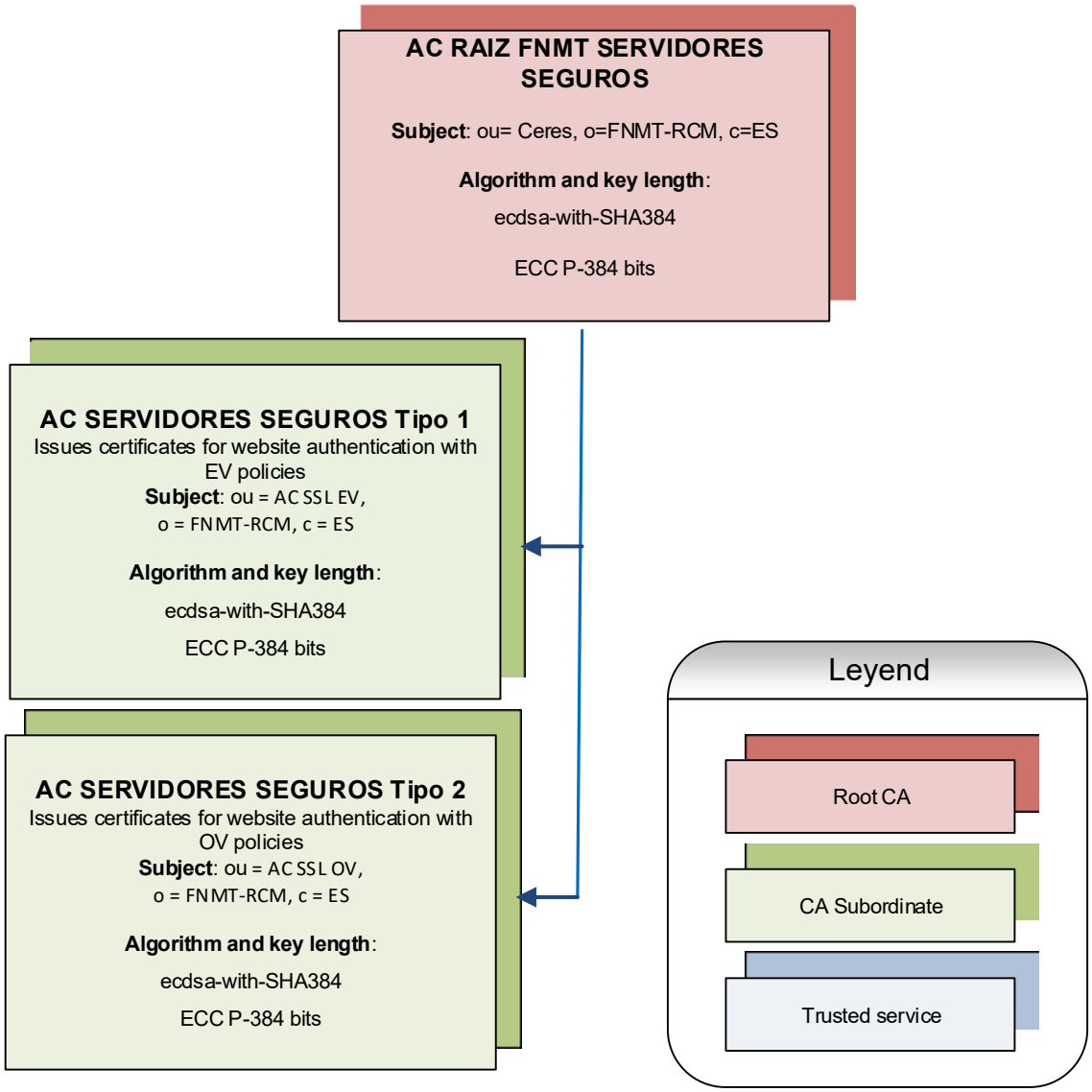

Illustration -2: CA root FNMT-RCM "SERVIDORES SEGUROS" hierarchy

21. The FNMT-RCM will not use its *Signature Creation Data* to issue *Certification Authority Certificates* to holders other than itself or any third party that may request it.

22. In order to check the authenticity of any "Self-signed *Certificate*", the final element in any *Certification Chain*, the relevant digital fingerprint may be verified (in different formats).

23. In the interests of interoperability and forecasts, these *Certification Authorities*' *Signature / Seal Creation Data* have been self-signed using different algorithms. The following information is therefore published:

1.3.1.1. Signature Algorithm

24. **Information about "AC RAIZ FNTM-RCM" Certificate**:

- pkcs1-sha1WithRSAEncryption,
- pkcs1-sha256WithRSAEncryption,
- pkcs1-sha512WithRSAEncryption

pkcs1-sha1WithRSAEncryption certificate

- Serial number: 00 81 bb dd 6b 24 1f da b4 be 8f 1b da 08 55 c4
- Digital fingerprint (SHA-1): b8 65 13 0b ed ca 38 d2 7f 69 92 94 20 77 0b ed 86 ef bc 10
- Digital fingerprint (MD5): 0C:5A:DD:5A:AE:29:F7:A7:76:79:FA:41:51:FE:F0:35

pkcs1-sha256WithRSAEncryption certificate

- Serial number: 5d 93 8d 30 67 36 c8 06 1d 1a c7 54 84 69 07
- Digital fingerprint (SHA-1): ec 50 35 07 b2 15 c4 95 62 19 e2 a8 9a 5b 42 99 2c 4c 2c 20
- Digital fingerprint (MD5): E2:09:04:B4:D3:BD:D1:A0:14:FD:1A:D2:47:C4:57:1D

pkcs1-sha512WithRSAEncryption certificate

- Serial number: 0e 1c d8 cd 45 32 5a 47 00 51 0c aa c2 db 1e
- Digital fingerprint (SHA-1): 14 4e 9a 4c d1 52 a9 47 5c dd 87 58 96 9c 13 e2 88 66 57 0e
- Digital fingerprint (MD5): 8B:F1:A3:E2:DA:D9:61:99:AF:7F:73:3A:00:2E:DF:E0

25. **Information about "AC RAIZ FNTM-RCM SERVIDORES SEGUROS" Certificate:**

- Sha384ECDSA
- Serial number: 62:F6:32:6C:E5:C4:E3:68:5C:1B:62:DD:9C:2E:9D:95
- Digital fingerprint (SHA-256):

  55:41:53:B1:3D:2C:F9:DD:B7:53:BF:BE:1A:4E:0A:E0:8D:0A:A4:18:70:58:FE:60:A2:B8:62:B2:E4:B8:7B:CB
- Digital fingerprint (SHA-1):

  62:FF:D9:9E:C0:65:0D:03:CE:75:93:D2:ED:3F:2D:32:C9:E3:E5:4A

1.3.2. Registration Authority

26. The *Registration Authority* carries out tasks to identify applicants or certificate holders, verify the documentation attesting to the circumstances stated in the certificates, and validate and approve requests to issue, revoke and, if applicable, renew *Certificates*.

27. Registration entities for the FNMT-RCM may be *Registration Offices* designated by the *Certificate Subscriber* body or entity with which the latter entity signs a legal instrument for this purpose.

1.3.3. Certificate subscribers

28. There may be a *Certificate Subscriber*, separate from the *Signatory*, when there is a representative relationship or membership of an Organisation, so that the latter is deemed to be the *Subscriber*, or in the case of *Electronic Seal certificates or Web authentication*. Nonetheless, each Specific Certification Policy Statement will indicate this possible separation of the *Signatory* and the *Subscriber*.

29. *Signatories* are the natural persons that exclusively use the *Signature creation data* associated with the *Certificates* of which they are *Holders*.

1.3.4. Trusting parties

30. Trusting parties are natural persons or legal entities, other than the *Signatory*/*Subscriber*, that receive and/or use *Certificates* issued by the FNMT-RCM and, as such, are subject to the provisions of the relevant Certification Practices Statement when they effectively decide to place their trust in the *Certificates*.

1.3.5. Other participants

1.3.5.1. Time Stamping Authority

31. The FNMT-RCM is the *Time Stamping Authority* when it provides the *Trust Service* consisting of the creation of *Electronic time stamps*, in accordance with the relevant Specific Practices Statement.

1.4. USE OF CERTIFICATES

1.4.1. Permitted uses of certificates

32. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

1.4.2. Restrictions on the use of certificates

33. The end-entity *Certificates* issued by the FNMT-RCM may not be employed to/for:

- Sign or Seal a different *Certificate*, unless specific prior authorisation is obtained.
- Private uses, barring relations with Administrations where permitted.
- Sign or Seal software or components with the exception of the *Component Certificates for code signature*.
- Generate time stamps for electronic dating procedures with the exception of *Certificates* issued for *Time Stamping Units*.
- Provide services for no consideration or for valuable consideration, unless specific prior authorisation is obtained, such as, for illustrative purposes:
  - Provision of OCSP services.
  - Generation of Revocation Lists.
  - Provision of notification services.

1.5. POLICY ADMINISTRATION

1.5.1. Entity responsible

34. The Spanish Mint, holding tax code Q2826004-J, is the Certification Authority that issues the certificates to which this *Trust Services Practices and Electronic Certification General Statement* applies.

1.5.2. Contact details

35. 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

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 MADRID

E-mail: ceres@fnmt.es

Tel.: 902 181 696

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

1.5.3. Parties responsible for adapting the General Statement

37. The FNMT-RCM's remit includes the capacity to specify, revise and approve review and maintenance procedures both for this *Trust Services Practices and Electronic Certification General Statement* and for the relevant *Specific Certification Practices* and *Certification Policy*.

1.5.4. General Statement approval procedure

38. The FNMT-RCM, through its *Trust Service Provider* Management Committee, oversees compliance with the *Certification Practices and Policies Statements*, approves them and reviews them annually.

39. The FNMT-RCM has *Policies and Practices* for the trust services provided, which are specific to each type of *Certificate* or trust service. In particular, it declares that:

- The FNMT-RCM has the capacity to specify, review and approve the *Certification Policies* and its trust services through its General Management and other management bodies.
- The FNMT-RCM has *Specific Trust Service Practices* that describe the practices applicable to the services identified in each service *Policy*.
- The FNMT-RCM's Management and other bodies have the capacity to specify, revise and approve the review and maintenance procedures both for the *Specific Certification Practices* and the relevant *Certification Policy*.
- The FNMT-RCM, through its Trust Service Provider Management Committee, oversees compliance with the *Certification Practices and Policies Statements* and *server signature service* approves them and reviews them annually.
- The FNMT-RCM carries out risk analyses to assess threats to the system and propose suitable security measures (safeguards) for all the areas involved.
- The *Certification Policies and Practices* are available to the general public at the following URL:

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

- The *Certification Policies* contain the general obligations and responsibilities of the parties involved in each certification service for use within the stipulated limits and relevant application framework, always subject to each party's remit. This is all without prejudice to any special provisions of applicable contracts, commissions or agreements.
- There are specific OIDs identifying each *Certification Policy*. A priori, no condition is envisaged that entails changes to the OIDs identified in this DGPC and the Specific Practices and Policies.
- The FNMT-RCM's *Certification Policies* will take into account regulations and legislation applicable in each case.
- All the information, systems and procedures, from a qualitative and quantitative viewpoint, deadlines, amounts, forms and, in general, any matters stated in the declarative documents relating to *Certification Policies and/or Practices*, may be amended or removed by the FNMT-RCM, without the need for consent from the members of the *Electronic Community* nor from the service *Users*. The FNMT-RCM assumes the commitment to report any changes that arise through the systems stipulated in applicable legislation and in the Entity's website.

- The members of the *Electronic Community* and the *Users* of the services are required to regularly check the relevant declarative documents (applicable *Certification Policies and/or Practices*), requesting any information deemed fit from the FNMT-RCM. Nonetheless, in order to facilitate knowledge of new developments by *Recipient users* (*User entity* and *Subscriber*), when the amendments made to any of the *Certification Policies and/or Practices* directly affect the rights and obligations of the parties forming the *Electronic Community*, or restrict the scope of the *Certificates*, the FNMT-RCM will notify the interested parties at least thirty (30) days prior to the effective date of the changes, so that the members of the *Electronic Community* may take a decision as deemed fit. FNMT-RCM will not make any indemnity commitment for amendments or eliminations affecting the Statement while exercising its rights as a *Trust Service Provider*.
- 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.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

40. Information on the basic concepts of Cryptography, *Trust Service Providers* and *Public Key Infrastructures* may be found at http://www.ceres.fnmt.es.

41. Nonetheless, for the purposes of this *Trust Services Practices and Electronic Certification General Statement* and, if applicable, the relevant *Specific Certification Statements*, the terms will have the following meanings, only where they begin with an upper-case letter and are in italics:

- *Advanced electronic Seal*: An *Electronic Seal* that is linked uniquely to the *Seal creator* and allows the *Seal creator* to be identified, has been created using *Electronic Seal creation data* that the *Seal creator* is able to use to a high level of trust under his or her exclusive control and that is linked to the data to which it refers, such that any subsequent change in the data is detectable.
- *Advanced electronic signature*: *Electronic signature* that is linked uniquely to the *Signatory* and allows the *Signatory* to be identified, has been created using *Electronic signature creation data* that the *Signatory* is able to use to a high level of trust under his or her exclusive control and that is linked to the data signed, such that any subsequent change in the data is detectable.
- *AEPD:* "Spanish Data Protection Agency". A public-law entity with its own legal personality and full public and private capacity which is entirely independent from the Public Administrations in the performance of its functions. Its main purpose is to oversee compliance with and control the application of personal data protection legislation.

- *Applicant*: A natural person aged 18 or over or an emancipated minor who, following identification and, if applicable, duly empowered, requests an operation relating to a *Certificate* in her or her name or on behalf of the *Certificate Holder*.
- *Asymmetric encryption*: Transcription in symbols, in accordance with an encryption *Key*, of a message the content of which is intended to be concealed by means of an algorithm so that knowledge of the encryption *Key* is insufficient to decipher the transcription and knowledge of the relevant decoding *Key* is necessary. Knowledge of the encryption *Key* does not entail knowledge of the decoding *Key* and vice versa.
- *Availability*: Quality of data or information implying that it is available, i.e. the possibility of using the data or information.
- *BOE:* (or Official State Gazette) The Official Gazette published and distributed by Boletín Oficial del Estado, a public body attached to the Ministry of the Presidency and also responsible for publishing and distributing the Commercial Registry's Official Gazette, for publishing collections of law reports and compilations of legal texts, and for printing official documents requested by ministries, bodies and other public entities.
- *Browser (web browser)*: A program that allows the content of *web pages* in the Internet to be viewed. Also known as a *browser*. Some examples of *web browsers* or *browsers* are as follows: Internet Explorer, Chrome and Mozilla Firefox.
- *C:* Within the scope of this document, this is an abbreviation of the English word "Country", which means "País" in Spanish. The "Country" is an attribute that forms part of the Distinctive Name (*DN*) of an object within directory structure *X.500,* used to name the entry pertaining to the object.
- *Certificate Revocation Lists (CRLs)*: Lists exclusively containing revoked and suspended *Certificates*.
- *Certificate serial number*: A whole number, unique to each *FNMT-RCM Certification Authority*, which is unequivocally associated with a *Certificate* issued by the FNMT-RCM.
- *Certificate Problem Report*: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
- *Certificate validity status information and consultation service*: A service provided by the FNMT-RCM to interested parties to furnish information on the status of *Certificates* requested by the user.
- *Certification Authority* (CA): A trust system managed by a *Trust Service Provider* and responsible for issuing and revoking *Certificates* used in *Electronic signatures*. From a legal viewpoint, it is a specific case of a *Trust Service Provider* and, by extension, the provider is referred to as the *Certification Authority*.
- *Certification chain*: An ordered list of *Certificates* containing at least one *Certificate* and the FNMT-RCM *root Certificate,* the *Signature verification data* contained in the root certificate being used to authenticate the *Certificate.*
- *Certification Policy (specific):* A document that lays down the set of rules indicating the applicability of a certain type of *Certificate* to the *Electronic Community* and/or application class with common security requirements.

- *Certification Practice (specific)*: A document containing the specific procedures followed by the FNMT-RCM to manage the life cycle of a certain type of *Certificate* and other certification services that may be included in the scope of the practice.
- *CN:* The Common Name or "Nombre Común" in Spanish. The "Common Name" is an attribute that forms part of the Distinguished Name (*DN*) of an object within directory structure *X.500,* used to name the entry pertaining to the object.
- *Confidentiality*: A quality which entails that the information is not accessible to or has not been disclosed to unauthorised persons, entities or processes.
- *Contract, Commission* and *Agreement*: Legal instruments provided by legislation corresponding to and/or in accordance with the autonomy of will, in which the relationship for the provision of services by the FNMT-RCM is formalised. This category includes issuance contracts (forms) and agreements for the revocation and renewal of the relevant *Certificates* and the acceptance of terms and conditions of use and restrictions of which the members of the *Electronic Community* are informed by means of electronic, computer and telematic systems having that nature.
- *Coordinated Universal Time (UTC)*: The time in the zone of reference with respect to which all other zones are calculated worldwide. It is the successor to GMT as a time standard and, unlike GMT, is based on atomic time.
- *CPD*: Data Processing Centre.
- *Cryptographic card*: A medium containing a microprocessor or chip forming a cryptographic device used to make *Electronic signatures* with the *Signature creation data* held inside it. The *Cryptographic card* may be a QSCD if it matches the definition.
- *Cryptographic system*: A collection of transformations of clear text to *encrypted text* and vice versa, in which the transformation(s) to be used are selected by *Keys*. Transformations are normally defined by a mathematical algorithm.
- *Cryptography*: A discipline that encompasses the principles, meanings and methods for data transformation in order to conceal the content/information, preventing undetected modification and/or unauthorised use.
- *Directory*: Information repository following the ITU-T's X.500 standard.
- *DN*: The acronym of "Distinguished Name" or "Nombre Distintivo" in Spanish. The "Distinguished Name" unequivocally identifies an entry in the *X.500* directory structure. The DN comprises the entry's common name (*CN*) plus a series of attributes that identify the route followed inside the *X.500* directory structure to reach that entry.
- *ECT*: Electronic, computer and telematic techniques and media.
- *Electronic Community*: A group of persons and entities interrelated through *Certificates*, under the general framework of this *Trust Services Practices and Electronic Certification General Statement*, and, in particular, of the relevant agreements and/or contracts that may have been concluded, directly or through representatives, with the FNMT-RCM.
- *Electronic document*: Information of any kind in electronic form, filed in an electronic medium in a specific format and able to be identified and processed in a distinctive manner.

- *Electronic National ID card (DNI*e). A national ID card attesting electronically to the holder's personal identity and allowing the electronic signing of documents.
- *Electronic Seal certificate*: An electronic statement that links the *Validation data* for a Seal to a legal entity and confirms the entity's name.
- *Electronic Seal*: Data in an electronic format attached to other data in an electronic format, associated with them in a logical manner, to guarantee the source and integrity of the latter data.
- *Electronic signature certificate*: An electronic statement that links the *Validation data* for a signature to a natural person and confirms, at least, that person's name or pseudonym.
- *Electronic signature*: Data in an electronic format attached to other electronic data or data associated with them in a logical manner and used by the *Signatory* to sign.
- *Electronic time stamp:* Electronic data linking other data in an electronic format to a specific instant in time so as to provide evidence that the latter data existed at that time.
- *FNMT root certificate*: *Certificate* of which the FNMT-RCM is the *Holder* and, as it is self-signed, i.e. issued using the *Signature creation data* linked to the *Signature verification data* contained in the *Certificate* itself, is the last *Certificate* in the chain of trust of all the *Certificates* issued by the FNMT-RCM.¡
- *FNMT-RCM Information Security Management System Manual as a Trust Service Provider*: Also referred to as the *CERES Security Manual* or *Security Manual*. This manual contains the procedures of the FNMT-RCM's CERES Department's Information Security Management System under the *ISO 27001* standard: *Information Security Management Systems (SGSI).*
- *Hash function*: A *Hash function* is an operation performed on a data set of any size resulting in a different data set, sometimes referred to as a "summary" or "Hash" of the original data, that has a fixed size and is separate from the original set, in addition to the property of being associated unequivocally with the initial data, i.e. it is virtually impossible to find two different messages that have an identical *Hash*.
- *Hash*: A fixed-size result obtained by applying a *Hash function* to a message, irrespective of the message size, which has the property of being associated unequivocally with the initial data.
- *Holder* (of a *Certificate*): The person whose identity is linked to the *Signature verification data* (*Public Key*) of the *Certificate* issued by the *Trust Service Provider*. Consequently, the *Holder*'s identity is linked to the information signed electronically, as a *Signatory*, using the *Signature creation data* (*Private Key*) associated with the *Certificate*.
- *Integrity*: Quality implying that the data set forming the message does not lack any of its parts and no additional part has been included in it. From the viewpoint of the information that could be implied by those data, this means that neither the content nor the structure may be altered.
- *Issuance Law:* A set of technical and legal characteristics of a certain type of electronic *Certificate*, pursuant to the applicable *Certification Policies and Practices* and the

relevant contracts and/or agreements with the members of the *Electronic Community*, based on the autonomy of will.

- *ITU (International Telecommunications Union)*: UN international organisation in which governments and the private sector coordinate worldwide telecommunications services and networks
- *Key*: Sequence of symbols controlling the encryption and decoding operations.
- *Legal person:* A group of people constituting a unit having its own purpose, which acquires, as a legal entity, the legal capacity to act which is separate from that of the members forming it.
- *Malware (malicious software):* See *Malicious software*.
- *Malicious software* (malware)*:* Any program, document, message or element of a message that may cause damage and/or harm to users.
- *MD5:* Message Digest (message summary algorithm), version 5. Developed by R. Rivest in 1991. Description published in RFC 1321. The algorithm consists of taking messages of an arbitrary length and generating a *Hash* 128 bits long. The probability of finding two different messages that generate the same *Hash* is virtually zero. For this reason, it is used to provide *Integrity* in documents during the *Electronic signature* process.
- *O:* Within the scope of this document, it is an abbreviation of the English word "Organization" or "Organización" in Spanish. The "Organization" is an attribute that forms part of the Distinguished Name (*DN*) of an object within the *X.500* directory structure, used to name the object entry.
- *OCSP (Online Certificate Status Protocol):* A computer protocol that allows the validity of an electronic *Certificate* to be verified quickly and securely.
- *OCSP client*: A tool necessary for the *User entities* to make *OCSP* requests. The FNMT-RCM will provide a list of freely distributable products but will not supply the *OCSP client* since it is easily available in the Market.
- *OID (Object Identifier)*: A value that has a hierarchical nature and includes a sequence of variable components, though always non-negative whole numbers separated by a dot, which may be assigned to registered objects and have the property of being unique with respect to other *OIDs*.
- *OU*: The acronym of "Organizational Unit" or "Unidad Organizativa" in Spanish. An organizational unit is an attribute forming part of the Distinguished Name of an object within the *X.500* directory structure.
- *PIN*: An abbreviation of the English "Personal Identification Number" or "Número de Identificación Personal" in Spanish. It is an alphanumeric data set known only to the person that has access to a resource protected by this mechanism.
- *PKCS (Public-Key Cryptography Standards)*: *Public-Key* cryptographic standards created by RSA Laboratorios and accepted internationally.
- *PKCS#7* (Cryptographic Message Syntax Standard): *Public-Key* cryptographic standard, created by RSA Laboratorios and accepted internationally, defining a generic syntax for messages that include cryptographic improvements, such as a digital signature and/or encryption.

- *PKCS#10* (Certification Request Syntax Standard): *Public-Key* cryptographic standard, created by RSA Laboratorios and accepted internationally, defining the syntax of a certification request.
- *PKCS#11 (Cryptographic Token Interface Standard): Public-Key* cryptographic standard, created by RSA Laboratorios and accepted internationally, defining a programming interface that is independent from the base technology in order to use cryptographic tokens (e.g. cryptographic smart cards) as a means of authentication.
- *Private Key*: Of the pair of cryptographic *Keys* in *Asymmetric encryption*, the one to be kept secret. The *Private Keys* may serve as *Signature creation data,* depending on their generation and use.
- *Public Key Infrastructure* (PKI): Infrastructure capable of supporting *Public Key* management for authentication, encryption, integrity and non-repudiation.
- *Public Key*: Of the pair of cryptographic *Keys* in *Asymmetric encryption*, the one to be disclosed. The *Public Keys* may serve as *Signature verification data, depending* on their generation and use.
- *QSCD (Qualified Electronic Signature Creation Device):* See *Qualified signature creation device.*
- *Qualified electronic Seal*: An advanced electronic Seal created by means of a qualified electronic Seal creation device and based on a qualified electronic Seal certificate.
- *Qualified electronic signature Certificate*: An electronic *Certificate* issued by a *Trust Service Provider* fulfilling the requirements 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, as well as Law 6/2020 regulating certain aspects of electronic trust services, as regards identity verification and other circumstances of the *Applicants* and the reliability of and guarantees for the trust services provided.
- *Qualified electronic signature*: *Advanced electronic signature* based on a *Qualified electronic signature certificate* and generated through a *Qualified signature creation device*.
- *Qualified Trust Service Provider*: A *Qualified Trust Service Provider* that provides one or more qualified trust services, having been qualified by the supervisory body.
- *Registration Offices*: Offices installed by the FNMT-RCM, or by a different entity under an agreement entered into with the FNMT-RCM by that entity or its administrative hierarchical superior, to allow citizens and companies, nationally and internationally, to submit applications relating to *Certificates*, so as to confirm their identity and the delivery of the relevant documents attesting to personal qualities, powers of attorney and other requirements applicable to the type of *Certificate* requested.

  Where there are sufficient guarantees to confirm identity and other personal data necessary to manage *Certificates*, the registration operations may be completed telematically
- *ROA: Real Observatorio de la Armada (Spanish Navy Observatory*): Laboratory of the Spanish Navy's Royal Institute and Astronomical Observatory, attached to the Ministry of Defence, associated with the Spanish Metrology Centre and a member of the

International Weights and Measures Bureau; designated by RD 1308/1992 as Spain's national timing centre.

- *RSA*: Acronym of Ronald Rivest, Adi Shamir and Leonard Adleman, the inventors of the asymmetric key cryptographic system (1977). A public-key cryptosystem allowing encryption and digital signing.
- *Seal creation data:* The unique data used by the *Electronic Seal creator* to create the Seal.
- *Seal creator*: A legal entity that creates an *Electronic Seal*.
- *Server signature service Practice Statement and Policy:* Document that establishes the set of specific rules and procedures followed by the FNMT-RCM for the provision of its electronic signature service on serve
- *Signatory*: Natural person that creates an electronic signature in his or her own name or on behalf of a represented legal entity or entity without a legal personality.
- *Signature creation data*: They are the unique data, such as private cryptographic codes or keys, used by the *Signatory* to create electronic signatures. For practical purposes relating to this *Certification Practices Statement,* they will always coincide, from a technical viewpoint, with an asymmetric, cryptographic *Private Key*.
- *Signature or Seal verification/validation data*: Data such as public cryptographic codes or keys used to verify electronic signatures or seals. For practical purposes relating to this *Certification Practices Statement,* they will always coincide, from a technical viewpoint, with an asymmetric, cryptographic *Public Key*.
- *Subscriber*: A person, body, organisation or entity of the Public Administration that accepts the terms and conditions of use of the service provided by the FNMT-RCM.
- *Time Stamp Practices Statement*: A statement made available to the general public through electronic means and free of charge by the FNMT-RCM as a *Time Stamp Service Provider*.
- *Time Stamping Authority (TSA)*: A trust system managed by a *Trust Service Provider*, responsible for issuing *Electronic time stamps*. From a legal viewpoint, it is a specific case of a *Trust Service Provider* and, by extension, the provider is referred to as the *Time Stamping Authority*.
- *Time Stamping* Inclusion of the date and time in an electronic document by means of indelible electronic procedures based on the specifications *Request for Comments*: 3161 – *"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)",* allowing objective document dating.
- *Time Stamping Policy (specific)*: A document that lays down the set of rules indicating the applicability of a certain type of *Time Stamp* to the *Electronic Community* and/or application class with common security requirements
- *Time Stamping Service Provider*: The natural or legal person that issues *Electronic time stamps* pursuant to *Time Stamping* legislation.
- *Time Stamping Service:* A service provided on demand by the FNMT-RCM to interested parties that request it. On the basis of the specifications of Request for Comments: RFC 3161 – "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" and ETSI

EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", documents are dated objectively so that the existence of the electronic document at that instant in time may be demonstrated beyond doubt. The FNMT-RCM will only provide this service to certain entities and related restrictions on use and the parties' obligations and responsibilities will be described in the relevant service policies and practices.

- Time Stamping Unit (TSU): A set of hardware and software managed independently which, at all times, only has one stamp key active for the issuance of Electronic time stamps.
- Triple-DES: Symmetric encryption system that has evolved from the DES (Data Encryption Standard) described in FIPS 46-3 (Federal Information Processing Standard), developing the DEA (Data Encryption Algorithm) also defined in the ANSI X9.32 standard.
- *Trust Service Provider:* A natural or legal person that provides one or more trust services, either as a qualified provider or as an unqualified provider of trust services, 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.
- *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.
- *User* (of a service) or *User party*: The natural or legal person that places trust in the electronic identification or trust service.
- *User entity*: A person, public entity or private entity that has entered into a *Contract*, *Commission* or *Agreement* with the FNMT-RCM to act in the *Electronic Community*.
- *X.500*: A standard developed by the ITU that defines the recommendations of the Directory. It corresponds to the ISO/IEC 9594-1 standard. This results in the following series of recommendations: X.501, *X.509*, X.511, X.518, X.519, X.520, X.521 and X.525.
- *X.509*: A standard developed by the ITU for *Public Key Infrastructures* and the so-called "attribute certificates".

1.6.2. Acronyms

42. For the purposes of this Trust Services Practices and Electronic Certification General Statement and, if applicable, the Specific Certification Statements related to it, the following acronyms are applicable, the meaning of which is in line with the European standard ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates":

CRL: *Certificate* Revocation List
DVC: Domain Validation *Certificate*
EV: Extended Validation
LCP: Lightweight *Certificate* Policy
NCP: Normalised *Certificate* Policy
NCP+: Extended Normalised Certificate Policy
OCSP: Online Certificate Status Protocol
OID: Object IDentifier
OVC: Organisation Validation *Certificate*
TLS/SSL: Transport Layer Security/Secure Socket Layer protocol
TSP: Trust Services Provider
UTC: Coordinated Universal Time

2. PUBLICATION AND REPOSITORIES

2.1. REPOSITORY

43. The FNMT-RCM, as a *Trust Service Provider*, has a repository of public information available 24x7, every day of the year, at the address:

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

2.2. PUBLICATION OF CERTIFICATION INFORMATION

44. Additionally, the FNMT-RCM has the following information repositories:

a. *Trust Services Practices and Electronic Certification General Statement* and *Specific Certification Policies and Practices* Access:

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

b. Electronic *Certificates* of Certification Authorities (accessible through https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt)

1. ROOT certificate AC RAIZ FNMT
   - Subordinate certificate AC Administración Publica
   - Subordinate certificate AC Components Informáticos
   - Subordinate certificate AC Representación
   - Subordinate certificate AC FNMT Usuarios
   - Subordinate certificate AC Sector Público

- Subordinate certificate AC Unidades de Sellado de Tiempo

2. ROOT certificate AC RAIZ FNMT SERVIDORES SEGUROS
   - Subordinate certificate AC Servidores Seguros Tipo 1
   - Subordinate certificate AC Servidores Seguros Tipo 2

2.3. PUBLICATION FREQUENCY

45. 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.

46. The frequency of publication of CRLs is defined in paragraph "4.9.7. CRL generation frequency".

2.4. REPOSITORY ACCESS CONTROL

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

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

48. *Certificate* encoding follows the RFC 5280 standard "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

3.1.1. Name types

49. End-entity electronic *Certificates* contain a distinguished name (DN) in the Subject Name field, composed as described in the information on the *Certificate* profile. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

3.1.2. Meaningful

50. All the distinguished names (DN) of the Subject Name field are meaningful. The description of the attributes associated with the *Certificate Subscriber* is human-readable (see section 7.1.4 Name formats of this document).

3.1.3. Pseudonymous

51. Each Particular Certification Policies Statement will determine this aspect for the *Certificates* issued under said policies.

3.1.4. Rules for interpreting various name forms

52. The requirements defined by the X.500 reference standard are applied (ISO / IEC 9594 standard).

3.1.5. Name uniqueness

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

3.1.6. Registered trademark recognition and authentication

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

3.2. INITIAL VALIDATION OF IDENTITY

55. Without prejudice to the relevant specific policies, practices and/or Issuance Laws applicable to the services, accreditation for operations, where applicable, will be carried out through a *Registration Office*.

56. The provisions of the corresponding specific *Certification Policies and Practices* for each type of *Certificate* notwithstanding, the FNMT-RCM will conduct the appropriate control procedures to check the veracity of the information included in the *Certificate.*

57. Where the *Certificate* includes details such as domain names or IP addresses, the FNMT-RCM will check, by means of the information systems made available to the general public in each case by the authorised registrars, that the correct documentation is validated by the *Registration Office*.

58. To this end, publications in Official State Gazettes and Regional Government Gazettes, public registers and registers accessible to the FNMT-RCM relating to the registrars of domain names and IP addresses will be taken into account.

3.2.1. Methods to prove possession of the private key

59. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

3.2.2. Authentication of the organisation's identity

60. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

3.2.3. Authentication of the individual applicant's identity

61. To this end, personal appearance at the *Registration Office*, submitting the official document attesting to the person's identity under prevailing legislation, will prevail over other methods. The FNMT-RCM will take into consideration the functionalities stipulated in applicable legislation in relation to national e-ID cards and other systems for identifying and verifying the *Holder*'s qualities that provide sufficient guarantees of the veracity of the data.

62. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

3.2.4. Unverified subscriber information

63. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

3.2.5. Validation of authority

64. Each Particular Certification Policies Statement will determine this aspect for the *Certificates* issued under said policies.

3.2.6. Interoperation criteria

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

3.3. IDENTIFICATION AND AUTHENTICATION FOR KEY RENEWAL REQUESTS

3.3.1. Requirements for routine re-key

66. Each Particular Certification Policies Statement will determine this aspect for the *Certificates* issued under said policies.

3.3.2. Requirements for re-key after certificate revocation

67. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

68. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4. OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFE CYCLE

69. If applicable, the life cycle of the *Certificate Holder*'s *Keys* will be managed as defined in the *Certification Policies and Specific Certification Practices* for each of the FNMT-RCM's *Certification Authorities*.

70. Without affecting the provisions of the said specific documents, in general, the FNMT-RCM will not store the *Private Keys* of *Holders* that use its certification services infrastructure.

4.1. APPLICATION FOR CERTIFICATES

4.1.1. Who may request a Certificate

71. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.1.2. Registration process and responsibilities

72. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.2. CERTIFICATE APPLICATION PROCEDURE

73. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.2.1. Performing Identification and Authentication Functions

74. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.2.2. Approval or Rejection of Certificate Applications

75. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.2.3. Time to Process Certificate Applications

76. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA actions during issuance

77. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.3.2. Subscriber notification

78. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Acceptance process

79. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.4.2. Publication of certificate by the CA

80. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.4.3. Notification of issue to other entities

81. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.5. KEY PAIR AND USE OF CERTIFICATE

82. Aspects relating to the *Trust Service Provider*'s keys are described in paragraph "6.1 Key generation and installation".

4.5.1. Subscriber's private key and use of the certificate

83. As regards the end-entity *Certificate Keys*, each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.5.2. Use of the certificate and the public key for trusting third parties.

84. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstances for renewal of a certificate

85. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.6.2. Who can request a certificate renewal

86. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.6.3. Processing of certificate renewal requests

87. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.6.4. Notification of certificate renewal

88. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.6.5. Conduct indicating acceptance of the certificate renewal

89. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.6.6. Publication of renewed certificate

90. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.6.7. Notification of certificate renewal to other entities

91. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.7. RENEWAL WITH REGENERATION OF CERTIFICATE KEYS

4.7.1. Circumstances for renewal with key regeneration

92. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.7.2. Who can request renewal with key regeneration?

93. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.7.3. Process for requesting renewal with key regeneration?

94. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.7.4. Notification of renewal with key regeneration?

95. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.7.5. Conduct indicating acceptance of renewal with key regeneration

96. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.7.6. Publication of renewed certificate

97. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.7.7. Notification of renewal with key regeneration to other entities

98. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.8. CERTIFICATE AMENDMENT

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

4.8.1. Circumstances for modification of a certificate

100. Modification is not stipulated.

4.8.2. Who can request a certificate modification?

101. Modification is not stipulated.

4.8.3. Processing of certificate modification requests

102. Modification is not stipulated.

4.8.4. Notification of certificate modification

103. Modification is not stipulated.

4.8.5. Conduct constituting acceptance of the certificate modification

104. Modification is not stipulated.

4.8.6. Publication of modified certificate

105. Modification is not stipulated.

4.8.7. Notification of certificate modification to other entities

106. Modification is not stipulated.

4.9. CERTIFICATE REVOCATION

107. *Certificates* issued by the FNMT-RCM will be revoked as stipulated in the *Certification Policies and Specific Certification Practices* applicable to each *Certificate*.

108. The effects of the revocation of the *Certificate*, i.e. its expiration, will automatically entail the expiration of the associated *Signature creation data*. These effects will arise as from the date on which the FNMT-RCM has certain knowledge of any of the determining events, which will be stated in its *Certificate status information and consultation service*.

4.9.1. Revocation circumstances

109. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.9.2. Who may apply for revocation

110. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.9.3. Revocation application procedure

111. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.9.4. Grace period for revocation application

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

4.9.5. Time period for revocation application processing

113. The FNMT-RCM immediately revokes the *Certificate* once the *Holder*'s identity is verified or, if applicable, the veracity of the application made by means of a court or administrative ruling is verified.

4.9.6. Trusting parties' obligation to verify revocations

114. 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 generation frequency

115. *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 of an *Authority certificate*; they have a 6-month validity period.

4.9.8. Maximum CRL latency period

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

4.9.9. Availability of the online certificate status verification system

117. 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 verification requirements

118. The revocation status of subordinate CA or end-entity *Certificates* may be verified online by means of the *Certificate status information service* provided through the OCSP, as described in paragraph 4.10 "Certificate status information services" 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 available revocation notification methods

119. Not defined.

4.9.12. Special revocation requirements for committed keys

120. There are no special requirements for the revocation of *Certificates* due to committed keys; the steps described for the other revocation causes are applicable.

4.9.13. Suspension circumstances

121. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

4.9.14. Who may apply for suspension?

122. The suspension of certificates is not covered.

4.9.15. Procedure for requesting suspension

123. The suspension of certificates is not covered.

4.9.16. Limits on the suspension period

124. The suspension of certificates is not covered.

4.10. CERTIFICATE STATUS INFORMATION SERVICES

125. The information of revocation status allows users to know the status of the *Certificate*, not only until it expires, but beyond its validity period, because revoked Certificates are not removed from the CRL after they have expired. In case of termination of the activity and / or commitment of keys of the CA, to guarantee the availability of the information on the status of the certificates, a last CRL will be generated and will remain intact and available for consultation for at least 15 years since its publication.

126. The provision of the information of revocation status, in case of termination of the activity of the FNMT-RCM as a Trusted Services Provider, is guaranteed by means of the transfer to another Provider with whom it is reach the corresponding agreement, of all the information related to the *Certificates* and, especially, of the data of its revocation status.

127. When the infrastructure performs the revocation of a *Certificate*, the system reflects this fact in the database consulted by the *Certificate status information and consultation service* through the OCSP, while generates a new CRL and publishes it in the LDAP repository. The aforementioned database has a backup copy. In case of any failure in the described sequence, an alarm occurs in order to correct the possible error. In this way, the consistency of the information provided by these two methods is guaranteed (OCSP and CRL query). In addition, periodic monitoring of the LDAP repository is performed as preventive maintenance.

128. Information may be consulted to verify the revocation status of electronic *Certificates* issued by the FNMT-RCM by means of CRLs and/or the *Certificate status information and consultation service* through the OCSP, accessible as follows:

- AC RAIZ FNMT hierarchy

  a. Certificate Revocation Lists:

     i. ROOT CA "AC RAIZ FNMT-RCM" Accesses:

        - ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint
        - http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

     ii. Subordinate CA "AC Administración Pública". Accesses:

        - ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,CN=AC%20Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

- http://www.cert.fnmt.es/crlsacap/ CRL<xxx*>.crl

iii. Subordinate CA "AC Componentes Informáticos". Accesses:

- ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>,OU=AC%20Componentes%20Informaticos,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
- http://www.cert.fnmt.es/crlscomp/CRLxxx*.crl

iv. Subordinate CA "AC Representación". Accesses

- ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
- http://www.cert.fnmt.es/crlsrep/CRLnnn.crl

v. Subordinate CA "AC FNMT Usuarios". *Accesses*

- ldap://ldapusu.cert.fnmt.es/CN=CRL<xxx*>, CN=AC%20FNMT%20Usuarios, OU=CERES, O=FNMT-RCM, C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

*xxx: whole number identifying the CRL (partitioned CRLs)

vi. Subordinate CA "AC Sector Público"

- ldap://ldapsp.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Sector%20Publico,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

*xxx: whole number identifying the CRL (partitioned CRLs)

vii. Subordinate CA "AC Unidades de Sellado de Tiempo"

- http://www.cert.fnmt.es/crlsacst/CRL.crl

b. Certificate status verification service (OCSP):

i. ROOT CA. "AC RAIZ FNMT-RCM".Access:

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

ii. Subordinate CA "AC Administración Pública". Access:

http://ocspap.cert.fnmt.es/ocspap/OcspResponder

iii. Subordinate CA "AC Componentes Informáticos". Access:

http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder

iv. Subordinate CA "AC Representación". Access:

http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder

v. Subordinate CA "AC FNMT Usuarios".Access

http://ocspusu.cert.fnmt.es/ocspusu/OcspResponder

vi. Subordinate CA "AC Sector Público"

http://ocspsp.cert.fnmt.es/ocspsp/OcspResponder

vii. Subordinate CA "AC Unidades de Sellado de Tiempo"

http://ocspst.cert.fnmt.es/ocspst/OcspResponder

- AC RAIZ FNMT-RCM "SERVIDORES SEGUROS" hierarchy

a. Certificate Revocation Lists:

i. AC RAIZ FNMT-RCM "SERVIDORES SEGUROS". Acceso:

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

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

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

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

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

b. Certificate status verification service (OCSP):

i. AC RAIZ FNMT-RCM "SERVIDORES SEGUROS". Acceso:

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

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

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

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

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

4.10.1. Operational features

129. The *Certification status information and consultation service* works as follows: the FNMT-RCM's OCSP server receives an OCSP request made by an OCSP Client and checks the status of the *Certificates* included in it. If the request is valid, an OCSP response will be issued on the status at that moment of the *Certificates* included in the request. This OCSP response is

signed using the *Signature/Seal Creation Data* associated with the OCSP server specific to each CA, thus guaranteeing the integrity and authenticity of the information supplied on the revocation status of *Certificates* consulted.

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

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

4.10.2. Service availability

132. The FNMT-RCM guarantees 24x7 access to this service, barring circumstances beyond the FNMT-RCM's control or maintenance operations. The FNMT-RCM will post a notification of the latter circumstance at http://www.ceres.fnmt.es at least forty-eight (48) hours in advance, if possible, and will try to resolve it within twenty-four (24) hours. The service will be accessible to all *Certificate* users, holders and trusting parties securely, quickly and free of charge.

4.10.3. Optional features

133. No stipulation.

4.11. END OF SUBSCRIPTION

134. The subscription will end when the *Certificate* ceases to be valid. If the *Certificate* is not renewed, the relationship between the *Subscriber* and FNMT-RCM will be deemed to have expired.

135. *Certificates* 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, once evidence that the *Subscribers* do not object has been obtained, 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 the relevant *Certification Practices Statement*.

4.12. KEY CUSTODY AND RECOVERY

4.12.1. Key custody and recovery practices and policies

136. The FNMT-RCM will not recover the *Private keys* of the *Certificate Holders*.

4.12.2. Session key protection and recovery practices and policies

137. Not stipulated.

5. PHYSICAL SECURITY, PROCEDURE AND PERSONNEL CONTROLS

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

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

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

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

5.1. PHYSICAL SECURITY CONTROLS

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

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

5.1.1. Location of facilities

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

5.1.1.1. Data Processing Centre location

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

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

5.1.2. Physical access

5.1.2.1. Physical security perimeter

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

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

5.1.2.2. Physical entry controls

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

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

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

5.1.2.3. Work in secure areas

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

5.1.2.4. Visits

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

5.1.2.5. Separate loading and unloading areas

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

5.1.3. Electricity and air conditioning

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

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

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

5.1.3.1. Cabling security

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

5.1.4. Water exposure

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

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

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

5.1.6.1. Information recovery

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

5.1.7. Waste elimination

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

5.1.8. Backups outside facilities

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

5.2. PROCEDURE CONTROLS

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

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

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

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

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

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

169. The FNMT-RCM, through its Code of Conduct Review Committee, oversees compliance with the Code to avoid situations that could result in a conflict of interest. Additionally, the specific regulations[1] that apply to trust roles, as civil servants, guarantee the impartiality of the operations in the activity of the FNMT-RCM, in its activity as Trust Services Provider.

5.2.1. Trusted roles

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

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

5.2.2. Number of persons per task

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

5.2.3. Role identification and authentication

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

5.2.4. Roles requiring the segregation of functions

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

5.3. PERSONNEL CONTROLS

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

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

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

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

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

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

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

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

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

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

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

5.3.1. Knowledge, qualifications, experience and accreditation requirements

184. All the personnel involved in the activity of the FNMT-RCM, as a Trusted Service Provider, and especially the managerial staff, possess necessary experience and knowledge to manage said activity. These requirements are guaranteed by the corresponding criteria in the personnel selection processes so that the employee's professional profile is as appropriate as possible to the characteristics of the tasks to be developed.

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

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

5.3.2. Background verification procedures

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

5.3.3. Training requirements

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

5.3.4. Refresher training requirements and frequency

189. The FNMT-RCM implements ongoing training plans, paying particular attention to substantial modifications of *Trust Service* infrastructure operations.

5.3.5. Employee turnover sequence and frequency

190. Not stipulated.

5.3.6. Penalties for unauthorised actions

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

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

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

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

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

5.3.7. Personnel hiring requirements

195. Personnel recruitment and policies are included in the Collective Agreement regulating work relationships between the FNMT-RCM and its employees, as well as in legislation applicable to the civil service and the related Statute (Royal Decree 1114/1999 of 25 June adapting the Spanish Mint to Law 6/1997 of 14 April on the Organisation and Functioning of the General State Administration, approving its Statute and agreeing on the name *Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda* and its status as a State-owned enterprise attached to the Ministry of Economy and Finance (now Ministry of Finance)).

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

5.3.7.1. Third-party contracting requirements

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

5.3.8. Supply of documentation to personnel

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

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

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

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

5.4. AUDIT PROCEDURES

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

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

5.4.1. Event types logged

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

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

206. All events logged may be audited.

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

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

- Management monitoring logs.
- Design, development and related review logs.
- Corrective action logs.
- Customer satisfaction logs.
- System review logs.
- Other logs.

5.4.2. Log processing frequency

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

5.4.3. Log retention period

210. Audit logs will be held for at least fifteen (15) years.

5.4.4. Log protection

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

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

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

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

5.4.5. Audit log backup procedures

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

5.4.6. Log collection system

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

5.4.7. Notification to party causing the events

217. Not envisaged.

5.4.8. Vulnerability analysis

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

5.5. LOG ARCHIVING

5.5.1. Log types archived

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

220. The following will be logged:

- Issuance, revocation and other relevant events related to the *Certificates*, as well as operations related to the management of the *Trust Service Provider*'s keys and *Certificates*.

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

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

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

5.5.2. Archive retention period

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

5.5.3. Archive protection

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

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

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

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

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

5.5.4. Archive backup procedures

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

5.5.5. Log time stamping requirements

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

5.5.6. Archive system

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

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

5.5.7. Procedures to obtain and verify information archived

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

5.6. CHANGE OF CA KEYS

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

5.7. INCIDENT AND VULNERABILITY MANAGEMENT

5.7.1. Incident and vulnerability management

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

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

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

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

5.7.2. Actions relating to corrupt data and software

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

5.7.3. Procedure if the CA's private key is compromised

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

1) Stop providing the affected service.
2) Revoke any certificates that might be affected.
3) Execute the Communication Plan to notify of the events affected parties and to the browsers in whose root programs the FNMT-RCM certificates are included.
4) Study the need to execute the Discontinuance of the CSP's Activities as per the Certification Practices Statement and prevailing legislation.

5.7.4. Business continuity following a disaster

238. The FNMT-RCM has a business continuity plan describing the actions to be implemented in case of disaster. So, it has a backup system that stores in safe places the data necessary to resume CA operations in case of incident/disasters, even in the alternative support centre, in

order to ensure that all essential information and software can be recovered following a disaster or media failure.

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

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

- Redundancy of the most critical components.
- Start-up of an alternative support centre.
- Full, periodic checking of backup copy services.
- Compromised *Signature creation data* of the *Trust Service Provider or algorithm compromise that leads a real threat, considering the current state of the art, identity impersonation*. In these cases, the FNMT-RCM will schedule the revocation of the affected *Certificates* and will inform all members of the *Electronic Community* that all the *Certificates*, *Revocation Lists*, *Electronic time stamps* and any other data structure able to be signed are no longer valid due to the compromised data. The FNMT-RCM will restore the service as soon as possible and on the new terms applicable.

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

5.8. DISCONTINUANCE OF THE TRUST SERVICE PROVIDER'S ACTIVITIES

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

243. In any case, the FNMT-RCM:

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

- The *Supervisory body* will be informed of the discontinuance of the activity and the destination of the *Certificates*, specifying, if applicable, whether they are to be transferred or will expire. That body must be notified at least two (2) months in advance by means of a document signed by hand or electronically.

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

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

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

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

6. TECHNICAL SECURITY CONTROLS

6.1. KEY GENERATION AND INSTALLATION

6.1.1. Key pair generation

6.1.1.1. CA Key Pair Generation

246. The FNMT-RCM possess a procedure described in the document "Gestión del ciclo de vida de las claves de la FNMT-RCM como Prestador de Servicios de Certificación y Sellado", for conducting CA key pair generation for all CAs, whether root CAs or subordinate CAs that issue certificates to end users. As a result of this procedure, a report is produced proving that ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair is ensured. This report is signed by the persons who exercise the corresponding trust roles in the generation of *Keys* of a subordinate CA, and in the case of a root CA will be additionally signed by a reliable and independent assessment body. This procedure describes the following:

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

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

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

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

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

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

6.1.1.2. RA Key Pair Generation

252. No stipulation.

6.1.1.3. Subscriber Key Pair Generation

253. *Certificate Holder*'s *Private keys* are generated and custodied as described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.1.2. Sending of private key to the subscriber

254. The sending of the *Certificate Holder*'s *Private keys* is described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.1.3. Sending of public key to the certificate issuer

255. The sending of the *Certificate Holder*'s *Public keys* is described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.1.4. Distribution of the CA's public key to the trusting parties

256. The *Signature Verification Data* of the *Trust Service Provider* are distributed in a format that meets market standards and may be consulted at www.cert.fnmt.es.

257. In order to check the authenticity of any "self-signed *Certificate*", the final element in any *Certification Chain*, the relevant digital fingerprint may be verified (in different formats; see the section 1.3.1 *"Certification Authority"*).

6.1.5. Key sizes and algorithms used

258. The algorithm used is RSA with SHA-256 for the CA FNMT root hierarchy and ecdsa-with-SHA384 for the CA FNMT root "SERVIDORES SEGUROS" certificate.

259. The *Key* size, depending on each case, is:

- AC RAIZ FNMT-RCM root CA *Keys:* 4096 bits.

- AC RAIZ FNMT-RCM SERVIDORES SEGUROS root CA Keys: ECC P-384 bits.
- Keys of the FNMT Subordinate CAs that issue end-entity *Certificates*: described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.
- Keys of the end-entity *Certificates*: described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.1.6. Public key generation parameters and quality verification

260. The *Public keys* for the *Certificates* are encoded under RFC5280 and PKCS#1.

6.1.7. Permitted uses of keys (KeyUsage field X.509v3)

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

262. The authorised *Key* uses of the FNMT root CA *Certificate* are the signing/sealing of FNMT Subordinate CA Certificates and ARLs.

263. The authorised uses of the *Certificates* of the FNMT Subordinate CAs that issue end-entity *Certificates* are exclusively the signing/sealing of end-user *Certificates* and CRLs.

264. The uses of end-entity *Certificate Keys* are described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE CONTROLS

6.2.1. Cryptographic module standards

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

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

6.2.2. Private key multi-person control (n of m)

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

6.2.3. Private key custody

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

269. The *Holders*' *Private Keys* are held, at a high level of trust, under the exclusive control of the *Holder*. Each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

6.2.4. Private key backup

270. A copy is kept of the files and components in case of the need to restore the cryptographic device's security environment, in security envelopes duly custodied inside a fire-resistant cabinet, which may only be accessed by authorised personnel.

6.2.5. Private key filing

271. The FNMT-RCM may make a backup of the *Private keys,* guaranteeing that the security level of the copied data is at least equal to that of the original data and that the number of data duplicated does not exceed the minimum necessary to assure service continuity. The *Signature creation data* are not duplicated for any other purpose. Nonetheless, each Specific Certification Policy Statement will determine this aspect for the *Certificates* issued under the policy.

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

272. The *Certification Authorities*' *Private keys* are generated as described in point "6.1 *Key* generation and installation". Consequently, the *Keys* cannot be transferred, although there is a recovery procedure as a contingency measure, as described in point "6.2.4 Private key backup".

6.2.7. Storage of private key in the cryptographic module

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

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

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

6.2.8. Private key activation method

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

276. The mechanisms for the activation and use of end-entity *Certificate Private keys* are described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.2.9. Private key deactivation method

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

278. The deactivation of end-entity *Certificate Private keys* is described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.2.10. Private key destruction method

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

280. In the case of end-entity *Certificate Private keys*, this method is described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.2.11. Cryptographic module classification

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

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key filing

282. The FNMT-RCM will keep the *Holder*'s *Public Key* and evidence of possession of the *Private Key* (*Public Key* encrypted with the *Private Key*) in accordance with prevailing legislation, for a period of not less than 15 years after the expiration of the validity of the associated certificate.

6.3.2. Certificate operating periods and key pair usage periods

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

- FNMT root CA *Certificate* and its *Key* pair: to 1 January 2030.

- FNMT root "SERVIDORES SEGUROS" CA Certificate and its *Key* pair: to 20 December 2043.
- *Certificates* of subordinate CAs that issue end-entity *Certificates*: described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.
- End-entity *Certificates*: described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

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

285. As regards the deactivation data for end-entity *Certificate Keys*, a description is provided in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

6.4.2. Activation data protection

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

6.4.3. Other aspects of activation data

287. Not stipulated.

6.5. IT SECURITY CONTROLS

6.5.1. Specific technical requirements for IT security

288. When defining security for all the technical components used by the FNMT-RCM in the course of its *Trust Service Provider* activities and in its structure and procedures, all aspects of Information System security certification are taken into consideration, in accordance with the National Information System Security Certification Framework approved in Spain, in particular those relating to EESSI published in the Official Journal of the European Union or in the relevant Spanish Official Journals. Information technology security evaluation under ISO 15408 (Common Criteria) is also taken into account in the design, development, evaluation and acquisition of IT products and systems for use by the *Trust Service Provider*, in addition to the EESSI regulations.

289. Infrastructure security management processes will be evaluated periodically.

6.5.1.1. Notification of security incidents

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

6.5.1.2. Notification of security weaknesses

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

6.5.1.3. Notification of software failures

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

6.5.1.4. Learning from incidents

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

6.5.2. IT security level evaluation

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

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

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

6.6. TECHNICAL LIFE CYCLE CONTROLS

6.6.1. System development controls

297. Before undertaking a software development project, the *Trust Service Provider* follows the "Guidelines for the establishment of security requirements for applications developed by

Ceres". This guarantees that computer applications developed undergo a risk assessment process and an analysis of security requirements.

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

6.6.2. Security management controls

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

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

6.6.3. Life cycle security controls

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

6.6.3.1. Algorithm update

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

6.7. NETWORK SECURITY CONTROLS

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

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

305. The means of communication through public networks employed by the FNMT-RCM in its activities are equipped with sufficient security mechanisms to avoid or adequately control any

external aggression through these networks. This system is audited periodically to check that it functions correctly.

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

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

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

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

6.8. TIME SOURCE

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

6.9. OTHER ADDITIONAL CONTROLS

6.9.1. Service provision capacity control

311. The FNMT-RCM periodically controls the level of demand for services related to its *Trust Service Provider* services and the capacity of its infrastructure to provide the services, such as the information system for resource consumption, availability and occupancy. These controls allow future infrastructure investments to be identified in order to maintain service provision capacity.

6.9.2. IT systems and applications development control

312. Before undertaking any new software development project, or in case a change in an existing development is required, the establishment of additional controls to those specified in the current procedures will be evaluated.

7. CERTIFICATE PROFILES, CRLS AND OCSP

7.1. CERTIFICATE PROFILE

313. All *Certificates*, in order to be treated as such and to avoid alteration or falsification, must be signed with the FNMT-RCM's *Signature creation data* as a *Trust Service Provider*.

7.1.1. Version number

314. All the *Certificates* issued by the FNMT-RCM comply with the standard defined by the International Telecommunications Union, Telecommunication Standardisation Sector, in ITU-T X.509, dated June 1997, or higher (ISO/IEC 9594-8), version 3, unless the *Certification Policies* and *Specific Certification Practices* state otherwise for *Certificates* to which they are applicable.

7.1.2. Certificate extensions

315. An appendix to this document provides the full profile of the FNMT-RCM ROOT AC *Certificate*.

316. The document describing the profiles of the *Certificates* issued by the FNMT-RCM, including all extensions, is published at http://www.cert.fnmt.es/dpcs/.

7.1.3. Algorithm object identifiers

317. The object identifier (OID) relating to the cryptographic algorithm used (SHA-256 with RSA Encryption) is 1.2.840.113549.1.1.11.

7.1.4. Name formats

318. *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 restrictions

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

7.1.6. Certificate policy object identifier

320. The object identifier (OID) of the policy for *Certificates* issued by the FNMT-RCM is described in each *Certification Policies Statement* and *Specific Certification Practices* defined for each *Trust Service*.

7.1.7. Use of the policy constraints extension

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

7.1.8. Syntax and semantics of policy qualifiers

322. 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 a text that may drop down on the *Certificate* user's screen during verification.

7.1.9. Semantic treatment of the certificate policy extension

323. 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

324. The format of the *Revocation Lists* published by the FNMT-RCM follows the profile proposed in recommendation ITU-T X.509, version 2, on *Revocation Lists*.

7.2.2. CRL and extensions

325. The CRL profile has the following structure:

Table 2 – CRL profile

Fields and extensions	Value
Version	V2

Fields and extensions	Value
Signature algorithm	Sha256WithRSAEncryption for the CA FNMT root. ECDSA-with-SHA384 for the CA FNMT root "SERVIDORES SEGUROS".
CRL number	Incremental value
Issuer	Issuer DN
Issuance date	UTC issuance time
Date of next upgrade	Issuance date + 24 hours (except for ARL, that it is Issuance date + 1 year).
Authority key identifier	Issuer key hash
ExpiredCertsOnCRL	NotBefore CA value
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

326. 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

327. *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

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

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

8. COMPLIANCE AUDITS

330. The system for issuing *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".

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

332. The *Qualified Time Stamping Service* offered by the FNMT-RCM is subject to annual audits, in accordance with the certification scheme for *Trusted Service Providers*, in terms of compliance with the requirements defined by the European standards ETSI EN 319 401 "General Policy Requirements for Trusted Service Providers", ETSI EN 319 421 "Trusted Service Providers issuing Time-Stamps" and ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles".

333. The Server signing service offered by the FNMT-RCM is subject to annual audits, in accordance with the certification scheme for *Trusted Service Providers*, in terms of compliance with the requirements defined by the European standard ETSI EN 319 401 "General Policy Requirements for Trusted Service Providers".

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

- Audit of the Information Security Management System in accordance with UNE-ISO / IEC 27001 "Information Security Management Systems. Requirements".
- Audit as ruled in the National Security Scheme (Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration).
- Audit of the Quality Management System according to ISO 9001.
- Audit of the Social Responsibility Management System in correspondence with IQNet SR10.
- Audit of the Business Continuity Plan according to ISO 22301.

- Audit in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/, and Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (RGPD / LOPD-GDD).

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

8.1. AUDIT FREQUENCY

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

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

8.2. AUDITOR QUALIFICATIONS

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

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

8.3. AUDITOR'S RELATIONSHIP WITH THE COMPANY AUDITED

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

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

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

8.4. ASPECTS AUDITED

343. The following controls will be carried out:

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

8.5. DECISION-MAKING ON WEAKNESSES DETECTED

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

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

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

8.6. NOTIFICATION OF FINDINGS

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

8.7. SELF-AUDITS

348. Additionally, the FNMT-RCM performs internal audits to self-assess compliance with its *Certification Policies*, *Certification Practices Statement*, applicable regulations, and the requirements established by the CA / Browser forum and to control the quality of the provision of services. These internal audits are carried out at least quarterly, taking a randomly selected sample of at least 3% of the *Certificates* issued during the period that begins immediately after the previous self-assessment sample.

9. OTHER LEGAL AND BUSINESS MATTERS

9.1. FEES

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

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

9.1.1. Certificate issuance or renewal fees

351. 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

352. Not stipulated.

9.1.3. Status or revocation information access fees

353. The FNMT-RCM provides *Certificate* status information services free of charge by means of CRLs or the OCSP.

9.1.4. Fees for other services

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

9.1.5. Refund policy

355. Each *Certification Policies Statement* and *Specific Certification Practices* may define a refund policy for each *Trust Service.*

9.2. FINANCIAL LIABILITY

356. The FNMT-RCM has the necessary human, material and financial resources to reasonably cover the application requirements of each declared policy. As a governmental Entity attached to the Ministry of Finance, in patrimonial matters, Law 33/2003, of November 3, of the Patrimony of Public Administrations and its Statute (currently approved by Royal Decree 1114 / 1999, of June 25), in terms of adequacy, sufficiency, effective application,

identification and control of their assets to serve the public service to which they are intended. Additionally, although the national regulations on the provision of trust services establish the exemption of the FNMT-RCM, due to its governmental nature, about the constitution of a civil liability insurance to exercise as a qualified trust services provider, this Entity possess, voluntarily, said insurance, as defined in the following section.

9.2.1. Third-party liability insurance

357. The FNMT-RCM, as a *Trust Service Provider*, as well as a Spanish government body, has third-party liability insurance covering its *Trust Service Provider* activities, with a coverage limit of above €3,000,000.

9.2.2. Other assets

358. No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

359. No stipulation.

9.3. INFORMATION CONFIDENTIALITY

9.3.1. Scope of confidential information

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

9.3.2. Information not included in the scope

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

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

9.3.3. Responsibility to protect confidential information

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

9.4. PERSONAL DATA PROTECTION

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

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

9.4.1. Privacy plan

364. The processing of personal data carried out by the FNMT-RCM aligns with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter GDPR) as well as the requirements that are application by specific national regulations in this matter.

9.4.2. Information treated as private

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

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

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

9.4.3. Information not deemed private

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

9.4.4. Responsibility to protect private information

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

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

9.4.4.1. Data Protection Officer

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

9.4.4.2. Records of processing activities

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

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

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

9.4.4.3. Subject's rights

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

9.4.4.4. Cooperation with the Authorities

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

9.4.4.5. Notification of personal data breach

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

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

9.4.5. Notice and consent to use private information

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

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7. Other Information Disclosure Circumstances

380. No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

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

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

383. The FNMT-RCM holds all rights, title and interest to all intellectual and industrial property and knowledge related to this *DGPC*, the statements (policies and practices) specifying or

completing this *DGPC*, the services provided and the computer programs or hardware used to provide them. Any other use other than viewing, including the reproduction, redistribution and / or modification of this *DGPC* as well as the declarative documents (policies and practices) that specify and complete this *DGPC*, is prohibited without the express authorization of the FNMT-RCM.

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

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

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

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

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

9.6. OBLIGATIONS AND GUARANTEES

388. The obligations and responsibilities of the FNMT-RCM, as a *Trust service provider*, of the *Certificate Holder* and of the other participants will be determined mainly by the document on the terms and conditions of use or *Certificate* issuance agreement and, secondarily, by this *Certification Practices and Policies Statement* and the relevant *Specific Certification Policies and Practices*. Nonetheless, and in general, the participants' obligations in the *Certificate* issuance and acceptance process are as follows:

9.6.1. CA's obligations

9.6.1.1. Prior to Certificate issuance

389. a) Check the identity and personal circumstances of the *Certificate Holders* pursuant to the provisions of this *Certification Practices and Policies Statement*. *Certificates* will not be issued for minors, unless they are and provide evidence of being emancipated minors.

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

c) Check that the *Certificate Applicant* controls the *Private Key* that, once the *Certificate* is issued, will form the *Signature creation data* relating to the *Signature verification data* that will appear in the *Certificate*, and verify that they are complementary.

9.6.1.2. Holder identification

390. a) Identify the natural person that requests a *Certificate*, requiring, in general, personal appearance and possession of the national ID card or alien ID card. Identification will take place following the registration procedure approved by the FNMT for this purpose.

b) The FNMT-RCM may involve the authorised *Registration Offices* or third parties holding notarised powers to participate in the processes undertaken to verify the above aspects.

9.6.1.3. Generation of signature creation data and additional information

391. a) Guarantee that the procedures followed assure that the *Private Keys* forming the *Signature creation data* are generated under the *Holder*'s exclusive control.

b) Make the following information available to the *Applicant* (http://www.ceres.fnmt.es):

i. Instructions for the *Holder*, in particular:
   - The way in which the information necessary to access the *Signature creation data* must be custodied.
   - General mechanisms guaranteeing the reliability of a document's *Electronic signature*.
   - Procedure for notifying the loss of access or undue use of the data.
   - Conditions applicable to the use of the *Certificate*, limits on use and the way in which liability for assets is guaranteed.

ii. A description of the method employed by the FNMT-RCM to verify the *Holder*'s identity and other data included in the *Certificate*.

iii. Certification obtained by the FNMT-RCM.

iv. Applicable dispute resolution procedure.

v. A copy of this *Certification Practices and Policies Statement*, available through the FNMT-RCM's *Electronic Site*.

9.6.1.4. Preservation of information by the FNMT-RCM

392. a) Keep all information and documentation relating to each *Certificate* securely for fifteen (15) years as from the issuance date, so that the relevant signatures made may be verified.

b) Keep a secure, up-to-date repository of *Certificates* identifying *Certificates* issued and their validity, including *Revocation Lists* of *Certificates* revoked or suspended. The integrity of this *Directory* will be protected using systems that comply with specific regulations issued in Spain and, if applicable, in the EU.

c) Provide a *Certificate validity status information and consultation service*.

d) Put in place a dating mechanism to precisely determine the date and time of issuance, expiration or suspension of a *Certificate*.

e) Securely keep this *Certification Practices and Policies Statement* for 15 years following its amendment or repeal due to the publication of a new statement.

9.6.1.5. Personal Data Protection

393. The FNMT-RCM undertakes to know and comply with prevailing personal data protection legislation, basically Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights. It also guarantees that the use of the personal data collected will be limited to the purposes for which they were obtained.

9.6.2. RA's obligations

394. The *Registration Offices* of the FNMT *Registration Authority* are obligated to:

i) Verify irrefutably the identity and any personal circumstances of the *Applicants* of the *Certificates* relevant to the purposes for which they are intended, using any of the means permitted by law and in accordance with this *Certification Practices and Policies Statement*.

ii) Preserve for the period of time stipulated in prevailing legislation all information and documentation relating to *Certificates* the application, renewal or revocation of which is managed.

iii) Allow the FNMT-RCM to access the archives and audit their procedures in relation to the data obtained as a *Registration Office*.

iv) Report to the FNMT-RCM any aspect that may affect the *Certificates* issued by the Entity (e.g. applications for issuance, renewal…).

v) Diligently report *Certificate* issuance requests to the FNMT-RCM.

vi) As regards the expiration of *Certificates*:

1. Diligently check the causes for revocation that could affect the validity of *Certificates*.
2. Diligently report *Certificate* revocation requests to the FNMT-RCM.

vii) As regards personal data protection, the provisions of the relevant section of this *Certification Practices and Policies Statement* will be applicable.

viii) The *Registration Offices*, through the personnel assigned to the service as employees or public officials, must carry out public functions pursuant to the specific legislation applicable to the FNMT-RCM.

395. In any event, the FNMT-RCM may bring an action for recovery against a *Registration Office* that performs the identification procedure if damage is caused by the latter's wilful misconduct or negligence.

9.6.3. Holders' obligations

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

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

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

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

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

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

402. The Holder will be responsible for informing the FNMT-RCM of any change affecting his or her status or information reflected in the Certificate so it may be revoked and a new Certificate may be issued.

403. The Holder will also be answerable to the members of the Electronic Community and other User entities or, if applicable, to third parties for the undue use of the Certificate, or for the falseness of the declarations contained in it, or for acts or omissions causing harm to the FNMT-RCM or third parties.

404. The Holder will have the responsibility and thus the obligation not to use the Certificate in the event that the Trust service provider has discontinued its activities as an issuer of Certificates and the subrogation envisaged in the law has not taken place. In any event, the Holder must not use the Certificate where the Provider's Signature/Seal creation data may be jeopardised and/or compromised and the Provider has notified this or, if applicable, the Holder has become aware of these circumstances.

9.6.4. Trusting parties' obligations

405. The rest of the *Electronic Community*, *User entities* and third parties will regulate their relations with the FNMT-RCM through the *DGPC* and, if applicable, through this *Certification Practices and Policies Statement*, all without prejudice to the provisions of electronic signature legislation and other applicable laws.

406. Without affecting the content of the preceding paragraph, the members of the *Electronic Community*, *User entities* and third parties that place their trust in the *Certificates* and in the *Electronic signatures* generated using them will comply with the following obligations, holding the *Trust Service Provider* harmless from liability if any are not fulfilled:

- Verify, before placing their trust in the *Certificates*, the advanced *Electronic signature* or *Electronic Seal* of the *Trust Service Provider* that issued the *Certificate*.
- Check that the *Holder*'s *Certificate* is still valid.
- Verify the status of the *Certificates* in the *Certification Chain* by consulting the FNMT-RCM's *Certificate validity status information and consultation service*.
- Check the restrictions on use contained in the *Certificate* verified.
- Ascertain the terms and conditions of use of the *Certificate* pursuant to this *Certification Practices and Policies Statement*.
- Notify the FNMT-RCM or any *Registration Office* of any anomaly or information relating to the *Certificate* that might be regarded as a cause for revocation, providing all evidence available.

407. The User entity and third parties that place their trust in the Certificates issued by the FNMT-RCM, unless this obligation is contracted with the latter entity, will be responsible for verifying the Electronic signatures in documents and in Certificates; they must not in any event presume the authenticity of the documents or Certificates without such verification.

408. The User entity may not be deemed to have acted with the minimum due diligence if it trusts an Electronic signature based on a Certificate issued by the FNMT-RCM without having observed the provisions of this Certification Practices and Policies Statement and checked that the Electronic signature may be verified by reference to a valid Certification Chain.

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

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

9.6.5. Other participants' obligations

411. The FNMT-RCM in the provision of its service as a Time Stamping Authority, is responsible for any variation in the time reference, in relation to the source supplied by the Time Section of the Spanish Royal Navy's Institute and Observatory, which is introduced into the Electronic Time Stamps when the request is made, and has no responsibility whatsoever for the truthfulness and contents represented by the electronic data sent by the entities using the service that are subject to the Electronic Time Stamp issued.

9.7. WAIVER OF GUARANTEES

412. Not stipulated.

9.8. LIMITATIONS OF LIABILITY

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

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

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

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

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

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

419. The FNMT-RCM in the provision of its service as a Time Stamping Authority, shall not be held responsible for any damage or harm and/or defective operations that the Electronic Time

Stamps that it issues cause as a result of the uses that are made of them, either due to the fault of interested parties or defects in the original data.

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

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

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

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

9.9. INDEMNITIES

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

9.9.1. Indemnification by CAs

425. Not stipulated.

9.9.2. Indemnification by Subscribers

426. Not stipulated.

9.9.3. Indemnification by Relying Parties

427. Not stipulated.

9.10. VALIDITY PERIOD OF THIS DOCUMENT

9.10.1. Period

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

9.10.2. Termination

429. 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

430. 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 NOTIFICATIONS AND COMMUNICATION WITH PARTICIPANTS

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

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

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

9.12. AMENDMENTS TO THIS DOCUMENT

9.12.1. Amendment procedure

434. Amendments to this *Certification Practices and Policies Statement* will be approved by Ceres Department management which is integrated into the TSP Management Committee. Updates 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 period and mechanism

435. The *Trust Service Provider*'s Management Committee will review these Statements annually and, in any event, whenever any amendment is necessary.

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

437. 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 in which an OID must be changed

438. 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. CLAIMS AND DISPUTE RESOLUTION

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

9.14. APPLICABLE LEGISLATION

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

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

- Law 6/2020 (11 November) regulating of certain aspects of electronic trust services.
- Law 39/2015 (1 October) on the Common Administrative Procedure for Public Administrations.
- Law 40/2015 (1 October) on the Public Sector.
- Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights.

- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- Royal Decree 366/2007, of March 16, which establishes the conditions of accessibility and non-discrimination of persons with disabilities in their relations with the General State Administration.
- Royal Decree 505/2007, of April 20, which approves the basic conditions of accessibility and non-discrimination of persons with disabilities for the access and use of urbanized public spaces and buildings.

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

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

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

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

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

9.15. COMPLIANCE WITH APPLICABLE LEGISLATION

446. The FNMT-RCM declares that it complies with applicable legislation.

9.16. SUNDRY STIPULATIONS

9.16.1. Entire agreement

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

9.16.2. Assignment

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

9.16.3. Severability

449. Not stipulated.

9.16.4. Enforcement

450. Not stipulated.

9.16.5. Force Majeure

451. Not stipulated.

9.17. OTHER STIPULATIONS

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

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

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

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

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

457. The organizational structure of the FNMT-RCM guarantees that the units related to the *Certificate* generation and revocation management are independent of other units for its decisions relating to the establishing, provisioning and maintaining and suspension of services in conformance with the applicable certificate policies. The document "P.E.CE.21007.- ORGANIZACION DEL DEPARTAMENTO DE CERES" defines this organizational structure. Additionally, the legal nature of the FNMT-RCM, as a governmental entity attached to the General State Administration, guarantees that its senior executive, senior staff and staff in trusted roles are free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

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

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

APPENDIX: FNMT-RCM ROOT CERTIFICATE PROFILE

Field		Content	Critical ext.
1. Version		2	
2. Serial Number		Unique Certificate ID Number	
3. Signature Algorithm		Sha256withRsaEncryption	
4. Issuer Distinguished Name		Certificate Issuer (Root CA)	
	4.1. Country	C=ES	
	4.2. Organisation	Name (organization's "official" name) of the trust service provider (certificate issuer). O=FNMT-RCM	
	4.3. Organisation Unit	OU=AC RAIZ FNMT-RCM	
5. Validity		To 01/01/2030	
6. Subject			
	6.1. Country	C=ES	
	6.2. Organisation	Name (organization's "official" name) of the trust service provider (certificate issuer). O=FNMT-RCM.	
	6.3. Organisation Unit	OU=AC RAIZ FNMT-RCM	
7. Subject Public Key Info		Algorithm: RSA Encryption Length: 4096 bits	
8. Subject Key Identifier		CA's public key identifier Means to identify certificates containing a specific public key and facilitate the building of certification routes.	
9. Key Usage		Permitted use of keys certified.	Yes
	9.1. Digital Signature	0	
	9.2. Content Commitment	0	
	9.3. Key Encipherment	0	
	9.4. Data Encipherment	0	

Field			Content	Critical ext.
	9.5. Key Agreement		0	
	9.6. Key Certificate Signature		1	
	9.7. CRL Signature		1	
10. Certificate Policies			Certification Policy	
	10.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	
	11.2. Policy Qualifier Id			
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	
11. Basic Constraints				Yes
	11.1. cA		TRUE value (CA)	
	11.2. pathLenConstraint		None	

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

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

Field		Content	Critical ext.
	9.6. Key Certificate Signature	1	
	9.7. CRL Signature	1	
10. Basic Constraints			Sí
	10.1. cA	Value TRUE (CA)	
	10.2. pathLenConstraint	None	