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 / 5.1	17/12/2016
Revised by:	FNMT-RCM / 5.1	29/12/2016
Approved by:	FNMT-RCM / 5.1	03/01/2017

BACKGROUND OF THE DOCUMENT			
Version	**Date**	**Description**	**Author**
		Certification Practices Statement (of all of the certification policies of the FNMT-RCM)	FNMT-RCM
3.0	05/05/2009	Creation of the document	FNMT-RCM
3.1	04/01/2010	Updating of aspects relating to the time stamping service	FNMT-RCM
3.2	22/06/2010	It reflects a new chain of confidence for the provision of certification services for the Public Administration. New security controls are included to increase the guarantees and trust in the services. A specific section is included to identify the FNMT-RCM as Certification Services Provider.	FNMT-RCM
3.3	19/12/2011	*Certification Policies* are included in a specific paragraph.	FNMT-RCM
3.4	20/01/2012	A Redrafting of paragraph 12.1 is included describing the resale services conditions.	FNMT-RCM

BACKGROUND OF THE DOCUMENT			
Version	**Date**	**Description**	**Author**
3.5	02/07/2013	Periodicity of one year to the fulfilment of audits in accordance with ETSI 101-456 rule is included. Prohibition to issue CA certificates to other different entities to FNMT-RCM. Limitation to a maximum of 3 years the period of validity of the end-entity certificates. Reordering in the same section of issues about policies. Elimination of references to CA Mobile Signature for unsubscribing the service. Inclusion of Computer Components AC in the Root CA certification chain.	FNMT-RCM
3.6	02/04/2014	All references to annexes of 3.5 version are removed. Definitions of owner and signatory to the LFE are in line. Some web links of CERES have been updated.	FNMT-RCM
4.0	17/06/2014	All references to annexes of 3.5 version are removed. Definitions of owner and signatory to the LFE are in line. Some web links of CERES have been updated. Audit review according to WebTrust and ETSI. The maximum certificate validity has been extended to 5 years as modifying the LFE.	FNMT-RCM
4.1	16/02/2015	FNMT agrees to comply with CAB/Browser forum requirements	FNMT-RCM
4.2	14/07/2015	FNMT agrees to comply with ETSI 101 456 requirements	FNMT-RCM
4.3	12/04/2016	Inclusion of references to “AC Usuarios” and “AC Representación” and removal of “AC APE” and “AC ISA”.	FNMT-RCM

BACKGROUND OF THE DOCUMENT			
Version	**Date**	**Description**	**Author**
5.0	24/06/2016	Compliance requirements with ETSI 101 456 and updating definitions under Regulation (EU) No 910/2014.	FNMT-RCM
5.1	03/01/2017	Update to eIDAS Regulation (ETSI 319 401).	FNMT-RCM

Reference: DPC/DGPC0501/SGPSC/2017

Document classified as: *Public*

TABLE OF CONTENTS

1. INTRODUCTION

1. The Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (*Royal Spanish Mint*), (hereinafter FNMT-RCM), through the CERES (CERtificación ESpañola) (*Spanish Certification*) Department, in order to provide secure electronic transactions on the Internet, has since 1996 constructed the infrastructure required in order to provide electronic certification services with maximum guarantees. This infrastructure is currently fully operative and tested. The CERES Department was the first *Spanish Trust Service Provider* to obtain the ISO 9001 Quality Certification *Trust Service Provider*.

2. It is also important to emphasis the involvement in adaptation projects to the ISO 27000 series and to the European Electronic Signature Standardization Initiative[1] (hereinafter "EESSI") in collaboration with the Information Technology Evaluation Centre – National Aerospace Technique Institute.

3. The objective of the FNMT-RCM, through its CERES Department, is to provide its clients with the *Public Key Infrastructure,* as well as a full catalogue of services to support the services of administrations and companies, in order to provide them with legal security and validity in a simple and comfortable manner for the citizens. The FNMT-RCM shall seek these objectives mainly using encrypting techniques (to ensure the confidential nature of the information) and electronic signatures, which guarantee the identity of the signatory and the integrity of the information exchanged, with the adopted electronic identification framework being coherent with the 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, with the national legislation, as well as with the specific regulations of the FNMT-RCM itself which guarantee, complying with a series of limited requirements, the legal equivalence of the qualified *electronic signature* with the handwritten signature within the legally established scope, and without prejudice to the effects envisaged for the other types of electronic signatures.

4. The FNMT-RCM has been manufacturing high security and particularly sensitive products like banknotes and coins for over a century. But it also manufactures other security products like the DNI (Spanish National Identification Card), passports, stamps, paper for official contracts, registry books, intelligent cards, secure labels, etc. for both the national and the international markets.

5. In this way, the FNMT-RCM continues with its traditional role offering public security guarantees to Spanish society, and now also from the perspective of Internet and new technologies, adapting to the new times and providing the qualitative jump from the physical document to the *Electronic Document,* which is the case of the new Electronic National Identity Card (DNI-e) and the electronic passport.

[1] Initiative developed under the mandate given by the European Commission to the Information & Communications Technologies Standard Board, which started through the Information Society Standardisation System of the European Committee for Standardisation and the European Telecommunication Standards Institute.

1.1. OBJECT

6. This document aims to inform the public about the conditions and characteristics of the certification services from the FNMT-RCM as Trust Service Provider, specifically containing the obligations which are undertaken in relation to

   - The administration of the *Signature creation and verification data* and the *Certificates*, the conditions applicable to the application, issue, use, suspension and extinction of the effects of the *Certificates* and, if applicable, the existence of coordination procedures with the corresponding Public Administration which allow for the information to be exchanged immediately and confidentially on the validity of the powers indicated in the *Certificates* and which must compulsorily be entered in said registries.
   - The provision of the consultation service on the state of validity of the *Certificates*, whether they are issued by the FNMT-RCM itself or, if applicable, by third parties, indicating the special characteristics of each case, as well as the conditions applicable to the use of the service and guarantees offered.
   - The management of the *Time Stamping* requests, which are offered as part of the *Time Stamp* service provision.

7. This document also contains the details of the responsibility regime applicable to the user parties and/or relying parties in relation with the services mentioned in the preceding paragraph, the security controls applied to their procedures and installations in that which can be published without harming their effectiveness, and the secrecy and confidentiality s, as well as issues relating to the ownership of their goods and assets, to the personal data protection and other informative issues which it considers of interest to the public.

1.2. IDENTIFICATION OF THE FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA

8. The Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, hereinafter FNMT-RCM, with NIF (Tax identification number) Q2826004-J, is a public company under article 43.1.b) of the Public Administration and Functioning Act 6/1997, of 14th April, which, as a public body, has its own differentiated public legal status, assets and autonomous administration under the terms of said Act.

9. It is attached to the Spanish Ministry for Treasury and Public Administrations which, through Treasury Department and Public Administrations, performs the strategic management and control of the entity's effectiveness under the terms of articles 43 and 59 of the aforementioned Act 6/1997, of 14th April.

10. The FNMT-RCM has a long history in performing its industrial activities, as well as backing from the State. Since article 81 of the Fiscal, Administrative and Social Order Measures Act 66/1997, of 30th December, and its modifications, it has contributed to promoting the extension of the services to which it is authorized and has got the recognition of the private sector in this new sector that represents the electronic certification and the teleprocessing networks, becoming a significant player in the provision of trust services.

11. In the development of this activity, the FNMT-RCM has managed to endorse its quality management system in accordance with ISO 9001 standard granted by AENOR and IQNET for the provision of electronic signature certification and time-stamp services, and the development of cryptographic operative systems for intelligent cards.

12. It has also endorsed, through an independent entity and as part of a certification scheme, its Practices as *Qualified Trust Service Provider* in accordance with European standard ETSI EN 319 401 "General Policy Requirements for Trust Service Providers".

13. The FNMT-RCM will respond to any request, complaint or claim from its clients or relying parties, in accordance with the protocols approved by the Entity through the internal procedure of "Management of complaints, incidents and corrective and preventive actions". Contact information to forward complaints and claims to the following:

Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda
C/ Jorge Juan, 106
28009 Madrid
Correo electrónico: ceres@fnmt.es

1.3. DEFINITIONS AND ABBREVIATIONS

1.3.1. Definitions

14. To find out more information about the basic concepts relating to Cryptography, Trust Service Providers and the Public Key Infrastructures, go to this internet address http://www.ceres.fnmt.es

15. However, for the purposes of that set out in this Trust Services Practices and Electronic Certification Statement, and the Declarations of particular certifications dependent of that, when the terms start with a capital letter and are in italics, they shall be understood as:

- *AEPD:* "Spanish Data Protection Agency". Public Body, with its own legal status and full public and private capacity, which acts with full independence from the Public Authorities in the performance of its duties. Its main purpose is to ensure compliance with the personal data protection legislation and to control its application.
- *Certification Authority* (CA): Confidence system, managed by a *Certification Services Provider*, responsible for issuing and cancelling the digital certificates or certificates used in the electronic signature. Legally it is a specific case of Certification Services Provider and by extension the provider is called *Certification Authority*.
- *Time Stamping Authority (TSA)*: Confidence system, managed by a *Trust Services Provider*, responsible for issuing *Time Stamps*. Legally it is a specific case of Certification Services Provider and by extension the provider is called *Time Stamping Authority*.
- *Official State Gazette (BOE):* Official Book edited and distributed by the Official State Gazette; Public body, attached to the Ministry for the Presidency, also entrusted with editing and distributing the Official Gazette of the Trade Register (*Boletín Oficial del Registro Mercantil*), publishing repertoires, compilations of legal texts, and the

execution of the official printing work requested by Ministries, bodies and other public entities.

- *C:* Within the scope of this document it is an abbreviation of "Country". The "Country" is an attribute which forms part of the Distinctive Name (*DN*) of an object within the structure of the directory *X.500* used to name the entry corresponding to the object.
- *Certification chain*: An ordered list of *Certificates* which contains at least one *Certificate* and the *Root certificate* of the FNMT-RCM, with the *Signature verification data* contained in the latter being used to authenticate the *Certificate*.
- *Certificate*: An electronic certificate is a document signed electronically by a *Trust Service Provider* which links certain signature verification data with a *signatory* and confirms his/her identity. The specific conditions for each type of certificate issued by the FNMT-RCM are in the corresponding certification policies and specific practices.
- *Root Certificate*: Certificate owned by the FNMT-RCM and which, 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 confidence of all of the *Certificates* issued by the FNMT-RCM.
- *Qualified certificate*: The electronic *Certificate* issued by a *Trust Service Provider* which fulfils the requirements established in Annex I, Annex III or Annex IV (depending on what type of *Certificate* concerned) of the 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.
- *Asymmetric encrypting*: Transcription in symbols, in accordance with an encrypting *Key,* of a message whose content they want to conceal according to an algorithm so that knowing the encrypting *Key* is not enough in order to decipher the transcription, and what is needed is to know the corresponding deciphering *Key*. Knowing the encrypting *Key* does not imply knowing the deciphering *Key,* or vice versa.
- *Key*: Sequence of symbols which control the encrypting and deciphering operations.
- *Private Key*: Out of the pair of cryptographic *Keys* corresponding to an *Asymmetric encrypting*, the one to remain secret. The *Private Key* can constitute, according to their generation and use, *Signature creation data*.
- *Public key*: Out of the pair of cryptographic *Keys* corresponding to an *Asymmetric encrypting*, the one to be disclosed. The *Public keys* can constitute, according to their generation and use, *Signature creation data*.
- *Client OCSP*: Tool necessary so that the Private Law *User entities,* and, if applicable, Public Law *User entities, can make OCSP* requests. The FNMT-RCM will provide a list of free distribution products, but will not supply *Client OCSP* as they are widely available on the Market.
- *CN: "*The Common Name" is an attribute which forms part of the Distinctive Name (*DN*) of an object within the *X.500* directory structure used to name the entry corresponding to the object.
- *Electronic Community (hereinafter Electronic Community or user persons and/or entities):* Set of persons and *user entities* which are related with *Certificates* between

themselves, under the general framework of this Trust Services Practices and Electronic Certification Statement, and particularly the corresponding agreements and/or contracts that they have signed, directly or through representatives, with the FNMT-RCM.

- *Confidentiality*: Quality which means that the information is not accessible or has not been revealed to unauthorized persons, entities or processes.
- *Contract and agreement*: Legal instruments set out in the corresponding legislation and/or in agreement with freewill, in which the relationship is formalized for the provision of services by the FNMT-RCM. Included in the category are issue (forms), revocation, renewal contracts for corresponding certificates, as well as the acceptance of the conditions of use and limitations which are provided to the members of the *Electronic Community* through electronic, informative and teleprocessing systems.
- *DPC*: Data Processing Centre.
- C*reator of the electronic seal*: Legal person who creates an electronic seal.
- *Cryptography*: Discipline which covers the principles, meanings and methods for the transformation of data in order to conceal the content-information, preventing their undetected modification and/or preventing their unauthorized use.
- *Seal creation data*: Data, which is used by the C*reator of the electronic seal* to create an electronic seal;.
- *Signature creation data*: This is the unique data, like private cryptographic keys, which the signatory uses to create electronic signatures. For the purpose of this *Certification Practices Statement* it shall always, from a technical point of view, coincide with a *Private* asymmetric cryptography *Key*.
- *Signature or Seal verification data*: This is the data, like public cryptography keys which are used to verify electronic signatures or seals. For the purpose of this *Certification Practices Statement* it shall always, from a technical point of view, coincide with a *Public* asymmetric cryptography *Key*.
- *Trust Services Practices and Electronic Certification Statement*: Statement made available to the public via electronic channels and free of charge, which the FNMT-RCM makes as *Trust Service Provider* and in compliance with the 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.
- *Declaration of Time Stamp Practices*: Declaration made available to the public via electronic channels and free of charge, which the FNMT-RCM makes as *Time-stamp Services Provider*.
- *Directory*: Repository of information which follows the X.500 standard of the ITU-T.
- *Availability*: Quality of the data or of the information which means that it is available, i.e. the possibility of obtaining it or the possibility of using it.
- *Qualified electronic signature creation device (QESCD):* Element which is used to apply the *Signature creation data*, which complies with the requirements established in Appendix II of the 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.

- *Qualified Trust Service Provider*: *Trust service provider* who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
- *DN*: Contraction of "Distinctive Name" which is the univocal identification of an entry with the *X.500* directory structure. The DN is made up of the common name (*CN*) of the entry plus a series of attributes which identify the route followed within the *X.500* directory structure to reach said entry.
- *Electronic document*: Any type of information in electronic format, filed in an electronic support according to a specific format and capable of differentiated identification and treatment.
- *Electronic National Identity Card (DNI*-e): This is the national identity card which electronically proves the personal identity of its holder and allows for documents to be electronically signed.
- *LOPD Security Document*: Document whose objective is to establish the security measures to be implemented by the FNMT-RCM in the setting of *Services Provider* , in order to protect the personal data contained in the User Files of the Electronic, Computer and Teleprocessing Systems (EIT), regulated by Order EHA/2357/2008, of 30th June (BOE – Official State Gazette of 7th August).

  Related concepts:

  - *Administrator of the Application*: Personnel entrusted with implementing the policies defined by the *Party Responsible for the File* in the application which contains the EIT Systems User File. They shall have the access necessary in order to grant, alter or cancel the authorized access to the data or resources, after being authorized by the *Party Responsible for Security* . They are entrusted with communicating the security incidents which occur to the Party *Responsible for Security.*
  - *Security Auditor*: Personnel entrusted with revising and evaluating the controls proposed in this document or any other referenced. They prepare reports with the degree of compliance and the discrepancies which have been found.
  - *Cession or communication* (of data): any obtaining of data resulting from the consultation of a file, the publication of all or part of the information contained in a file, their interconnection with other files, and any communication of data made to a person other than the affected party.
  - *Consent* (from the interested party): all free, unequivocal, specific and informed statement through which the interested party consents to the handling of their personal data.
  - *Data Processor*: the individual or legal entity, public authority, service or any other body which processes personal data on behalf of the party responsible for the processing.
  - *Computer Security Personnel*: Personnel entrusted with coordinating and controlling the measures defined in this security manual as regards the Spanish Personal Data Protection Act - *LOPD*. They are also entrusted with

both maintaining and revising the incidents which occur and to prepare the reports on these incidents in order to send them to the *Party Responsible for the File,* via the *Party Responsible for Security*. Following instructions from the *Party Responsible for the File,* they shall provide the authorizations in order to carry out the requests for registrations, modifications or withdraws of accesses to the application containing the data of the EIT Systems Users File and if they do not apply with the request, to contrast it with the *Party Responsible for Security* and the *Party Responsible for the File.*

- *Backup operator*: Personnel responsible for making security copies and their subsequent labelling and safe storage, who depend on the Exploitation Department of the *Trust Service Provider* of the FNMT-RCM.
- *Party responsible for the File (or Processing)*: Person who decides on the purpose, content and use of the processing. They are entrusted with authorizing the necessary access and defining the policy which they deem appropriate for the data security. They are also entrusted with revising the periodic incidents reports. All without prejudice to the consideration of the FNMT-RCM as responsible for the file for the purposes of that set out in the current personal data protection regulations.
- *Party Responsible for Security*: Entrusted with coordinating and controlling the measures imposed by the *LOPD (Personal Data Protection Act) Security Document* as regards the EIT Users File according to the Spanish Personal Data Protection Act – LOPD. Said function corresponds to the Information Systems Director of the FNMT-RCM.
- *Users of the Application*: Personnel who require the data from the EIT Systems Users File in order to perform their functions. There are different types of access depending on the work performed. The users are employees of the *Trust Service Provider* of the FNMT-RCM and have access to the information depending on the level of authorization granted by the *Party Responsible for the File.*

- *EIT*: Electronic, computer and teleprocessing techniques and measures.
- *User entity*: That person, public or private entity which has signed a contract or agreement with the FNMT-RCM to act in the *Electronic Community*.
- *Digital dating:* See *Time Stamp*.

- *Electronic signature*: Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
- *Advanced electronic signature*: That *Electronic signature* which is uniquely linked to the signatory; is capable of identifying the signatory; is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
- *Qualified electronic signature*: It is an *Advanced electronic signature* that is created by a Q*ualified electronic signature creation device*, and which is based on a *Qualified certificate* for electronic signatures.

- *Signatory*: The individual who possesses a signature creation device and who acts (signs) on their own behalf or on behalf of the legal entity that represent.
- *Hash function*: A *Hash function* is an operation which is done on a set of data of any size so as to obtain as a result another set of data, sometimes called "summary" or "Hash" of the original data, of a fixed size and independent of the original size which also has the property of being unequivocally associated to the initial data, i.e. it is practically impossible to find two different messages which contain an identical *Hash* summary.
- *Hash*: Fixed size result which is obtained after applying a *Hash function* to a message, regardless of its size, which complies with the property of being unequivocally associated to the initial data.
- *Public Key Infrastructure (PKI)*: Infrastructure capable of supporting the management of Public *Keys* for the authentication, encrypting, integrity and non-rejection services.
- *Integrity*: Quality which implies that the set of data in the message does not lack any part, nor suffered any type of addition. From the point of view of the information that this data may involve, it means that neither the content nor the structure has altered.
- *Issue law:* Set of legal and technical characteristics of a certain type of electronic *Certificate*, in accordance with the applicable *Certification Policies and Practices* and in the corresponding contracts and/or agreements with the members of the *Electronic Community*, on the basis of freewill.
- *Revocation Lists (CRL; Certificate Revocation List)*: List exclusively containing the lists of revoked and suspended *Certificates.*
- *LOPD:* Spanish Constitutional Personal Data Protection Act 15/1999, of 13th December, which is aimed at guaranteeing and protecting, as regards the processing of personal data, individual's public freedoms and fundamental rights, and particularly their personal and family honor and privacy.
- *MD5:* Message Digest (message summary algorithm) in its version 5. Developed by R. Rivest in 1991 and its description published in the RFC 1321. The algorithm consists in taking arbitrary long messages and generating a summary 128 bits long. The probability of finding two different messages which produce the same summary is practically zero. For this reason it is used to provide *Integrity* to the documents during the electronic signature process.
- *Malware (Malicious software):* See *Malicious Software*.
- *The Information Security Management System Manual of the FNMT-RCM* as *Trust Service Provider*: Also referred to as *CERES Security Manual or Security Manual.* This manual covers the procedures of the Information Security Management System of the CERES Department of the FNMT-RCM under the regulation *ISO 27001: Information Security Management Systems (SGSI).*
- *Navigator (Web navigator, browser)*: Programme which allows for the visualization of the contents of Internet WebPages. It is also known as a *browser*. Some examples of *Web navigators or browser* are: Internet Explorer, Chrome and Mozilla Firefox.
- *Certificate serial number*: Whole number, unique in the ambit of each *Certification Authority* of the FNMT-RCM, which is unequivocally associated with a *Certificate* issued for it.

- *OCSP (Online Certificate Status Protocol):* Computer protocol that allows for the fast and secure check of the state of validity of an electronic *Certificate*.
- *Registry Offices*: Offices installed by the FNMT-RCM, or by another entity provided that there is an agreement with the FNMT-RCM signed by said entity or by its hierarchical administrative superiors, which are constituted in order to facilitate for the citizens and companies, both nationally and internationally, the presentation of requests relating to the *Certificates*, with the aim of confirming their identity and the delivery of the corresponding titles proving personal qualities, powers of representation and other requirements for the type of *Certificate* that is requested. When there are sufficient guarantees to confirm the identity and other personal data necessary to manage the certificates, the registry operations, they can be teleprocessed.
- *OID (Object Identifier)*: Value, of a hierarchical and comprehensive nature, of a sequence of variable components although always made up of whole non-negative numbers separated by a point, which may be assigned to registered objects and which have the property of being unique amongst the other *OID*.
- *OU*: Contraction of "Organizational Unit" which is an attribute which forms part of the Distinctive Name of an object within the structure of directory *X.500*.
- *O:* Within the scope of this document, it means "Organization" which is an attribute which forms part of the Distinctive Name of an object within the structure of directory *X.500* used to name the entry corresponding to the object.
- *Legal entity:* Group of people who constitute a unit with its own purpose which acquires as an entity legal status and capacity to act which is different to those of its members.
- *PIN*: Contraction of "Personal Identification Number" which is a set of alphanumeric data known only to the person who has to access a resource which is protected by this mechanism.
- *PKCS (Public-Key Cryptography Standards)*: Produced by RSA Laboratories and internationally accepted as standards.
- *PKCS#7* (Cryptographic Message Syntax Standard): Produced by RSA Laboratories and internationally accepted as a standard which defines a generic syntax for messages which include cryptographic improvements, such as digital and/or encrypted signature.
- *PKCS#10* (Certification Request Syntax Standard): Produced by RSA Laboratories and internationally accepted as a standard which defines the syntax of a certification request.
- *PKCS#11 (Cryptographic Token Interface Standard):* Produced by RSA Laboratories and internationally accepted as a standard which defines a programming interface independent from the base technology, to use cryptographic tokens (for example, cryptographic smart cards) as method of authentication.
- *Certification Policy (particular):* Document which establishes the set of rules which indicate the applicability of a certain type of *Certificate* to the *Electronic Community* and/or type of application of common security requirements.
- *Time Stamp Policy (particular)*: Document which establishes the set of rules which indicate the applicability of a certain type of *Time Stamp* to the *Electronic Community* and/or type of application of common security requirements.

- *Certification Practice (particular):* Document containing the specific procedures followed by the FNMT-RCM to manage the life cycle of a certain type of *Certificate* as well as other certification services which may be included within the scope of said practice.
- *Trust Service Provider (TSP)*: A natural or a legal person who provides one or more trust services either as a qualified or as a non-*Qualified trust service provider*.
- *Time Stamp Services Provider*: That individual or legal entity which, in accordance with the Time Stamp regulations, issues electronic *Time Stamps*.
- *ROA*: *Real Observatorio de la Armada* (*Royal Navy Observatory)*: Laboratory of the Royal Institute and Astronomical Observatory of the Spanish Navy dependent of the Ministry for Defence and associated to the Spanish Metrological Center, attached to the *International Bureaux for Weights and Measurements* and designated by Royal Decree 1308/1992 as depository of the National Time Standard.
- *RSA*: Acronym of Ronald Rivest, Adi Shamir and Leonard Adleman, inventors of the asymmetric key cryptographic system (1977). Public key cryptosystem which allows for digital encrypting and signing.
- *Time Stamping*: Consignment of the date and time on an electronic document using indelible cryptographic procedures, based on the *Request For Comments*: 3161 – *"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"* specifications, which manages to date the document in an objective manner. It also referred to as *Electronic dating or Digital dating.*
- *Electronic Time Stamp*: Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
- *Electronic seal*: Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
- *Advanced electronic seal*: An electronic seal, which is uniquely linked to the *Creator of the seal*; is capable of identifying the *Creator of the seal*; is created using *Electronic seal creation data* that the *Creator of the seal* can, with a high level of confidence, use under its control; and is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
- *Qualified electronic seal*: An A*dvanced electronic seal*, which is created by a Q*ualified electronic seal creation device*, and that is based on a *Qualified certificate* for electronic seal.
- *Information and consultation service on the state of validity of the certificates:* Service provided by the FNMT-RCM to those interested party, for which information is provided on the state of the *Certificates* that the user is interested in.
- *Digital Dating Service*: See *Time Stamping Service.*
- *Time Stamping Service:* Service provided on demand by the FNMT-RCM to those interested parties who request it, which basing itself on the 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, objectively dates the documents so that a time can undoubtedly be attributed to the existence of said electronic document. The FNMT-RCM shall only provide this service for certain *Certification Authorities* and the parties' limits of use,

obligations and responsibilities shall be described in the corresponding particular practices of the service.

- *Certificates Validation Service:* See *Information and consultation service on the state of validity of the certificates.*
- *Cryptographic system*: Collection of transformations of clear text into *encrypted text* and vice versa, in which the transformation or transformations to be used are selected by *Keys*. The transformations are normally defined by a mathematical algorithm.
- *Malware*: (Malicious software)*:* Any program, document, message or element therein which may cause damage and/or harm to the users.
- *Applicant*: Individual over 18 years old or emancipated minor, who following identification and, if applicable, with sufficient powers, requests an operation relating to a *Certificate* on their own behalf or on behalf of its *Owner*.
- *Tax payer*: This covers both *Legal entities* as well as those entities lacking legal status which however the tax regulations consider "tax payers". Individuals are therefore excluded from this concept.

- *Subscriber*: Contracting, authority, Public Administration authority or entity which subscribes the terms and conditions of the service offered by FNMT – RCM..
- *Cryptographic card*: Support which contains a microprocessor or chip and which constitutes a cryptographic device used to make the electronic signature with the *Signature Creation Data* housed in its interior. The Cryptographic Card may be a Qualified electronic signature creation device if it fulfils its definition.
  - *Coded text*: Set of signs, figures or conventional letters and which can only be understood knowing the *Key*, i.e. the sequence of symbols which control the encrypting and deciphering operations.
  - *UTC or Coordinated Universal Time*: This is the time of the reference time zone in relation to which all of the other zones in the world are calculated. It is the time scale which succeeds GMT and which, unlike GMT, is based on atomic references instead of astronomic references.
  - *Holder* (of a *Certificate*): This is the individual whose identity is linked to the *Signature verification data* (Public Key) of the *Certificate* issued by the *Trust Service Provider*. Therefore, the identity of the holder is linked to that electronically signed, as signatory, using the *Signature creation data* (Private key) associated to the *Certificate*.
  - *Triple-DES*: Symmetric encrypting system which arises as an evolution of the (Data Encryption Standard) described in the FIPS 46-3 (Federal Information Processing Standard) developed by the DEA (data encryption algorithm) also defined in standard ANSI X9.32.
  - *ITU (International Telecommunications Union)*: International Organization within the United Nations system in which the governments and the private sector coordinate the worldwide telecommunications services and networks.
  - *Time Stamping Unit (TSU):* Set of hardware and software independently managed and which only has one signature key active at each time to issue *Electronic Time Stamps*.
- *User* (of a service) or user party: The natural or legal person who relies on electronic identification and trust services.

- *X.500*: Standard developed by the ITU which defines the recommendations of the Directory. It corresponds to the standard ISO/IEC 9594-1. It gives rise to the following recommendations: X.501, *X.509*, X.511, X.518, X.519, X.520, X.521 and X.525.
- *X.509*: Standard developed by the ITU for the *Public Key Infrastructures* and those called "attributes certificates".

1.3.2. Abbreviations

16. For the purposes of that set out in this Trust Services Practices and Electronic Certification Statement, and the Declarations of particular certifications dependent of that, they shall be understood as:

CRL: Certificate Revocation List

DVC: *Domain Validation Certificate*

EV: Extended Valuation

LCP: Lightweight Certificate Policy

NCP: Normalized Certificate Policy

NCP+: Extended Normalized Certificate Policy

OCSP: Online Certificate Status Protocol

OID: Object IDentifier

OVC: Organizational Validation Certificate

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

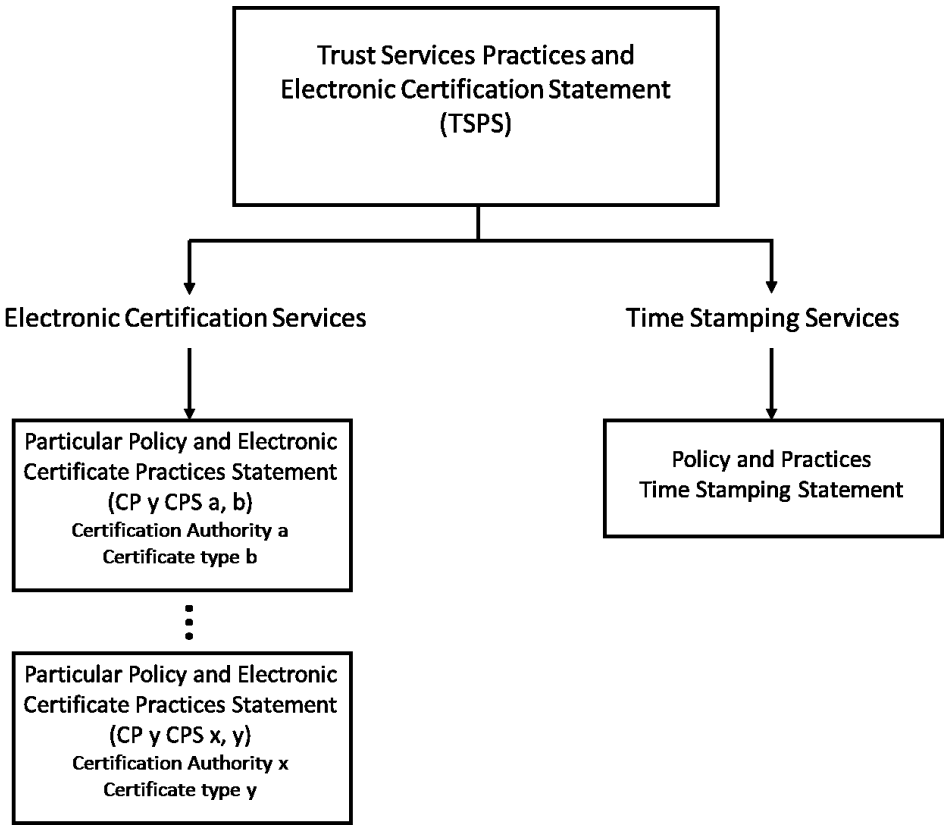
UTC: Coordinated Universal Time

1.4. IDENTIFICATION OF THIS TRUST SERVICES PRACTICES AND ELECTRONIC CERTIFICATION STATEMENT AND STANDARDS FOLLOWED IN ITS PREPARATION

17. This document is called the "Trust Services Practices and Electronic Certification Statementof the FNMT-RCM" and internally shall be called "*Trust Services Practices and Electronic Certification Statement*" or by its acronym "TSPS".

18. This document does not deal with the particular aspects of the different certification practices and policies, validation or time stamping that the FNMT-RCM implements for the provision of trust services. Said particular features are developed in the corresponding documents having this TSPS as general framework of application. The FNMT-RCM states that all the practices of its trust services are operated in any case under the principle of non-discrimination.

19. The conditions of use, limitations, responsibilities, properties and any other information which is considered specific for each type of certificate, shall be reflected in the particular certificate declarations of this GCDP. The document structure of the certification policies and practices of the certification services of the FNMT-RCM can be seen in the following chart:



20. This TSPS is referenced by the *OID* 1.3.6.1.4.1.5734.4 last version which can be found at the following address:

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

21. These procedures are principally based on the regulations of the *European Telecommunications Standards Institute* (ETSI).

1.5. AVAILABILITY OF THE INFORMATION AND CONTACT INFO

22. The FNMT-RCM shall interpret, register, maintain and publish the procedures referred to in the previous section "Identification of this *Trust Services Practices and Electronic Certification Statement* and standards followed in its preparation", also being able to receive communications from the interested parties on these issues, via the following email address: ceres@fnmt.es, and by the helpline: 902 181 696.

23. For organizational or administrative matters, the contact address of the FNMT-RCM as *Trust Service Provider* is as follows:

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

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

E-mail: ceres@fnmt.es

24. The FNMT-RCM, in its activity of *Trust Service Provider* when the current legislation thus allows, considers or requires, shall obtain the email address, mobile telephone number to receive text messages and the address of the *Holders* and/or *Subscribers* in the contracts that are signed by the *Applicants*, before issuing a *Certificate* or contracting a specific service.

25. This information is collected with the aim of provide trust services and notifying events of interest to the *Subscriber* related to such services of the FNMT-RCM and the *Certificates*, in particular those linked to the renewals or suspensions of the *Certificates*, like the cancellation of the contracts that the FNMT-RCM has signed with the *Subscribers*. It shall also be used as a communication channel to cover any requirement in the event of disaster contingencies which may prevent the FNMT-RCM.

26. It is the responsibility of the *Applicant* and afterwards the *Subscriber* to keep said information up to date and accurate.

1.6. GENERAL CONDITIONS OF THE CERTIFICATION SERVICES

27. The FNMT-RCM is constituted as root, independent *Trust Service Provider* which does not form part of external confidence structures. However it does have the technical infrastructure necessary to provide certification services based on external hierarchies.

28. The FNMT-RCM as *Trust Service Provider*, shall provide services to all interested parties which request them under the conditions set out in this TSPS and the Issue Policies, Practices and Laws applicable to the object of the request.

29. The properly used and combined certification services of the FNMT-RCM will allow *Users, Subscribers and Holders,* amongst others, to have the information exchanges of the security measures necessary for the identification, authentication, non-repudiation and confidentiality of the parties.

30. 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 CA/Browser Forum and which can be consulted in the following link: https://cabforum.org/baseline-requirements-documents/

31. The FNMT-RCM shall review its certification policies and practices in order to keep them in line with the referred requirements. In light of the publication of new versions of that document of requirements, the FNMT-RCM shall act diligently to address any deviation or, where appropriate, notify in this document any incurred noncompliance.

1.6.1. Trust Services Practices and Policies management

32. FNMT-RCM has *Practices* and *Policies* of the trust services provided and specific to each sort of *Certificate* or *Trust Service*. In particular, states that:

- FNMT-RCM holds specification, revision and approval of the *Certification Policies* and their trust services throughout its *General Direction* and other authorities directives.
- FNMT-RCM has *Particular Trust Services Practices* in which is determined the practices applicable to every service identifies in each *Trust Service Policy*.
- FNMT-RCM offers, within the competence of management and other executive organism, capable to specify, review and approve maintenance and reviewing procedures, for both *Particular Certification Practices, and Certification Policies*.
- FNMT-RCM, through its Management Trust Services Provider Committee, monitors the compliance of the Certification Policies and Practices Statements, approves and revises them with, at least, an annual periodicity.
- FNMT-RCM performs risk analysis to assess system threats and propose appropriate security measure (safeguards) to all involved areas.
- *Certification Practices and Policies* are set at public disposal in the URL address:

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

- *Certification Policies* collect general obligations and responsibilities of the involved parties in the various certification services for their use inside the limits and the related application framework, always in the competence field of each of those parties. The foregoing is understood without the prejudice of the specialties that may exist in the contracts, agreements or enforcement agreements
- To identify every *Certification Policy* specific OIDs are provided. A priori it is not expected any condition that implies changing the identification OIDs in this DGPC and *Particular Practices and Policies*.
- *Certifications Policies* of FNMT-RCM shall take into account the regulations and legislation applicable in each case.
- All information, systems, procedures, whether qualitative or quantitative, periods, amounts, forms and, in general, any issue stated in the declarative documents relating to *Certification Policies and/or Practices* can be modified or deleted by the FNMT-RCM, without requiring the agreement of the members of the *Electronic Community* or the *Users* of the services. FNMT-RCM assumes the undertaking to report the changes produced via the systems established in the applicable legislation and the entity's webpage.
- The members of the *Electronic Community* and the *Users* of the services are obliged to regularly check the corresponding declarative documents (applicable *Certification Policies and/or Practices)*, requesting as much information deemed appropriate from the FNMT-RCM

- However, in order to provide the *Recipient Users* (*User Entity* and *Subscriber*) with knowledge about the new features, when the modifications to any of the *Certification Practices Policies and Declarations* directly affect the rights and obligations of the parties in the *Electronic Community* or to restrict the scope of application of the *Certificates*, the FNMT-RCM shall notify the interested parties at least thirty (30) days before the entry into force of the changes, so that the members of the *Electronic Community* can adopt the decision which is deemed legally appropriate. FNMT-RCM shall not assume any compensation obligations for the modifications or withdrawals to the Declaration in the performance of its rights as *Trust Service Provider*.

1.6.2. About the information and consultation service on the state of validity of the certificates

33. The information on the state of the *Certificates* is provided according to format RFC 2560 – "Online Certificate Status Protocol – OCSP", amongst others.

34. The FNMT-RCM can provide *Information and consultation service on the state of validity of the certificates* on its own or external *Certificates* always in accordance with the particular policies and practices which are applicable and those agreements signed with the participating third parties.

1.6.3. About the Time Stamping service

35. The format of the *Electronic Time Stamps* issued by the *Time Stamping Service* shall be as indicated in the RFC 3161 – "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" and the European standard ETSI EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

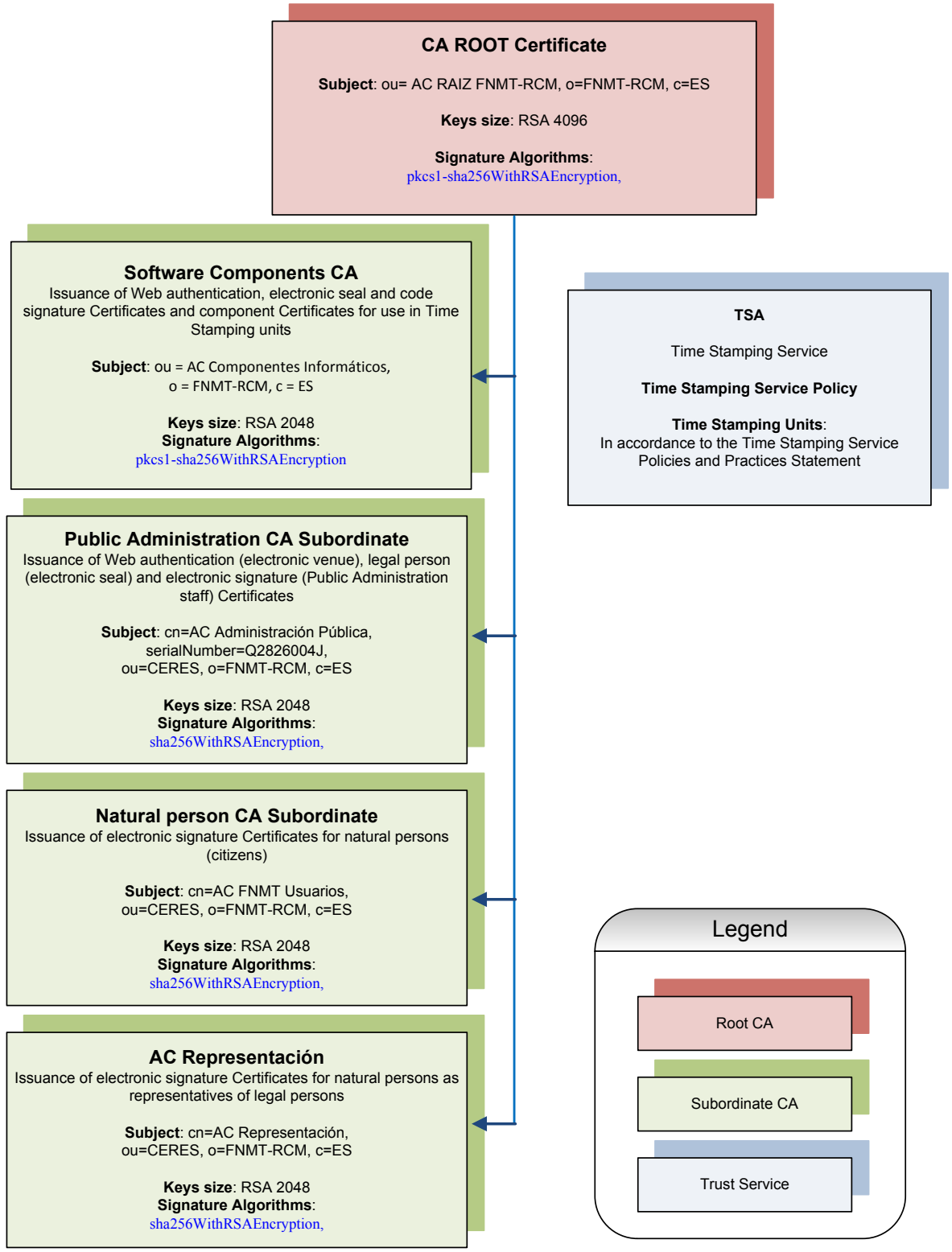
36. The *Certificates* used to provide the service can be internal or external and always in accordance with the particular policies and practices which are applicable and those agreements signed with the participating third parties.

1.6.4. Impartiality of operations

37. The legal nature of the FNMT-RCM, as a public body attached to the Central Government, is free from any commercial, financial and other pressure that might adversely affect trustworthy in the services provided. Its organizational structure ensures impartiality in making decisions regarding the establishment, provisioning and maintenance and suspension of the certification services, and in particular the certificates generation and revocation operations.

1.7. CERTIFICATION CHAINS

38. The *Certification Chains* used by the FNMT-RCM as *Trust Service Provider* in the performance of its functions, the signature algorithms and their parameters are as follows:


CA ROOT Certificate
Subject: ou= AC RAIZ FNMT-RCM, o=FNMT-RCM, c=ES
Keys size: RSA 4096
Signature Algorithms:
pkcs1-sha256WithRSAEncryption,
Software Components CA
Issuance of Web authentication, electronic seal and code signature Certificates and component Certificates for use in Time Stamping units
Subject: ou = AC Componentes Informáticos, o = FNMT-RCM, c = ES
Keys size: RSA 2048
Signature Algorithms:
pkcs1-sha256WithRSAEncryption
TSA
Time Stamping Service
Time Stamping Service Policy
Time Stamping Units:
In accordance to the Time Stamping Service Policies and Practices Statement
Public Administration CA Subordinate
Issuance of Web authentication (electronic venue), legal person (electronic seal) and electronic signature (Public Administration staff) Certificates
Subject: cn=AC Administración Pública, serialNumber=Q2826004J, ou=CERES, o=FNMT-RCM, c=ES
Keys size: RSA 2048
Signature Algorithms:
sha256WithRSAEncryption,
Natural person CA Subordinate
Issuance of electronic signature Certificates for natural persons (citizens)
Subject: cn=AC FNMT Usuarios, ou=CERES, o=FNMT-RCM, c=ES
Keys size: RSA 2048
Signature Algorithms:
sha256WithRSAEncryption,
AC Representación
Issuance of electronic signature Certificates for natural persons as representatives of legal persons
Subject: cn=AC Representación, ou=CERES, o=FNMT-RCM, c=ES
Keys size: RSA 2048
Signature Algorithms:
sha256WithRSAEncryption,
Legend
Root CA
Subordinate CA
Trust Service

39. FNMT-RCM shall not use their *Signature Creation Data* to issue *Certificates of Authority* to holders different from them or to anyone else who may ask.

40. In order to check the authenticity of any "Self-signed Certificate", ultimate element in any *Certification Chain*, the corresponding digital fingerprint (in its different formats) can be checked.

1.7.1. FNMT-RCM root CA

41. For reasons of interoperability and future forecasts, the *Signature Creation Data* of this *Certification Authority* has been self-signed with different algorithms giving rise to three *Root Certificates* corresponding to "FNMT-RCM ROOT CA". As such, the following information is published:

1.7.1.1. Signature Algorithm:

- pkcs1-sha1WithRSAEncryption[1],
- pkcs1-sha256WithRSAEncryption,
- pkcs1-sha512WithRSAEncryption

[1] It is published for interoperability reasons to facilitate the systems which do not support pkcs1-sha256WithRSAEncryption/ pkcs1-sha512WithRSAEncryption, the foundation of confidence chain in the certificates and signature validation processes.

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

2. PUBLICATION AND REPOSITORIES

2.1. REPOSITORIES LIST AND ACCESS CONTROLS

42. FNMT-RCM, as *Trust Service Provider*, maintains the following information repositories:

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

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

b. *Electronic certificates of Certification authorities* (reachable from) https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt)

i. CA ROOT Certificate ("AC Raíz")

ii. Public Administration CA Subordinate Certificate ("AC Administración Pública")

iii. Software Components CA Subordinate Certificate ("AC Componentes Informáticos")

iv. Representative CA Subordinate ("AC Representación")

v. Natural person CA Subordinate ("AC FNMT Usuarios")

c. Certificate Revocation Lists:

i. CA ROOT. Access:

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

2. http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

ii. Public Administration CA Subordinate Certificate. Access:

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

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

iii. Computer Components CA Subordinate Certificate. Access:

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

2. http://www.cert.fnmt.es/crlscomp/CRL<xxx*>.crl

iv. Representative CA Subordinate

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

v. Natural person CA Subordinate

1. 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: integer number that identifies the CRL (partitioned CRL)

d. Checking certificates status of revocation Service (OCSP):

i. ROOT CA. Access:

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

ii. Public Administration CA Subordinate Certificate. Access:

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

iii. Computer Components CA Subordinate Certificate. Access:

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

iv. Representative CA Subordinate

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

v. Natural person CA Subordinate

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

43. All repositories previously referenced have universal Access, without any Access control for downloading information.

2.2. PUBLICATION FREQUENCY

44. *Certificate Revocation Lists* (*CRL)* of the authority´s certificates are issued every six months, or when a subordinate authority certification is revoked and has a validity period of 6 months. *CRL* of final entity certificates are issued, at least, every 12 hours, or when a revocation occurs and has a validity period every 24 hours.

45. Whatever modification in the *TSPS* or in the *Particular Certificate Policies and Practices* is made, it shall be published immediately in their Access URL.

3. IDENTIFICATION AND AUTHENTICATION

46. Without prejudice to the fact that the corresponding particular Issue policies, practices and/or laws of the services may be established, those operations which require the accreditation of the interested parties shall be performed through a *Registry Office.*

47. The issue of *Certificates* involves the generation of *Electronic Documents* which prove the identity, and if applicable, other qualities or powers of the *Holder.*

48. Without prejudice to that established in the corresponding particular *Certification Policies and Practices* for the different types of *Certificates,* the FNMT-RCM shall perform the proper controls in order to check the accuracy of the information included in the *Certificate*.

49. For these purposes, when accrediting the identity of the *Applicant or Holder* of the *Certificate,* the physical attendance at the *Registry Office* with the corresponding official document proving the identity of the person according to the current legislation shall prevail. The FNMT-RCM shall take into account the functions set out in the applicable legislation in relation to the DNI-e (Electronic National Identity Card), as well as other identification and checking systems of the qualities of the *Holder* which provide sufficient guarantees of the accuracy of the data.

50. In the cases in which the *Certificate* includes data like domain names or IP addresses, the FNMT–RCM shall check, via the information systems that the authorized registrars for each case make available to the public, that the documentation required and validated by the *Registry Office* is correct.

51. For such purpose the publications in the different official state and autonomous region gazettes shall be taken into account, as well as the public registers and the registers accessible by the FNMT-RCM of the different registry bodies of domain names and assignation of IP addresses.

52. All *Certificates*, as such, and with the aim of avoiding their alteration or falsification, must be signed with the *Signature Creation Data* of the FNMT-RCM as *Trust Service Provider*.

53. The format of the *Certificates* used by the FNMT-RCM is based on that defined by the International Telecommunications Union, telecommunications normalization sector, in the ITU Recommendation -T X.509, from June 1997 or later (ISO/IEC 9594-8). The format shall be that specified in Version 3 of said format *X.509* and shall be valid for use with standard communication protocols type SSL, TLS, etc.

54. The format of the *Revocation Lists* published by the FNMT-RCM follows the profile proposed in the ITU recommendation -T X.509, in its Version 2 as regards *Revocation Lists*.

55. Furthermore in the practices and procedures followed in the issue of the different types of *Certificates* by the FNMT-RCM must consult the particular *Certification Policies and Practices* and if appropriate the applicable *Issue Laws*.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

56. If applicable, the management of the lifecycle of the *Keys* of the *Holder* of the *Certificate* shall be performed as defined in the particular *Certification Policies and Certification Practices* of each of the *Certification Authorities* of the FNMT-RCM.

57. Without prejudice to that established in said particular documents, in general the FNMT-RCM shall not store the *Private keys* of the *Holders* whom use its certification services infrastructure.

58. The *Private keys* of the *Holders* are used, with a high level of confidence, under the sole control of the *Holder*.

59. The FNMT-RCM shall only conserve the *Public key* of the *Holder* and the proof of possession of the *Private Key (Public key* or encrypted message with Private Key) according to the current legal regulations, for a period of no less than 15 years.

60. The use of the *Keys* of the *Holders* is detailed in each of the Particular *Certification Practices* covered by the FNMT-RCM as *Trust Service Provider*.

61. *Data Signature Creation* and *Data Verification Signature* of the Electronic Community may be used throughout the lifetime of the certificate that may be up to five years. See each one of the different *Particular Certification Practices* covered by FNMT-RCM as *Trust Service Provider*.

4.1. PUBLIC KEYS FILE

62. FNMT-RCM keeps all public keys during the time required by the current legislation, and in any case during the certification services are active with the certificates.

4.2. CERTIFICATES REVOCATION

63. The certificates revocation issued by FNMT-RCM shall be deployed according to Certification Policies and Certification Practices that applies to every *Certificate*.

64. As regards the period in which the Certification authority solves the revocation request, FNMT-RCM proceeds to the immediate revocation of the certificate at the time of verifying the signatory identity or, when appropriate, the veracity of the request made by a judicial or administrative decision.

The Revocation Lists (CRL) publication is made when these lists are generated, so the period of latency between the CRL and its publication is null.

65. Third parties that trust and accept the use of certificates released by FNMT-RCM are required to verify:

- *The Advanced Electronic Signature* or the *Advanced electronic seal* by the *Trust Service Provider* who emits the *Certificate*.
- The *Certificate*is current and active.
- The certificate´s status included in the *Certification Chain*.

66. The Certificates Revocation Lists (*CRL*) of the final entity are released at least every 12 hours, or when a revocation occurs and has a validation period of 24 hours. Authority´s CRL are issued every 6 months, or when a subordinate Certification authority occurs and has a validation period of 6 months.

67. The related information about the certificate´s status is available on-line 24 hours per day, 7 days a week. In case of system failure the Business Continuity Plan shall be launched in order to solve the incident as soon as possible.

5. FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS

68. The FNMT-RCM has physical, personnel and operation control procedures aimed at guaranteeing the necessary security in the management of the systems under its control and involved in the provision of certification services. Furthermore, the FNMT-RCM will register those events relating to its services which may be relevant in order to verify that all of the internal procedures necessary in order to develop the activity are performed in accordance with the applicable regulations so as to determine the causes of any anomaly detected.

69. Afterwards and taking as working model the document *RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* the European standards ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", all of the controls are shown implemented by the FNMT-RCM as *Trust Service Provider*, without prejudice to the confidential and secret nature of those which are not report for security reasons.

5.1. PHYSICAL SECURITY CONTROLS

70. The FNMT-RCM guarantees that it complies with the applicable regulations in all aspects of physical security and describes them in this chapter.

71. Different security parameters have been established, where the critical or sensitive activities are performed, with security barriers and with appropriate entry controls provided with security control mechanisms to reduce the risk of unauthorized accesses or damage to the computer resources.

5.1.1. Location of the installations

72. The building where the infrastructure of the *Trust Service Provider* is located has access control security measures to the building so that the development of the activity and provision of the services is performed with sufficient *Confidentiality* and security guarantees.

5.1.2. Situation of the Data Process Centre

73. The DPC of the *Trust Service Provider* has been constructed according to the following physical requirements :

- In a floor away from smoke outlets in order to avoid possible damage that this could cause in the event of a fire in the upper floors.
- Absence of windows which can be opened to the outside of the building.
- Intrusion detectors and security cameras in the restricted access areas during the periods when the systems are left unattended.
- Access control based on cards and passwords.
- Fire protection and prevention systems: smoke detectors, fire extinguishers, training the operators in how to extinguish fires, etc.
- Existence of transparent partitions, limiting the different areas, which allow for the rooms to be seen from the access corridors in order to detect intrusions or unlawful activities inside the DPC.
- All wiring shall be protected against damage or electromagnetic interception or interception of the transfer of both data and telephones.
- The installations for the provision of certification services are in the high security setting of the Entities other activities.

5.1.3. Physical Access

5.1.3.1. Physical security perimeter

74. After the security areas for the performance of the activity of FNMT-RCM as *Trust Service Provider* was established, the appropriate physical access control measures have been established, without forgetting that the site of the FNMT-RCM has an advanced physical security perimeter system made up of different rings with the appropriate technical and human resources, with the protection and security of the State security forces, as well as specialized security.

75. Apart from the different access controls there are various internal control measures to the rooms and installations like the access controls based on card readers, video security cameras, intrusion detectors, smoke detectors, etc., as well as the human resources devoted to attending to both the outside and the inside of the site.

5.1.3.2. Physical entry controls

76. There is a comprehensive physical control system of people at the entry and exit which consist of various security rings.

77. All of the critical operations of the *Trust Service Provider* are performed within the physically secure site with different security levels to access the critical machines and applications.

78. These systems shall be physically separate from the other systems of the FNMT-RCM, so that only the Department's authorized personnel can access them, and guaranteeing the independence from the other general purpose networks.

5.1.3.3. The work in secure areas

79. The work in secure areas is protected by access control, and, when the area thus requires, monitored by the Security Department of the FNMT-RCM. Unless expressly authorized by the management, the presence of photographic, video, audio or other registry systems is not permitted.

5.1.3.4. Visitors

80. The access of persons outside the FNMT-RCM to its facilities shall be previously reported to the Security Department and authorized by the Director of the Ceres Department. These people shall carry permanently a visible identification and shall be accompanied all the time by personnel of the FNMT-RCM.

5.1.3.5. Isolated loading and unloading areas

81. The loading and unloading areas are isolated and permanently monitored by technical and human resources.

5.1.4. Electricity and Air Conditioning

82. The rooms housing the machines of the infrastructure of the *Trust Service Provider*, have sufficient electricity and air conditioning supply in order to create a reliable work setting. This productive infrastructure is protected against power cuts or any anomaly to the electricity supply via an independent source from the main supply center, as well as an autonomous electricity generator.

83. Mechanisms have also been installed to control the temperature and humidity at proper levels in order to achieve that the system of the *Trust Service Provider* operates correctly.

84. Those systems that thus require shall have uninterrupted power units and double supplier electricity supply and generator.

5.1.5. Wiring security

85. The wiring is in a false floor or false ceiling and has the appropriate measures (detectors in floor and ceiling) in order to protect them against fires, as well as humidity detectors for the early detection of leaks of liquids.

5.1.6. Exposure to water

86. The proper measures have been taken in order to prevent the equipment and wiring being exposed to water.

5.1.7. Fire Prevention and Protection

87. The rooms have the proper resources (detectors) to protect their contents against fires.

5.1.8. Storage of Supports

88. The FNMT-RCM, as *Trust Service Provider*, establishes the procedures necessary to have back-up copies of all of the information of its productive infrastructure.

5.1.9. Recovery of the information

89. In the FNMT-RCM there are security copy plans for all sensitive information and that considered necessary for the continuity of the Department's business. There are different procedures for the preparation and recovery according to the sensitivity of the information and the means installed.

5.1.10. Waste elimination

90. There is a waste management policy which guarantees the destruction of any material which may contain information, as well as a management policy for the removable supports.

5.1.11. Security copies outside of the installations

91. Security copies applicable to the FNMT-RCM as *Trust Service Provider* shall not be made outside of its installations.

5.2. CONTROLS OF PROCEDURE

92. The FNMT-RCM endeavors that all management of both operative procedures and administrative procedures is performed in a reliable manner and according to that established in this document, carrying out audits to avoid any defect which may lead to a loss of confidence (on this issue you can consult the "Audits" section).

- Audits shall be carried out in order to check compliance with the security requirements and the technical and administrative requirements.
- Segregation is performed of functions to avoid a single person being able to achieve total control of the infrastructure. In order to achieve that, multiple profiles are designed assigned to the infrastructure personnel, including the distribution of the different tasks and responsibilities.

93. The FNMT-RCM outsources certain activities, such as the call center service for users of the *Certificates*. These activities are carried out according with the FNMT-RCM Certification Policies and Practices and the contracts/agreements signed with entities that perform such activities. In these cases, access to FNMT-RCM information by third parties follow the protocol defined in the Security Policy of this company, in terms of identifying risks, establishing security controls to protect access to information and formalization of

the corresponding confidentiality agreements. If applicable, will be signed a contract for the treatment of personal data in compliance with current regulations.

94. The FNMT-RCM shall establish supervision and control programs in order to guarantee that the entities which performed delegated functions relating to the provision of certification services are performed complying with the policies and procedures of the FNMT-RCM.

95. The FNMT-RCM has an updated record of all information assets and systems used for processing inventory, detailing its owner or responsible, nature, classification and any other relevant information for incident prevention and response. There is categorizing systems processing information for the establishment of security controls in accordance with the Security National Scheme.

96. The FNMT-RCM, through its Code of Conduct Monitoring Committee, ensures compliance with the rules laid down in the Code of Conduct to avoid situations that might lead to a conflict of interest.

5.2.1. Trusted roles

97. People who play the trusted roles are properly trained and have the knowledge base and experience required for the execution of the associated work for each role. When this has been needed, FNMT has provided adequate technical and security training plans for the staff implicated in their dependable systems management.

98. The identification of different "Trusted roles", assignments and security profiles are reflected in the internal document of Information Systems FNMT - RCM Directorate defined as "Trusted roles and safety profiles." These Trusted Roles are: Security Officer, System Administrator, System Operator and System Auditor. The selection of the people who play these roles is performed requiring the principle of "least privilege" and taking into account their training, experience and personnel security controls described below. The persons who will exercise these roles will be designated by the TSP Management Committee.

5.3. PERSONNEL SECURITY CONTROLS

5.3.1. Security in the definition of the work and the resources

99. The definition of the work posts and their responsibilities, including those relating to security, are in the Collective Agreement which regulates the working relations between the FNMT-RCM and its employees as well as the regulations relating the applicable public function.

5.3.2. Inclusion of security in the working responsibilities

100. Security is included within the labor responsibilities without requiring further mention as FNMT-RCM is an entity whose main objective is security and therefore the objective and responsibility of all of its members.

101. In any event, and without prejudice to the corresponding public regulations, rules of the Criminal Code which are directly applicable and clauses from certain contracts with the management, it is specifically included in Chapter XVII "Disciplinary regime", article 63, Misdemeanors and Sanctions of said Collective Agreement :

> *"Serious misdemeanors are:*
>
> *...*
>
> *13. The improper use or disclosure of data or issues that are known as a result of the work in the Body.*
>
> *...*
>
> *Very serious misdemeanors are:*
>
> *...*
>
> *9. The use of internal information of the FNMT-RCM in one's own benefit or in the benefit of companies which compete with the FNMT-RCM.*
>
> *..."*

102. The sanction may be dismissal, without prejudice to the infringement of the general legislative framework and its corresponding sanction which may be brought before the courts.

103. Additionally and when thus required, there may be personal confidentiality agreements requested by the FNMT-RCM and/or third parties.

5.3.3. Personnel selection and policy

104. The personnel selection and policy is included in the Collective Agreement which regulates the working relations between the FNMT-RCM and its staff, as well as in the various regulations applicable by virtue of the civil service regulations and its Statute (Royal Decree 1114/1999, of 25th June), which adapts the *Fábrica Nacional de Moneda y Timbre* to the State General Administration Organization and Function Act 6/1997, of 14th April, its Statute is approved and its name *Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda* and its condition of Public Company dependant on the Ministry for Finance and Treasury (nowadays Treasury Minister and Public Function).

5.3.4. Outsourcing requirements

105. Outsourcing contracts made by FNMT - RCM are subject to Royal Legislative Decree 3/2011, of 14 November, approving the revised text of the Law on Public Sector Contracts (PSCA) is approved. In this context, the Entity is "contracting authority" and therefore is subject to those regulations, i.e. a "harmonized regulation" of their contracts. For cases in which the GCA does not apply, the FNMT-RCM uses its internal contracting instructions (IIC).

5.3.5. Proven Knowledge, qualification, experience and requirements

106. The procedures for managing the personnel of the infrastructure shall promote the competence and knowhow of its employees, as well as the compliance with their obligations.

107. To be considered positions of confidence within the scope of this document are those which involve access to or control of components which may directly affect the management of the systems which implement the services related to the *Certificates*, the information on the state of the *Certificates* and the issue of *Electronic Time Stamps*.

5.3.6. Frequency and sequence for job rotation

108. Not stipulated.

5.3.7. Documentation provided to staff

109. All employees who have access or control over reliable systems, in those services which are basic on third parties, are given access to the department knowledge base, including documentation on safety regulations, practices and policies of Certification, tasks entrusted to the staff, quality plan and security policy and business continuity plans and, in particular, provides the documentation necessary to develop the tasks assigned in each case.

5.3.8. Confidentiality Agreements

110. All own or contracted employees who have access to or control over the reliable systems on which the third party confidence services are based, including the restricted access to the *Directory*, are considered employees of trust. This personnel includes, but is not limited to, the customer service personnel, the system administration personnel, the engineering personnel, and executives who were appointed to verify the infrastructure of the security systems of the *Certification*.

111. The personnel permanently or temporarily devoted to these positions shall be duly endorsed and identified by the FNMT-RCM. Periodically an assurance shall be made that these persons continue having the confidence of the FNMT-RCM in order to carry out this confidential work.

112. The relations between third parties and the FNMT-RCM are protected by the corresponding confidentiality agreement if sensitive information has to be exchanged under said relationship.

113. The personnel of the FNMT-RCM, by virtue of their Collective Agreement, do not require personal confidentiality agreements, without prejudice to the fact that under exceptional circumstances there may be personal confidentiality agreements, normally at the request of third parties or at the criteria of FNMT-RCM.

5.3.9. Terms and conditions of the labor relationship

114. The terms and conditions of the labor relationship are also contained in the corresponding contract, in the Labor Agreement which regulates the working relationship between the FNMT-RCM and its staff, and also as already mentioned in the various regulations applicable by virtue of the civil service regulations and its Statute.

5.3.10. Communication of security incidents

115. The incidents are reported to the Management regardless of the fact that the corresponding corrective actions are activated via the Incident Management System established in the Department to find the quickest solution possible according to that described in the *Incident Communication Procedure* and the *Incident Management Procedure.*

5.3.11. Communication of the security weaknesses

116. The security weaknesses are classified as incidents, and as such are resolved, giving rise to the corresponding corrective actions, as described in the procedures mentioned above.

5.3.12. Communication of the software faults

117. The software faults are classified as incidents, and as such are resolved, giving rise to the corresponding corrective actions, as described in the *Incident Communication Procedure* and the *Incident Management Procedure.*

5.3.13. Learning from the incidents

118. The *Incident Communication Procedure* and the *Incident Management Procedure* also contain their grouping and classification in order to give rise to the corresponding corrective actions.

5.3.14. Disciplinary Procedure

119. In the development of their labor activity for the FNMT-RCM, or provided that they use materials and/or resources of the FNMT-RCM, its employees, in accordance with their employment contracts and/or the applicable legislation, exclusively cede, as broadly as possible and for the maximum duration set out in the law and worldwide, to FNMT-RCM all of the exploitation rights which may correspond to them and in particular, and with this list being considered as a limitation, the rights to reproduce, distribute, transform and publicly communicate relating to intellectual property rights, as well as any industrial property rights, or relating to semiconductor topography, over the work, inventions and creations that they start and/or develop. The worker, as a result of the exclusive cession of the aforementioned rights over the work, inventions and creations prepared or created as a result of the labor relationship that links them with the FNMT-RCM or as a result of the use of the material and/or technical resources of the FNMT-RCM, shall not enjoy the right to exploit said work and/or creations in any way, even if this does not prejudice their exploitation or use by the FNMT-RCM.

120. In order to achieve compliance with the internal regulations of the FNMT-RCM, the applicable laws and regulations and the security of its employees, the FNMT-RCM reserves the right to inspect at any time and monitor all of the computer systems of the FNMT-RCM.

121. The computer systems subject to inspection include, but are not limited to, the files of the email system, files on the hard drive of personal computers, voicemail files, printing queues, documentation obtained by fax, desk draws and storage areas. These inspections shall be carried out after being approved by the Security and Legal Department, with the procedures established in the applicable regulations and with the participation of the union representatives, and if applicable the FNMT-RCM also reserves the right to eliminate from the computer system any material that it considers offensive or potentially illegal or fraudulent.

5.3.15. Improper behavior

122. The management of the FNMT-RCM reserves the right to revoke the system privileges of any user at any time. No conduct shall be permitted which interfere with the normal and proper rhythm of the computer systems of the FNMT-RCM, which prevents others from using these systems or is dangerous or offensive.

123. The FNMT-RCM shall not be responsible for the opinions, acts, transactions and/or business that the users perform using the certification services of the FNMT-RCM; all without prejudice to the obligation on the FNMT-RCM to report to the competent authority if it becomes aware.

5.3.16. Applications which compromise the security

124. Unless the corresponding authorization is granted by the Information Systems Department of the FNMT-RCM, the employees of the FNMT-RCM must not acquire, possess, negotiate or use hardware or software tools which may be used to evaluate or compromise the computer security. Some examples of these tools are: those that ignore the software protection against unauthorized copies, detect secret passwords, identify vulnerable security points and decipher files. Furthermore, without proper authorization, the employees are prohibited from using trackers or other type of hardware or software which detect the traffic of a network system or the activity of a computer, except in those cases where their use is necessary in order to perform the system tests and following communication to the area manager.

5.3.17. Activities not permitted

125. The users must not check or try to compromise the security measures of a communication machine or system unless said action has been approved in advance in writing by the Information Systems Department of the FNMT-RCM. The incidents relating to “computer piracy”, discovery of passwords, file deciphering, unauthorized copies of software, personal data protection and other activities which threaten the security measures, or which are illegal, shall be considered very serious infringements of the internal regulations of the FNMT-RCM. It is also strictly prohibited to use bypass systems which are aimed to

avoid the protection measures, and other archives which may compromise the protection systems or resources.

5.3.18. Compulsory reporting

126. All cases of infringements of the regulations, intrusions into the system, malware and other conditions which involve a risk to the information or the computer systems of the FNMT-RCM must be immediately reported to the Information Systems Department.

5.3.19. Training

127. The FNMT-RCM through its training center, dependent of the human resource management, is responsible for managing the annual training plan, based on the general needs of the company and its department. On this point, all employees, own or hired, that have access or control about reliable systems in which are based trusted third party services, they are aim of the aforementioned training plan that, with annual character, it comes to cover the training needs and the raising awareness in security information, according to the internal document "standard training and awareness in information security" .Technical security controls.

5.3.20. Users management

128. The FNMT-RCM has internal procedures that establish the necessary controls to identify the activities that users perform in critical information systems in regards the provision of certification services. For this purpose there is an auditable record for each access or failed access attempt to the system's assets. All activities related to safety functions are registered, assuring traceability.

129. There is a policy on the management of access privileges to information and information systems, as well as user password management. The privileges granted in the system to each user are periodically reviewed by the person in charge of each system or information asset. Therefore, the FNMT-RCM manages the access of system operators, administrators and auditors with controls of logic security to ensure the separation of trusted roles identified in the practices of their trust services, so that the related privileges with access to critical applications of the Trust Services Provider's infrastructure, have a special treatment, previously identifying and authenticating the personnel with such access and providing electronic certificates on cryptographic cards.

5.4. REGISTRY OF EVENTS

5.4.1. Types of events registered

130. The FNMT-RCM shall register all those significant events in order to verify that all of the internal procedures necessary in order to develop the activity are performed in accordance with this document, the applicable legal regulations and that established in the Internal Security Plan and in the Quality and Security Procedure, and all for the causes to be detected of any anomaly detected. Such records shall be made available if required for the

purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

131. The registered events shall be all of those operations which are performed in the management of keys, management of *Certificates*, issue of *Electronic Time Stamps*, information about the state of *Certificates*, publication, file, recovery, directory, registration of events and registry of users. The FNMT-RCM shall file all of the most important registered events, keeping them accessible for at least 15 years.

132. All of the registered events can be audited.

133. As well as the events set out above, all of the registries shall be kept that are specified in regulation ISO 9001 in the manner set out in the general quality procedures of the FNMT-RCM, for at least 3 years. These registries are fundamentally:

- The Management's monitoring registries.
- Registries of design, development and their revisions.
- Registry of Corrective Actions.
- Registry of customer satisfaction.
- Registry of the system revisions.
- Other registries.

5.4.2. Protection of an activity registry

134. After the activity of the systems has been registered, the registries cannot be modified, or deleted, and shall remain filed in the original conditions.

135. This registry can only be accessed for reading, and is restricted to those persons authorized by the FNMT-RCM.

136. The recording of the registry, so that no data can be manipulated by anybody, shall be done automatically by the specific software deemed appropriate for such purpose by the FNMT-RCM.

137. The audited registry, as well as the security measures established in its recording and subsequent verification shall be protected against any contingency, modification, loss and disclosure of its data, during the recording in external supports, change of this support and their storage.

5.4.3. Security copy procedure for the audited registries

138. The FNMT-RCM, as *Trust Service Provider*, as it is a high security system, guarantees the existence of a security copy of all of the audited registries.

5.4.4. Registries archive system

139. The archive systems used by the FNMT-RCM to keep these audited registries, shall be those within the infrastructure, and external supports shall also be used with long term

storage capacity. These supports shall have sufficient guarantees in order to prevent the registries from suffering any type of alteration.

140. The FNMT-RCM shall make various copies which shall be stored in different locations, which shall have all of the physical and logistical security measures in order to avoid, insofar as reasonable possible, an alteration of the stored support and of the data contained therein. Each copy shall be stored in a different plan in order to avoid possible disasters in any of them.

141. This archive is provided with a high level of integrity, confidentiality and availability in order to avoid manipulation of the stored certificates and events.

142. All stored events contain a time stamp obtained from the time reference UTC (ROA). The Royal Observatory of the Navy (ROA), holds the pattern of official time in Spain. The FNMT-RCM and ROA have formalized an agreement for the time synchronization of their systems. System conditions are defined in the document "Sync System FNMT - ROA".

5.4.5. Relevant data which shall be registered

143. The following shall be registered:

- The issue and revocation, and other relevant events related to the Certificates, as well as the operations relating to the management of keys and Certificates of the *Trust Service Provider*.
- The signatures and other relevant events related to the Revocation Lists (CRL's).
- All access operations to the Certificates archive.
- All access operations to the Information Services on the State of the Certificates.
- Relevant events of the generation of random and pseudo-random pairs of numbers for the generation of Keys
- Relevant events of the generation of pairs of own Keys or authenticity support. Under no circumstances shall the numbers themselves or any date which facilitates their prediction be included.
- All of the operations of the Keys archive service and of access to the expired own Keys archive.
- All of the operations related to the activity as reliable third party.
- All relevant events of the operation of the Time Stamping Authority, especially those corresponding to the synchronization of clocks and losses of synchronism. The exact moment which they are produced shall always be included.

5.4.6. Archive Protection

144. The FNMT-RCM guarantees that the registered events archive complies with the following requirements:

- It cannot be modified by unauthorized means.

- It must have a high degree of availability and reliability.
- The information shall be kept confidential, and any access made shall be traceable.

5.4.7. Making of security copies of the archives

145. There shall at all times be a security copy of all of the archives considered critical for conducting activity of the FNMT-RCM, due to its activity as *Trust Service Provider*.

5.4.8. Obtaining and verifying the filed information

146. Access to the archives registry shall be limited to the personnel authorized by the FNMT-RCM.

147. Access to encrypted data by third parties via the data recovery service without the user's authorization must always be done under the conditions established by the law and, if applicable, the corresponding contracts and agreements.

5.4.9. CA key change

148. Prior to the expiration period of validity of the Certificate for Authority Root Certification, or a subordinate Certification Authority, it shall proceed to the establishment of the new Authority root or corresponding subordinate, by generating of a new pair of keys. Ancient Certification Authorities and their associated private keys shall be used only to CRLs sign while there are active certificates issued by this AC.

5.5. INCIDENT AND VULNERABILITY MANAGEMENT AND CESSATION OF THE ACTIVITY

5.5.1. Incident and vulnerability management

149. FNMT-RCM guarantees the application of a consistent approach and effective information security incident management. The document "Information Security Management System-Security Manual" sets procedures and responsibilities for the incident management, ensuring which response, effective and ordered for all security incidents.

150. FNMT – RCM obtains technical vulnerability information about systems and appropriate measures are taken. Associated responsibilities are defined and established with the technical vulnerability management, keeping all resources in the assets inventory up to date, to identify technical vulnerabilities. In addition, periodic audit about the undertaken procedures are carries out and technical vulnerability management is monitored and evaluated.

151. The FNMT-RCM shall address any unforeseen critical vulnerability within a period of 48 hours after its discovery. Once its impact has been analyzed, the critical vulnerability shall be documented and its resolution will be decided by means of a mitigation plan, depending on the cost of its resolution.

5.5.2. Activity cessation of the trust service provider

152. In the event of termination of the activity of the *Trust Service Provider*, the FNMT-RCM shall be governed by that stated in the electronic signature regulations.

153. The FNMT-RCM shall under all circumstances:

- Duly inform the Subscribers and Holders of the Certificates, as well as the Users of the affected services, about its intention to terminate its activity as *Trust Service Provider* at least two (2) months before ceasing this activity.
- Terminate any subcontracts that it has to provide functions on behalf of FNMT-RCM of the service to cease.
- Transfer, with the express consent of the Subscribers, those Certificates which continue in force on the effective date of the cessation of the activity to another *Trust Service Provider* which accepts them. If this transfer is not possible the Certificates shall be extinguished.
- Whatever the service being ceased, the FNMT-RCM shall transfer to a third party the registries of events and audit, as well as the Certificates and keys used in the provision of the service, for a sufficient period for the purposes set out in the current legislation.
- Communicate to the Ministry which has competence in the matter at that time, the cessation of its activity and where it is going to transfer the Certificates , specifying if appropriate: if it is going to transfer them, to who, or if they shall become without effect. The notification to said body shall be done at least two (2) months in advance in a hand-signed or electronically-signed document. It shall also send said body the information relating to the Certificates which have been extinguished so that it can take charge of looking after them for the appropriate purposes.

154. In the event that the cessation is related to the *Time Stamping Service,* the FNMT-RCM shall:

- Process the revocation of the *Certificates* of the affected *Time Stamping Units.*
- Destroy the *Private keys* of the *Time Stamping Units* and their security copies, so that they cannot be recovered.

5.5.3. Operating procedure against the vulnerability of the signature creation data

155. This contingency is contemplated in the FNMT - RCM Business Continuity Plan and the procedure to follow is described in the Plan of crisis management as member part of the Plan of continuity, and that it is determined, among others, the following actions to take:

1) Stop the provision of affected service.
2) Revoke the certificates which could be affected.
3) Execute the Communication Plan with the consideration to communicate the facts to affected parties.

4) Study the need to execute the Cessation of Activities PSC according to DPC and current legislation.

5.5.4. Change of the Signature / Seal creation data of the FNMT-RCM

156. This contingency and its consequences are described in the section "Management of the lifecycle of the *Keys* of the *Trust Service Provider*" of this *TSPS*.

6. CONTROLS OF TECHNICAL SECURITY

6.1. MANAGEMENT OF THE LIFECYCLE OF THE KEYS OF THE TRUST SERVICE PROVIDER

6.1.1. Generation and installation of the Keys of the Trust Service Provider

157. For security and quality purposes, the *Keys* that the FNMT-RCM needs in order to develop its activity as *Trust Service Provider*, shall be generated by it within the its own infrastructure in a secure physical setting and at least by two duly authorized persons.

158. The generation of the *Keys* and the protection of the *Private Key*, is done meeting the necessary confidentiality measures, using secure and reliable hardware and software systems according to the regulations EESSI CWA14167-1 and CWA14167-2, as well as taking the necessary precautions in order to prevent their unauthorized loss, disclosure, modification or use, in accordance with the security requirements specified in the ESSI regulations applicable to the *Trust Service Providers*.

159. The *Key* algorithms and longitudes used are based on widely recognized standards for the purpose for which they are generated.

160. The technical components necessary for the creation of *Keys* are designed so that a *Key* is only generated once, and so that a *Private Key* cannot be calculated from its *Public Key* .

6.1.2. Storage, safeguarding and recovery of the Signature creation and verification data of the Trust Service Provider

161. The *Signature creation data* of the *Trust Service Provider* is protected by a cryptographic device which meets the FIPS PUB 140-2 Level 3 security requirements. The signature operations of *Certificates, Revocation lists,* data structures relating to the validity of the *Certificates and Electronic Time Stamps* are performed within the cryptographic device, which provides the encrypting to the *Signature creation data* of the *Trust Service Provider*.

162. When the *Signature creation data* is outside of the cryptographic device, FNMT-RCM takes appropriate technical and organisational measures to ensure its confidentiality.

163. The copy, safeguard or recovery operations of the *Signature creation data* are performed under the exclusive control of the authorized personnel, using at least dual control and in a secure setting.

164. A copy of the files and components is kept in order to restore the security setting of the cryptographic device, in the event that they have to be used, in duly guarded security envelopes within a fireproof cabinet which can only be obtained by authorized personnel.

6.1.3. Distribution of the public keys of the Trust Service Provider

165. The *Signature verification data* of the *Trust Service Provider* is distributed in a format according to the market standards, which can be consulted at www.cert.fnmt.es.

166. In order to check the authenticity of any "self-signed certificate", ultimate element of any *Certification Chain*, the corresponding digital fingerprint can be checked (in its different formats, see "*Certification Chain*").

6.1.4. Period of use of the Signature creation and verification data

167. The *Signature creation and verification data* of the *Trust Service Provider* and of the *Holders*, can be used while the *Certificate* is in force (you can consult the specific *Certification Policies and Practices* about the validity of the *Certificates*).

6.1.5. Uses of the Signature creation and verification data of the Trust Service Provider

168. The Signature creation data of the FNMT-RCM Certification Authority shall be used only and exclusively for the purposes of:

- Signing Certificates.
- Signing the Revocation Lists.
- Signing data structures relating to the validity of the Certificates

169. Furthermore, the Signature / Seal creation data of the FNMT-RCM, in its activity as Provider of other trust services, can be used for other purposes, such as:

- Signing Electronic Time Stamps
- Signing electronic documents other than the Certificates envisaged for the purposes and activities of the FNMT-RCM, under the circumstances set out in this TSPS and in the corresponding regulations.

6.1.6. Change of the Signature creation and verification data of the Trust Service Provider

170. The FNMT-RCM, depending on the progress on the issue of cryptographic, shall study the change of its *Signature creation and verification data*, when the circumstances make it advisable and minimizing the impact in its *Electronic Community*. In the event that said change is chosen, the FNMT-RCM shall notify such a change in its *Signature creation and verification data* via the site www.cert.fnmt.es. Additionally, it can provide the new *Signature creation and verification data* to the interested parties via said website.

6.1.7. End of the lifecycle of the Cryptographic Keys of the Trust Service Provider

171. The FNMT-RCM shall destroy or properly store the *Keys* of the *Trust Service Provider* when their valid period comes to an end, in order to avoid their improper use.

6.2. LIFECYCLE OF CRYPTOGRAPHIC HARDWARE USED TO SIGN CERTIFICATES

172. FNMT-RCM has the necessary means to ensure that the cryptographic hardware used to protect their keys as Trust Service Provider:

- It has not been tampered with during shipment, through a process of inspection including checks for its authenticity and possible manipulation.
- It is functioning correctly, through processes of continuous monitoring, periodic preventive maintenance inspections and service of software and firmware update.
- It is kept in a physically secure environment from receipt to destruction, as appropriate.

6.3. ACTIVATION DATA KEY

173. Certification authorities´ private keys are generated and guarded by a cryptographic device meeting the FIPS PUB 140-2 Level 3 requirements.

174. The triggers and private keys of the Certification authority are based on segmentation roles management and operation that FNMT-RCM has implemented with multi-person access mechanism with cryptographic cards and their corresponding pin son an M N simultaneous use scheme (2 from 5).

175. The triggers and use of private keys for the final entity certificates are based on access pins to the generation private keys methods used by the subscriber, that in all cases are maintained under their control and whose custody lies under their responsibility.

6.4. SECURITY CONTROLS OF THE TECHNICAL COMPONENTS

176. The definition of the security of all of the technical components that the FNMT-RCM uses in the performance of its activity as *Trust Service Provider*, as well as in its structure and procedures, includes everything relating to the security certification of the Information Systems, in accordance with the National Framework for the Certification of Information Systems Security which is passed in Spain, in particular those relating to EESSI which are published in the Official Journal of the European Union or in the corresponding Spanish Official Journals. The evaluation criteria of the security of the information technology ISO 15408 (Common Criteria) shall also be taken into account in the design, development, evaluation and acquisition of Information Technology products and systems which are to form part of the *Trust Service Provider,* as well as the EESSI regulations.

177. The security management processes of the infrastructure shall be periodically assessed.

6.5. NET SECURITY CONTROLS

178. The means of communication via public networks which the FNMT-RCM used in the performance of its activities use sufficient security mechanisms in order to avoid or adequately control any external aggression via these networks. This system is periodically audited in order to check it is functioning correctly.

179. In the same way, the infrastructure of the network which provides the certification services is provided with the security mechanisms needed in order to know the date in order to guarantee a reliable and integral service. This network is also periodically audited.

6.6. CONTROL OF SECURITY OF THE SYSTEMS

180. The integrity of systems and information of the FNMT-RCM, as *Trust Services Provider*, is protected against viruses, malicious and unauthorized software.

181. The FNMT-RCM has procedures that ensure the application of security patches within a reasonable time since their availability, unless their application introduces vulnerabilities or instabilities, in which case the reasons for their non-application shall be documented.

6.7. ENGINEERING CONTROLS OF THE CRYPTOGRAPHIC MODULE

182. Amongst the technical components provided to its users, and in order to increase public opinion in its cryptographic methods, the FNMT-RCM assesses the security of the products and services that it offers, using for this purpose open criteria accepted by the market.

6.8. SECURITY LEVELS

183. The security levels of the different components of the infrastructure, as well as the procedures and components which make up the activity of the *Trust Service Provider* shall be evaluated according to "Evaluation Criteria of the Security of the Information Technology Products and Systems"(ITSEC/ITSEM) and/or Common Criteria (ISO15408) and in particular according to the EESSI initiative.

184. Furthermore, regarding the management of the security of the information, it is performed according to guidelines indicated in UNE-ISO/IEC 27001 "Management Systems of the Information Security. Requirement".

185. The personal data shall be subject to that set out in the current regulations and specifically by the provisions of the Spanish Personal Data Protection Act (LOPD) and by Royal Decree 1720/2007, of 21st December, which develops the Constitutional Data Protection Act.

6.9. AUDITING PROCESSES AND SYSTEM MONITORING

186. The FNMT-RCM has a system of independent monitoring and recording events of its productive infrastructure. This system runs continuously (24x7), collecting information

and security events of all sensitive items and trusted of the Certification Authority for further processing and correlation.

187. This system provides reports of infrastructure security monitoring. Also, it has rules and policies that provide real time alarms if there is any anomalous behavior in Certification Authority systems or evidence of a security incident.

6.10. RE-ESTABLISHING THE SERVICES IN THE EVENT OF A FAULT OR DISASTER

188. The *Trust Service Provider* shall start up a Disaster Recovery Plan which covers:

- The redundancy of the most critical components.
- The start-up of an alternative support center.
- The complete and periodic check of the support copy services.
- Compromise of the Signature creation data of the *Trust Service Provider*. In this case the FNMT-RCM shall inform all of the members of the Electronic Community indicating that the Certificates, Revocation Lists, Electronic Time Stamps and any other data structure which can be signed are no longer valid due to said compromise. The FNMT-RCM shall proceed to re-establish the service as soon as possible and under the new conditions that are applicable.

189. The FNMT-RCM shall not be liable for the failure of the service or anomalies therein, or for the damage which may be caused directly or indirectly, when the fault or disaster is caused by force majeure, terrorist attack, sabotage or serious strikes; all without prejudice to performing the actions necessary in order to correct and/or resume the services as soon as possible.

6.11. UPGRADE OF ALGORITHMS

190. The FNMT-RCM is permanently informed about 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 safety degree.

6.12. TERMINATION OF THE ACTIVITY OF THE FNMT-RCM AS TRUST SERVICE PROVIDER

191. This contingency and its consequences are described in this *TSPS* in the section "Cessation of the activity of the *Trust Service Provider"*.

6.13. MONITORING OF CERTIFICATION SERVICES PROVIDING CAPACITY

192. The FNMT-RCM makes regular checks on the level of demand for services related to its activity as *Trust Service Provider* and the capacity of their infrastructure to provide such services, such as information system about consumption, degree of availability and resources occupancy. These controls allow identify future investments in infrastructure to maintain the capacity to provide these services.

6.14. CONTROL OF SYSTEMS DEVELOPMENT AND SOFTWARE

193. Before boarding a software development project, the *Certification Service Provider* follows the guidelines in the "Guide for establishing security requirements of the applications developed in Ceres". In this way it is ensured that the development of computer applications follows a process of risks assessment and analysis of security requirements.

194. The evolution of *Trust Service Provider* applications is made according to "Procedure for change management applications developed in Ceres." Such Procedure identifies the need for emergency software fixes or change control procedures for releases, assess their impact, to incorporate the approved changes and their documentation and check the consistency of the product definition.

7. CERTIFICATES´ PROFILE

195. All *Certificates* released by FNMT-RCM are in accordance with the X.509 version 3 standard, unless the *Particular Certification Practices and Policies* express the opposite for those certificates that apply to them.

7.1. NAMING RESTRICTIONS

196. The distinguished name (DN) assigned to the *Certificate´s Subscriber* in the domain of the *Certificate Service Provider* shall be unique and with the composition defined in the *Particular Certification Practices and Policies that* are applicable to every certificate.

197. The coding of *Certificates* follows the standard RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. All fields are defined in the certificate´s profile of *Particular Certification Practices and Policies*, except in the fields that specifically states the contrary, employing coding UTF8String.

7.2. USING OF THE EXTENSION POLICY CONSTRAINS

198. The root AC extension Policy Constrains of the certificate is not used.

7.3. SYNTAX AND SEMANTICS OF THE POLICY QUALIFIERS

199. The extension Certificate Policies includes, as a rule unless the Particular Certification Practices and Policies express different information, two fields:

- CPS Pointer: contains the URL where the *TSPS* and the *Particular Trust Service Practices and Policies* applicable are published.
- User notice: contains a text that could be displayed in the screen by the user of the certificate during the verification.

7.4. SEMANTIC PROCESSING EXTENSION OF "CERTIFICATE POLICY"

200. The extension Certificate Policy includes the field OID of policy, that identifies the policy associated to the certificate by FNMT-RCM, as well as the two fields related with the previous paragraph.

8. AUDITS

201. The FNMT-RCM shall maintain a specific system in order to make a registry of events for all those operations like: the issue, validation and revocation of the *Certificates*, issue of *Revocation Lists*, information about the state of the *Certificates* and issue of *Electronic Time Stamps*.

202. In order to minimize the impact on the systems in production, the audits on the affected systems in production are planned during times of low activity.

8.1. PROTECTION OF THE AUDIT TOOLS

203. All of the tools, reports, registries, files and sources related to the preparation or registry of an audit, are considered sensitive information and as such are treated in all aspects, and their access are restricted to authorized persons.

8.2. IDENTITY OF THE AUDITOR

204. The auditor, who checks the correct operation of the *Trust Service Provider* of the FNMT-RCM, must be a person or professional with sufficient official qualifications and adequate experience on the issue to be audited in accordance with the legislation in force at each time.

205. The performance of these audits can be entrusted to external Audit Companies, to qualified internal personnel (according to the current legislation) or both. In the case of internal personnel and depending on how critical the area to audit, the degree of independence of the personnel involved and their level of experience shall be specified in each case, according to parameters of functional independence.

206. In the cases where the audits are prepared by personnel external to the FNMT-RCM, the necessary measures and controls shall be established in order to regulate the audit requirements, the scope, access to the sensitive information and other agreements of *Confidentiality* and responsibility over the assets.

207. In the external audits, the auditor and the audit company shall never have any type of labor, commercial or any other type of relationship with the FNMT-RCM, or with the party requesting the audit, always being an independent company who performs the requested audit.

208. Together with the report obtained from the audit, the auditors shall be identified. The resulting audit report shall be signed by the auditors and by the manager of the audited entity.

8.3. RESULTS OF THE AUDIT AND CORRECTIVE ACTIONS

209. Any dissatisfaction detected in the audit shall be treated with the corresponding corrective actions. The action plan to start the corrective actions shall be prepared in the shortest possible period and shall be kept together with the audit report to be inspected and monitored in subsequent audits.

210. In the event that the defect found is a severe risk for the security of the System, of the *Certificates or Revocation Lists*, of the *Signature creation and creation data,* or any document or data considered *Confidential* in this document, of either the *Subscribers* or of the *Trust Service Provider*, the FNMT-RCM shall act as described in the *Contingencies Plan*, with the aim of safeguarding the security of the entire infrastructure.

211. Equally the FNMT-RCM shall act diligently to correct the error or defect detected in the shortest possible time.

8.4. COMMUNICATION OF THE RESULTS

212. The competent Administrative or Judicial Authorities can request the audit reports to check the proper functioning of the *Trust Service Provider.*

8.5. AUDIT PLAN

213. Periodically the corresponding audit plan shall be prepared which shall cover at least the performance of the following actions:

- Analysis of risks as pronounced in the Information Security Management System: An annual revision and a complete analysis every three (3) years.
- Revision of the Information Security Management System according to UNE-ISO/IEC 27001 "Information Security Management System. Requirements"
- Quality: ISO 9001: An external annual assessment examination plus a preparatory annual audit and a total external over three (3) years, in order to maintain the certification.
- Data protection. An internal one every two (2) years to be performed by the Information Systems Department.
- Every Certification Authority incorporated in the *Certification Chains* and the trust services set out in this Trust Services Practices and Electronic Certification Statement are subject to regular audits, as dictated by the relevant certification scheme related to:
    - The European standard ETSI EN 319 401 "General Policy Requirements for Trust Service Providers". Audit conducted annually by an accredited external company.
    - Each qualified trust service provided by FNMT-RCM is audited according to the corresponding scheme, and this is stated in the corresponding Particular Practices Statement.

- One audit every two (2) years of the information systems of the FNMT-RCM which it uses for the Provision of Certification Services and according to that set out in the National Security Guidelines (Royal Decree 3/2010, of 8th January, which regulates the National Security Guidelines within the scope of the Electronic Administration)

214. The following controls shall be performed:

- Internal controls on network security.
- Internal controls and tests of the contingency plan.
- Internal Quality and Security controls.
- Extraordinary: When thus required under the circumstances in the opinion of the FNMT-RCM.

8.6. VULNERABILITY ANALYSIS PROCEDURE

215. See vulnerability and incident management

8.7. INCIDENT DETECTION REPORTING PROCEDURE

216. In case of security incident, notification to affected parties shall be carried out as described in the *Security Policy* and its development regulations, especially in the *Incident Response Plan.* If a high impact incident occurs, shall be notified within 24 hours of the breach being identified.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. RATES

217. FNMT-RCM shall apply to Public Administrations the rates approved by the Sub secretary of which the provision depends for the certification services or, failing this, the rates agreed in the formally commissioned agreement for this purpose.

218. The rates applied to the private sector are governed by its contracts for certification services provision. Moreover, FNMT-RCM shall be able to establish their rates and payment terms appropriates at all times. The prices and payment terms shall be consulted in the website of FNMT-RCM, or shall be provided by the commercial department on request on email comercial.ceres@fnmt.es.

9.2. FINANCIAL RESPONSIBILITIES

219. FNMT-RCM, as a *Trust Service Provider*, is exempt from the provision of the guarantee required by the law (art. 20.2 of Law 59/2003 of December 19 on electronic signatures) for a liability insurance accordance with the additional provision fifth law 59/2003, of December 19, electronic signature, which amended section twelve Article 81 of Law 66/1997, of December 19, on Tax, Administrative and Social measures (norm range Act empowers the FNMT for the provision of services and electronic signature) with the following: "Twelve. In the exercise of the functions conferred upon this article, the

Fábrica Nacional de Moneda y Timbre- Real Casa de la Moneda shall be exempt from providing guarantee to what the paragraph 2 from article 20 in the Law 59/2003 electronic signature concerns".

220. However, the FNMT-RCM, besides being a public body of the Spanish state, has specific liability insurance for activity and *Trust Service Provider* with a coverage limit of 4,500,000.00 €.

9.3. PERSONAL DATA

221. The personal data protection regime deriving from the application of this *TSPS* and of the applicable joint action of any Administration, shall be that set out in the Constitutional Personal Data Protection Act 15/1999, of 13th December, and in the regulations which develop it. The files shall be publicly owned and their creation, modification or deletion shall be performed under general regulations published in the Official State Gazette.

222. As a result of the provision of the EIT services, the *Registry Offices* can access the files of users of Electronic, Computer and Teleprocessing Systems. In any event, it shall be the FNMT-RCM as *Party Responsible for the File* which shall decide on the purpose, content and use of the data processing, with the *Registry Offices*, as *Data Processers,* limiting themselves to using the personal data contained in said file only and exclusively for the purposes set out in the *TSPS*. The *Registry Office* in compliance with that established in article 12 of the Constitutional Personal Data Protection Act 15/1999, of 13th December, undertakes to:

- Process the data strictly following the instructions of the FNMT-RCM.
- Refrain from applying or using the personal data obtained for purposes other than those featuring in this TSPS.
- Refrain from communicating it to third parties, even for safekeeping.
- Maintain professional secret over them, even after the end of its relations with the FNMT-RCM and transfer the obligations cited in the previous paragraphs to the personnel devoted to fulfilling this TSPS.
- Adopt the technical and organizational security measures in order to guarantee the security of the personal data and avoid its unauthorized alteration, processing or access, in accordance with that set out in Royal Decree 1720/2007, of 21st December, which passes the Regulations which develop Constitutional Act 15/1999.
- Destroy or return all personal data object of processing once the relations ends for whatever reason with the FNMT-RCM, except that data which the legislation states must be kept for at least fifteen (15) years.

223. Without prejudice to other obligations, the *Registry Office* shall check that the *Subscriber* and the *Holder* are informed and provide their *Consent* to the processing of their data, with the purposes and communications set out in the corresponding *Consent* documents. It shall also check correct compliance with all of the personal data fields necessary for the provision of the service.

224. The *Registry Office* shall inform this obligation to all of its personnel and shall be liable for any harm caused to the FNMT-RCM as a result of breach of these obligations in the collection data, and must also and on this matter keep it unscathed from any third party claims or administrative sanction.

225. The personal data of the *applicant*, after being validated and, in its case, its application code collected in the request Certification phase shall be sent to the la FNMT-RCM via secure communications established for such purpose between the *Registry Office* and the FNMT-RCM.

226. The FNMT-RCM can identity, when thus required, the *Users* of the certification services via other *Certificates*. In these cases and as regards the personal data protection of the *Users* of the services, that declared for the management of *Certificates* shall be applicable as well as the aforementioned regulations.

9.3.1. Information to the Subscriber

227. In accordance with that established in article 5 of the Constitutional Personal Data Protection Act 15/1999, of 13th December, the *Subscriber* or *Holder* shall be informed that the personal data included in the forms or contracts which are presented during their appearance to request the issue of a *Certificate* shall be registered in the rule for users of Electronic, Computer and Teleprocessing Systems (EIT), established by Order EHA/2357/2008, of 30th July (BOE – Official State Gazette – of 7th August), which regulated the personal data files of the FNMT-RCM, and for which the FNMT-RCM is responsible.

228. The provision of the EIT services can only be performed if the forms are completely completed with true data and information. Said data is collected in order to provide the certification services under the terms established in the current regulations and in this *TSPS*. By their completion, the parties consent to the processing of their data for the envisaged uses and purposes, without prejudice to the exercise of the rights recognized for these purposes in the applicable legislation.

229. The personal data can be communicated without the consent of the *Subscribers* or *Holders* of the *Certificate* to another Public Administrations, their autonomous bodies and other related or dependent entities so that they can exercise their respective competences and always within the scope of article 81 of the Tax, Administrative and Social Order Measures Act 66/1997, of 30th December, and regulations that develop it. All for the purposes of guaranteeing the provision of the certification services and in order to check the validity of the *Certificates* issued to the *Holders,* also permitting the performance of actions in the scope relating to public law via electronic, computer and teleprocessing methods.

230. Furthermore, the personal data can be ceded and/or communicated to the members of the *Electronic Community* who are not considered Public Administration and/or Public Bodies, in accordance with article 11.2.c of the Constitutional Personal Data Protection Act (LOPD) in the scope of private law relations, when necessary to cede and/or communicate for the performance, compliance and control of the services contracted and/or requested from the FNMT-RCM by the *Subscribers* or *Holders* of the certificates or

persons or entities authorized by these certificate holders. This cession and/or communication shall be performed exclusively to comply with the purpose for which the *Certificate* has been issued, in accordance with the electronic signature regulations and according to the uses that the certificate holder is going to make under the terms of the corresponding contract and/or agreements with the FNMT-RCM and authorized third parties.

231. The holder of the data can exercise the rights to access, correct, cancel and oppose when the FNMT-RCM is responsible for the file by contacting the General Secretariat of the FNMT-RCM situated in Jorge Juan 106, 28071 Madrid, or via

https://www.sede.fnmt.gob.es/certificados/persona-fisica/modificar-datos

(Modification of personal data), without prejudice to the preservation obligations established in the Act. Equally, in order to know the scope of the *Electronic Community* its composition can be checked for the indicated purposes at the same website exercising the corresponding rights.

232. The FNMT-RCM adopts the security levels required by the Security Measures Regulations passed by Royal Decree 1720/2007 of 21st December.

9.3.2. Information to the User Entity

233. The data contained in the secure *Directory* of *Certificates* is considered personal data for the purposes of that set out in the Constitutional Personal Data Protection Act (LOPD) and other complementary regulations, and as such the FNMT-RCM does not allows access to them.

234. The FNMT-RCM does however make available to *User persons and Entities* the lists of revoked certificates (which do not contain personal data) in order to diligently fulfil the certification services in accordance with Order EHA/2357/2008, of 30th July, which regulates the personal data files of the FNMT-RCM. The *User entities* as assignee of this information can only use it in accordance with these purposes.

235. However and in general, any requirement or use for purposes other than the above or unauthorized requires the prior *Consent* of the owners of the data as well as other provisions set out in the Act. Its breach is sanctioned in the LOPD with fines of up to 600,000 Euros for each breach committed and without prejudice to the filing of criminal proceedings in accordance with Chapter I of Heading X of the Criminal Code as well as private claims from the affected parties.

236. The FNMT-RCM in accordance with the legislation regulating the DNI-e (Electronic National Identity Card) can perform validation services on the validity of the electronic certificates incorporated in the DNI-e, and as such in cases where electronic identification is possible with the DNI-e to access services envisaged in this TSPS, the FNMT-RCM is authorized by the holders of the DNI-e with activated computer function, to cede and/or communicate to other members of the *Electronic Community* when necessary within the scope of public and/or private law relations for the purposes set out in article 11.2 c) of the LOPD.

9.3.3. Constitutional Personal Data Protection Act (LOPD) Security Document

9.3.3.1. Objective and presentation of the LOPD Security Document

237. The objective of this document is to establish the security measures to be implemented by the FNMT-RCM on the setting of the *Trust Service Provider*, to protect the personal data contained in the File of Users of Electronic, Computer and Teleprocessing Systems (EIT), registered in the Spanish Personal Data Agency (*AEPD)* and identified in Order EHA/2357/2008, of 30th July, which regulate the personal data files of the FNMT-RCM.

238. The FNMT-RCM, as *Trust Service Provider*, needs the personal data of its registered users in order to be able to identify them and provide the *Signature verification data* and provide the corresponding certification services, essential for the relationship via electronic, computer and teleprocessing means. Given the nature of this type of data, as indicated by Royal Decree 1720/2007 of 21st December, medium level security measures must be adopted.

239. These Security Regulations aim to preserve the personal data processed by the *Trust Service Provider* of the FNMT-RCM, and affect all of the resources (personnel, machines, applications, methods) which are involved in processing this data. From the Information System which perform the registry functions of the users, where the data is collected, to its storage and filing in *Secure Directory* services, identification and/or authorization systems, filing and event registry systems, and any other which may participate in the provision of certification services, including the interfaces and communication between the different systems, whether private or public teleprocessing networks.

240. This document is compulsory for all personnel belonging to the *Trust Service Provider* of the FNMT-RCM, as well as all of the personnel relating to it who require access to the personal data.

241. The responsibility for all of the files which contain personal data declared by the FNMT-RCM corresponds to said entity, as it is the legal entity which decides on the purpose, uses and content of the files. However, as regards the File of "Users of EIT Systems", the Director of Information Systems of the FNMT-RCM is the personal authorized to decide and authorize its use and processing on behalf of the FNMT-RCM.

242. Within the scope are the *Registry Offices* as collaborating entities of the FNMT-RCM as *Trust Service Provider*, which have the mission of carrying out the identification and authentication of the citizen, registering their personal data for the *Trust Service Provider* of the FNMT-RCM.

9.3.3.2. Regulations and standards

243. The laws, regulations and standards which have been considered for the preparation of this document, without prejudice to any updates, are:

European Directives

- European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- European Parliament and Council Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector

Spanish Legislation

- Constitutional Personal Data Protection Act 15/1999, of 13th December.
- Royal Decree 1736/1998, of 31st July, which develops Title III of the General Telecommunications Act (Public Service Regulations).
- Royal Decree 1720/2007, of 21st December, which passes the Regulations developing Constitutional Act 15/1999
- Order EHA/2357/2008, of 30th June, which regulates the personal data files of the FNMT-RCM

9.3.3.3. Compulsory principles and regulations

244. This section contains all of the necessary compulsory aspects which respond to the sections established in *article 88 of the Regulations developed by Constitutional Act 15/1999 (Royal Decree 1720/2007).*

Functions and obligations of the personnel

245. This Document and any new version of it and those which represent the particular policies and practices of the different certification services are known by all of the persons belonging to the *Trust Service Provider* of the FNMT-RCM or who have the obligation with said personal data.

246. There is a series of clearly differentiated functions as regards the personnel involved in using and processing the personal data of the File of Users of EIT Systems, who are: *The Party Responsible for the File, the Party Responsible for the Security*, the *Computer Security Personnel*, *Administrator of the Application*, *Users of the Application*, *Backup Operator*, *Security Auditor*. These functions, and if applicable the people who assume them, are defined in the point "*LOPD Security Document*" of the "Definitions" section of this *TSPS*.

Structure of the files with personal data and description of the information systems which process it

247. The structure of the personal files used by the *Trust Service Provider* of the FNMT-RCM, is that contained in the File of Users of EIT Systems , which has been declared by the *Spanish Data Protection Agency* and described in the APPENDIX of Order EHA/2357/2008, of 30th June, which regulates the personal data files of the FNMT-RCM, with the file being identified as "File of users of electronic, computer and teleprocessing (EIT) systems".

248. The subsystems which have any involvement in processing the personal data within the scope of Royal Decree 1720/2007, are listed and described in brief below:

Certificate Management Subsystems

249. Whose mission is the creation of the *Certificates* in accordance with standard *X.509*, which introduce the *Keys* created by the *Key* generation subsystems and other identifying data.

Registry Office Subsystem

250. It has the objective of identifying and authenticating the *Subscriber*, where its personal data is registered in order to send it, encrypted, to the *Trust Service Provider* of the FNMT-RCM.

Publication Subsystem

251. It has the mission of managing the publication of the *Directory* of the *Trust Service Provider* of the FNMT-RCM and *Revocation Lists.*

Notification, management and response procedure in the event of incidents

252. The personal data lie in *Certificates*, structured in accordance with standard *X.509*, some of which are for public use.

253. The access, rectification, cancelation and opposition procedure of the personal data is formalized. It can be exercised in the General Secretariat of the FNMT-RCM or the webpage of the *Trust Service Provider* of the FNMT-RCM.

254. The accidental destruction incidents of personal data information are solved with *Available* security copies, properly stored and managed and duly registered.

255. There is a database of incidents which open and manage the incidents. Each person can perform different processes in accordance with the role that they perform. In short, any person belonging to the *Trust Service Provider* can open an incident. They are processed by personnel from the corresponding area and once settled are closed with the description of the actions performed. In the event that the incident involved modifications, a corrective action performed by the competent personnel is opened.

256. The main fields of an incident are:

- Name of the incident (brief description)
- Person opening the incident, date of opening
- Area competent for the incident
- Priority
- Type (in general it corresponds to the affected Hardware/Software)
- Description (detailed description of the incident)
- Actions (actions performed to solve the incident)
- Registry of persons handling the incident.

Security copies and data recovery procedures

257. The backup/recovery policies of the *Trust Service Provider* have defined six different types of data, according to its copy and backup requirements. All of the data processed by the *Public Key Infrastructure* have been classified in some of these "Types".

258. The Types referring to personal data are as follows:

TYPE 3. Audit Information: They show the functioning of the application systems and settings over time, and constitute evidence and traces of the actions which are being performed and the applications that are executed. As such, it may contain information relating to its clients' personal data.

TYPE 5. Personal data: Data associated to identified or identifiable individuals, whether considered private or public.

TYPE 6. Keys: Basically, this category covers the master access keys to the application systems and settings, critical keys of the systems, administration keys and emergency keys. Its use is occasional.

259. The characteristics which have been defined for making security copies take the following factors into account:

- Periodicity of the security copy (frequency with which they must be made)
- Duration of the security copies (time for which the copies must be kept)
- Type of security copy (total or incremental)
- Storage (destination of the security copies)
- Encrypting (providing Confidentiality)
- Firming (providing Integrity and authenticity)

260. Specifically for Type 5 data, i.e. personal data, the following characteristics have been defined:

- Periodicity of the security copy: At least one security and backup copy of this data shall be made every day, complying with the applicable legislation.
- Duration of the security copies: The security copies shall be stored for a period of seven working days.
- Type of security copy: The backup copies shall always be made complete.
- Storage: Then security and backup copies shall be stored in a high security fireproof file of the *Trust Service Provider* of the FNMT-RCM.
- Encrypting: The information shall not be encrypted
- Signing: The information shall not be signed.

261. The detailed information on these classifications is in the *Security Manual* of the *Trust Service Provider* of the FNMT-RCM. Said manual defines those responsible for the copies, who can access them and who must communicate any incidents.

262. More detail on this process is described in the document on security, back and recovery copies policies of the infrastructure called "Backup/recovery policies".

Access control

263. Only the assigned profile has access to the data, provided that said access is necessary in order to perform the different functions.

264. For example, the *Registry Office* must provide the access control requirements to the information system of the *Trust Service Provider* of the FNMT-RCM to the registrars, providing them with the level of access to perform the registry function.

- Access control based on profiles: using the identity or the profile of the system user who requests access, together with the type of access requested.
- Access shall be provided whenever the identified user requests a type of access which has been previously authorize, otherwise it will be refused.

265. The *Party responsible for the File* has established mechanisms to avoid the user being able to access personal data with rights which are not permitted and in order to prevent repeated unauthorized access attempts to the information system.

Working regime outside of the premises where the file is located

266. All work on the personal data is performed in the work center of the FNMT-RCM as *Trust Service Provider*.

267. As mentioned in the previous section, the registry function is performed in the *Registry Offices* by duly authorized persons.

Temporary files

268. The software available to process personal data needed in order to create electronic certificates in accordance with standard *X.509* generates temporary files (log files) which are duly guarded for tracking purposes of the *Trust Service Provider* activity in compliance with the Act 59/2003, of 19th December, of electronic signature.

269. In any event, these files have the same security level as the declared file and therefore the same security controls are applied to them.

Management of supports

270. The computer supports which contain personal data are diligently identified, being able to identify the information that they contain. They are also stored in a place with access restricted to authorized personnel and looked after by security personnel.

271. In the event that a computer support containing personal data leaves the work center of the *Trust Service Provider* of the FNMT-RCM, it can only be authorized by the *Party Responsible for the File.*

272. The destruction of supports will be done after said support is removed from the “backup application) security and backup copy application which acts as inventory of supports) and consists of the physical destruction of the support (extraction of the magnetic tape from its container and its shredding).

273. There is a supports entry registry system which directly or indirectly provides information on:

- The type of support.
- The date and time of entry.
- The issuer.
- The number of supports.
- The type of information it contains.
- The type of sending.
- The person responsible for receiving the information, who must be directly authorized by the Party Responsible for the File.

274. There is also a supports exit registry system which directly or indirectly provides information on:

- The type of support.
- The date and time of exit.
- The recipient.
- The number of supports.
- The type of information it contains.
- The type of sending.
- The person responsible for delivering the information, who must be directly authorized by the Party Responsible for the File.

275. When a support is going to be thrown away or reused, the envisaged procedure will be followed in order to prevent any subsequent recovery of the information stored therein. This procedure shall be followed before withdrawing the support from the Inventory.

276. When the supports are to leave the premises where the files are located due to maintenance operations, the necessary measures shall be adopted in order to avoid any improper recovery of the information stored therein.

Audit

277. In order to comply with all of the aspects indicated in the *LOPD* an audit will be performed to check compliance with the regulations and instructions indicated in this document. This audit shall be performed at least once every two (2) years.

278. This audit report refers to the adaptation of the regulations and instructions indicated in this document, identifying the weaknesses and proposing the relevant corrective actions. The report shall also include the data, events and observations on which the report is based, as well as the proposed recommendations.

Logical Access

279. There are various types of logical access to the file:

- Access with user name and passwords: access in which a user of the applications looks for the Public Key of a Holder starting with its identification data ("serial number of the Certificate, "common name", etc.).
- Privileged access to the Directory or database, which stores all of the personal data. For this type of access the application must be registered in accordance with the security regulations of the *Trust Service Provider* of the FNMT-RCM.

280. The parameters which are configured and which include that required by the LOPD Regulations are those described below:

- Each user is identified vis-à-vis the application with the user name which is unique for each person.
- All users must authenticate themselves by entering a password which is only known to the user. Every user is responsible for their password and they must not share it with anybody else.
- Groups of people have not been created who can access using the same user name and password, and nor are there generic users. The generic accounts which are created for tests or similar purpose are immediately eliminating after said tests.
- Each user is free to change their password if they think it may be compromised, but to do so they must have used it for at least one day. Notwithstanding the above, the user must not use the same password for over three (3) years.
- When a user is identified and authenticated more than three times incorrectly, the system blocks the account of said user.
- There is a control mechanism: the Registry of Events in charge of storing, amongst other information, all access to the different parts of the infrastructure.

Physical Access

281. Only the duly authorized personnel have physical access to the premises housing the information systems with personal data, i.e. the Data Processing Centre of the *Trust Service Provider* of the FNMT-RCM.

282. In order to access these installations there is an access control system using card readers and keypads.

283. Periodically there is a control of the registries of events generated by the access control system which will allow for the detection of any type of anomaly in the daily operations.

Tests with real data

284. The tests in the development of the applications which deal with the EIT File are not done with real data.

285. The various applications which require access to said file are done by loading test data.

9.3.3.4. Revision process

286. The "*LOPD Security Document"* section has been prepared to comply with Royal Decree 1720/2007, of 21st December, which passes the Regulations developing Constitutional Act 15/1999.

287. The Document will be kept updated. All modifications which are produced as a result of improvements or adaptation of the legal regulations shall be incorporated into the Document.

9.4. INTELLECTUAL AND INDUSTRIAL PROPERTY

288. The FNMT-RCM is the exclusive owner of all of the rights, including the exploitation rights, over the *Secure Certificates Directory*, *Revocation Lists*, information services on the state of the *Certificates* and *Time Stamping* services under the terms indicated in the Consolidated Intellectual Property Act passed by Legislative Royal Decree 1/1996, of 12th April (Intellectual Property Act), including the *sui generis* right recognized in article 133 of said Act. As a result, access to the *Secure Certificates Directory* is permitted for the members of the *Electronic Community* authorized for such purpose, with any reproduction, public communication, distribution, transformation or reorganizing being prohibited unless expressly authorized by the FNMT-RCM or the law. It is also prohibited to extract and/or reuse all or a substantial part of the content, whether considered as such from a quantitative or qualitative perspective, or their repeated or systematic performance.

289. Access to the *Time Stamping* services will be restricted according to that stated in the particular policies and practices which regulate said services.

290. The FNMT-RCM all rights, ownership and participation over the intellectual and industrial property right and know how relating to this *TSPS*, the declarative documents (policies and practices) which specify or complete this TSPS, the services that it provides, and the computer programs or hardware used in the provision of said services.

291. Furthermore, both the *Cryptographic card* used as a support to store the cryptographic *Certificates* and *Keys*, as well as the information generated through the provision of the services by the FNMT-RCM shall at all times by exclusively owned by the FNMT-RCM,

292. As regards the *Cryptographic card*, the FNMT-RCM only grants a user right to the *Subscribers* of the *Certificates*, for them to use them as a support to store and use the cryptographic *Certificates* and *Keys* issued by the FNMT-RCM or by another *Trust Service Provider* .

293. The *OID* used in the issued *Certificates*, in the *Certificates* used to provide the services, in the *Electronic Time Stamps* and for the storage of certain objects in the *Directory*, are owned by the FNMT-RCM and have been registered in the IANA (Internet Assigned Number Authority) under branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA-Registered Private Enterprises), having been assigned number 1.3.6.1.4.1.5734 (FABRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA). This can be consulted and checked at:

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

294. Unless expressly agreed and signed with the FNMT-RCM, the total or partial use of any of the *OID* assigned to the FNMT-RCM is expressly prohibited except for the specific requirements for which they are included in the *Certificate* or in the Directory.

295. It is prohibited to reproduce or copy even for private use of the information which may be considered as Software or Database in accordance with the legislation in force in relation to Intellectual Property, or its public communication or providing it to third parties.

296. Any extraction and/or reuse of all or a substantial part of the contents or databases which the FNMT-RCM has available to the *Subscribers or Use entities* are expressly prohibited.

9.5. ORDER OF PREVALENCE

297. The different Particular *Certification Policies and Practices* will have prevalence as regards the particular nature and referring to the types of *Certificates* and/or services in question, over that set out in the main body of this *TSPS*.

9.6. CHANGE MANAGEMENT PROCEDURE

298. Amendments to this document and to the Particular Practices and Policies Statements shall be approved by the Directorate of Ceres Department, which shall be reflected in the corresponding minutes of the Management Committee of the Trust Services Provider, in accordance with the internal procedure approved by the document "Procedure for review and maintenance of certification policies and declaration of practices of trust services".

299. The Management Committee of the Trust Services Provider shall annually review these Statements and, in any case, whenever any changes must be made.

300. If the changes to be made do not imply significant changes in the regime of obligations and liabilities of the parties or related to a modification of the policies of provision of services, FNMT-RCM will not previously inform users. The new version of the affected statement shall be published at the corresponding website.

301. Significant changes in service conditions, obligations and liabilities or limitations of use may lead to a change in service policy and its identification (OID), as well as a link to the new service policy statement. In this case, the FNMT-RCM may establish a mechanism to inform the proposed changes and, where appropriate, gather opinions of the affected parties.

9.7. APPLICABLE LAW, INTERPRETATION AND COMPETENT JURISDICTION

302. The provision of trust services by the FNMT-RCM shall be governed by the Laws of the Kingdom of Spain.

303. In general, the members of the *Electronic Community* and the *Users* of the trust services of the FNMT-RCM accept that any dispute, disagreement, issue or claim resulting from the execution or interpretation of the *Trust Services Practices Policies and/or Statements* or directly or indirectly relating to them, shall be settled in accordance with that established in the corresponding contracts, general conditions and/or agreements, under the terms set out in the entity's Articles of Association passed by Royal Decree 1114/1999, of 25th June

(BOE – Official State Gazette – no. 161 of 7th July). They can also agree, following agreement by the competent body of the FNMT-RCM, arbitration clauses in accordance with the applicable legislation.

304. In the event that contracts, general conditions and / or parcels or agreements do not specify conflict resolution systems, all parties submit to the exclusive jurisdiction of the courts of the Spanish State in the city of Madrid

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

9.8. PROVISION OF CERTIFICATION SERVICES AND ELECTRONIC SIGNATURE OF OWN CERTIFICATES

306. If there is no legal prohibition, the FNMT-RCM can perform its activity as provider of own electronic certificates when in the development of purposes other than the certification services validation and/or other services are necessary with the various members of the *Electronic Community*.

307. In the event of a conflict of interests due to the aforementioned activity, between the FNMT-RCM and other members of the *Electronic Community,* both parties can submit their disagreement to the one or more arbitrators, or resolve it before the courts or tribunals competent according to the rules of the aforementioned jurisdiction.

ANNEX: ROOT CA CERTIFICATE PROFILE

Campo		Contenido	Ext. Crit ica	Especificaciones
1. Version		2		Integer:=2 ([RFC5280] describes the certificate version. The value 2 indicate that the certificate is version 3 (X509v3)
2. Serial Number		Unique identification number of the certificate.		Integer. SerialNumber = e.g.: 111222. Established automatically by the Certification Entity. [RFC5280]. Will be a positive "integer", not longer than 20 octets (1- 2_{159}). The serial number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Issuing entity of the certificate (Root CA)		
	4.1. Country	C=ES		Will be encoded according to "ISO 3166-1- alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Name ("official" name of the organisation) of the Trust Service Provider (certificate issuer). O=FNMT-RCM		UTF8 String
	4.3. Organization Unit	OU=AC RAIZ FNMT-RCM		UTF8 String
5. Validity		Until 01/01/2030		UTCTime format, in accordance with RFC 5280
6. Subject				
	6.1. Country	C=ES		Will be encoded according to "ISO 3166-1- alpha-2 code elements". PrintableString, size 2 (rfc5280)
	6.2. Organization	Name ("official" name of the organisation) of the Trust Service Provider (certificate issuer). O=FNMT-RCM.		UTF8 String
	6.3. Organization Unit	OU=AC RAIZ FNMT-RCM		UTF8 String
7. Subject Public Key Info		Algorithm: RSA Encryption Length: 4096 bits		Field for carrying the public key and for identifying the algorithm with which the key will be used.

Campo			Contenido	Ext. Crit ica	Especificaciones
8. Subject Key Identifier			Identifier of the public key of the Subordinate CA. Used to identify certificates that contain a specific public key and facilitate the construction of certification paths.		RFC 5280: 20-byte SHA-1 hash calculated based on the BIT STRING of the subjectPublicKey field of the subject (excluding tag, length, and number of unused bits).
9. Key Usage			Permitted use of the certified keys.	Yes	Standardized in standard X509 and RFC 5280
	9.1. Digital Signature		0		See X509 and RFC 5280
	9.2. Content Commitment		0		See X509 and RFC 5280
	9.3. Key Encipherment		0		See X509 and RFC 5280
	9.4. Data Encipherment		0		See X509 and RFC 5280
	9.5. Key Agreement		0		See X509 and RFC 5280
	9.6. Key Certificate Signature		1		See X509 and RFC 5280
	9.7. CRL Signature		1		See X509 and RFC 5280
10. Certificate Policies			Certification policy		
	10.1. Policy Identifier		2.5.29.32.0 (anyPolicy)		According to rfc5280: *"In a CA certificate,these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }"*
	11.2. Policy Qualifier Id				
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/		IA5String String. URL of the conditions of use.
11. Basic Constraints				Yes	
	11.1. cA		Value TRUE (CA)		According to rfc5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."
	11.2. pathLenConstraint		No		There is no length restriction map root level CA