Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SPECIFIC CERTIFICATION POLICIES AND PRACTICES APPLICABLE TO ELECTRONIC CERTIFICATION AND SIGNATURE SERVICES FOR PUBLIC ORGANIZATIONS AND ADMINISTRATIONS, THEIR BODIES AND ATTACHED OR DEPENDENT ENTITIES

	NAME	DATE
Prepared by:	FNMT-RCM / v2.4	17/05/2016
Revised by:	FNMT-RCM / v2.4	17/06/2016
Approved by:	FNMT-RCM / v2.4	24/06/2016

BACKGROUND OF THE DOCUMENT		
Version	**Date**	**Description**
1.0	06/11/2008	Creation of the document
1.1	05/05/2009	Expansion of certificate validity to four years.
1.2	01/08/2010	Deletion of the organization aspects section as it is included in the DGPC Obligation to show entity to which signatory provides services (Certificate Subscriber) in the certificate of personnel working for public administrations in the extension subjectAltName Modification of certificate profiles. Inclusion of new profiles in accordance with new certification policies.
1.3	03/07/2011	Deletion of sections related to information on management of policies pertaining to this document as they are already included in the DGPC. Modification in certificate profiles to change AIA field value in certificates for end entities.
1.4	19/12/2011	Addition of definitions of people related to certificate management. Addition of definitions on delegate Registry Offices and requesting Registry Offices for implementation of user registration activities by delegation. Modification in certificate profile table: the serial number of AP certificates is assigned randomly.
1.5	31/10/2012	Removal of AC references known as "APE AC". This type of certificate-related information can be found in earlier versions of this document.. Deleted 2,4,7 and 9 profile certificate tables. Correction of errors in certificates profiles: the CRL's distribution point of end-entity certificates is http://www.cert.fnmt.es/crlsacap/CRLxxx.crl End-entity certificates will have a validity period of 3 years. Modification of certificates auto-revocation policies. When an equal Subscriber requests the issuance of a new certificate, the certificates of site and seal are not revoked. Remarks about considering the Cryptography Card a secure device for signature creation.
1.5	31/10/2012	Rectification of mistakes on reference to paragraphs ETSI 101 456 about the exclusions to this rule. Removed the sections of "Forms models" as these are available through each document generation.application.

BACKGROUND OF THE DOCUMENT		
Version	**Date**	**Description**
1.6	29/5/2013	Replacement of the term holder by signatory or subscriber. Removal of last paragraph of the description type of civil servant certificate, which interpreted the application of the law on electronic signature in the certificate of personnel working for public administration. Clarification of the private use of public employee certificate.
1.7	3/7/2013	Clarification of paragraph 51 about private use of the Certificate permitted to public employees
1.8	02/04/2014	Alignement with the LTE general liability regime PSC regarding the Registration Offices and for the consent of "signatory" in case of termination of activities of the PSC. Some links to the Risk Application have been updated.
2.0	16/06/2014	Alignement with the LTE general liability regime PSC regarding the Registration Offices and for the consent of "signatory" in case of termination of activities of the PSC. Some links to the Risk Application have been updated. Revision according to WebTrust.
2.1	17/11/2014	Issuance of certificate with SHA-256. Reduction of the maximum period of certificates suspension to 30 days. Elimination of QcLimitValue field profiles certificates. Revocation of certificates of personnel working for the Administration via phone 24x7
2.2	10/07/2015	Revision according to ETSI 101 456
2.3	27/01/2016	Revocation 24x7 of certificates for identification of electronic venues of the Public Administration and certificates for automated administrative actions.
2.4	24/06/2016	Modification of certificate profiles in accordance with CAB/Forum requirements.

Reference: DPC/ PCPAA0204/SGPSC/2016

Document classified as: *Public*

TABLE OF CONTENTS

1 PREAMBLE

1. Article 81 of Law 66/1997, of 30th December, on Tax, Administrative and Social Order Measures enabling provision of security services by the Fábrica Nacional de Moneda y Timbre *(Royal Spanish Mint)*, in communications through electronic, computer and telematic techniques and means, in section One, establishes that:

   "without prejudice to the competences attributed by the Law to administrative bodies with relation to registration of applications, written documents and communications, the Fábrica Nacional de Moneda y Timbre (FNMT) is empowered to provide the necessary technical and administrative services to ensure the security, validity and efficacy of issue and reception of communications and documents through electronic, computer and telematic techniques and means (EIT) in the relationships established between:

   a) Bodies of the State General Administration between each other or with public bodies attached to or dependent on the former, as well as between these bodies.

   b) Individuals or legal entities with the State General Administration (AGE) and public bodies attached to or dependent on the same"

2. Separately, its section Two, establishes:

   "Likewise, the FNMT is empowered, as appropriate, to provide to the Autonomous Communities, local entities and Public Law entities attached to or dependent on these, the services referred to in the above section, in the relations established through EIT techniques and means between each other, with the State General Administration or with individuals or legal entities; provided that, previously, all relevant agreements have been formalized".

3. The legal framework derived from approval of Law 11/2007, of 22nd June, on Citizens' Electronic Access to Public Services (LAECSP), establishes citizens' right to communicate with the various public administrations. Exercise of this right must be linked to implementation, within the Public Administrations and their bodies and attached or dependent entities, of the infrastructures and new electronic and telematic systems contemplated in the above regulation, all necessary for the foreseen undertaking and execution. Also, the Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration regulates identification systems and electronic signature used in the scope of Administration of Justice.

4. The various electronic identification and authentication systems which the Public Administrations may use and referred to by this Statement include:

   1) **Electronic signature** for personnel working for Public Administrations, Bodies and attached or dependent public entities, hereinafter **personnel working for the Public Administration**.

   2) Electronic signature systems based on the use of Certificates with secure devices or equivalent means that allow identifying the **electronic venue** and thereby establishing secure communications with it.

   3) Electronic signature systems for **automated administrative/legal actions**.

2 INTRODUCTION

5. This document is an integral part of the FNMT-RCM's General Certification Practices Statement and its purpose is to provide public information on the conditions and characteristics of the certification services and issuing services for electronic Certificates by the FNMT-RCM as Certification Services Provider, covering, in particular the duties and procedures it undertakes to fulfil with relation to the issue of Certificates for identification of electronic venues, electronic signature systems for automated administrative/legal actions and Certificates issued for personnel working for the Public Administration.

6. Of particular note in order to interpret these Specific Certification Policies and Practices, is the section "Definitions" in the General Certification Practices Statement, and, as the case may be, the Issuance Law corresponding to each body and/or user body or entity of the FNMT-RCM certification services.

7. Certificates issued by the FNMT-RCM for personnel working for the Public Administrations whose Specific Certification Policies and Practices are defined herein are considered technically Recognized Certificates, as defined under Law 59/2003 on Electronic Signatures and standard ETSI 101 456, and valid to conduct electronic signatures by personnel working for the Public Administrations and as defined under Law 11/2007, of 22nd June, on Citizens' Electronic Access to Public Services, under Royal Decree 1671/2009 (articles 21st and 22nd), and under Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration.

8. Certificates issued by the FNMT-RCM for electronic identification of electronic venues of the Public Administrations whose Specific Certification Policies and Practices are defined herein are considered technically Recognized Certificates, as defined under Law 59/2003 on Electronic Signatures and valid for identification of electronic venues as defined under Law 11/2007, of 22nd June, on Citizens' Electronic Access to Public Services, under Royal Decree 1671/2009 (articles 17th and 18th) and under Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration.

9. Certificates issued by the FNMT-RCM for electronic signature systems for automated administrative/legal actions whose Specific Certification Policies and Practices are defined herein are considered technically Recognized Certificates, as defined under Law 59/2003 on Electronic Signatures and valid for automated administrative actions as defined under Law 11/2007, of 22nd June, on Citizens' Electronic Access to Public Services, under Royal Decree 1671/2009 (article 19th) and under Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration.

3 DOCUMENT ORGANIZATION

10. The FNMT-RCM's Certification Practices Statement as Certification Services Provider is based, on the one hand, on the common section of the FNMT-RCM's General Certification Practices Statement (DGPC), as there are similar levels of action for all of the Entity's certification services and, on the other, on the specific sections of the relevant Certification Services which, organized in Annexes, comprise the Specific Certification Policies and Practices. Notwithstanding the above, the Issuance Law for each type of Certificate or group of Certificates may establish special characteristics applicable to the bodies, entities and personnel using the FNMT-RCM's certification services.

11. In accordance with the above, the structure of the FNMT-RCM's Certification Practices Statement is as follows:

1) On the one hand, the ***General Certification Practices Statement***, which shall be considered the main text of the *Certification Practices Statement* (sections 1 to 9) which describes, aside from that contemplated in article 19 of Law 59/2003, of 19th December, on Electronic Signatures, the responsibility system applicable to the members of the *Electronic Community*, the security controls applied to the FNMT-RCM procedures and facilities, for all that which may be published without detriment to their efficacy, regulations regarding secrecy and confidentiality, as well as issues related to ownership of its goods and assets, personal data protection and other general information issues to be made available to the public, regardless of their role in the Electronic Community.

2) And, on the other, organized in Annexes for each set or group of *Certificates*, identified and differentiated from the rest for its type and specific or distinguishing system, there is a specific ***Certification Policy*** describing the duties of the Parties, the limitations of use of the *Certificates* and liabilities and ***Specific Certification Practices*** describing the terms defined in the corresponding policy and they grant additional or specific features aside from the general ones established in the ***General Certification Practices Statement***.

12. These Specific Certification Policies and Practices set that formulated in the main text of the General Certification Practices Statement and, therefore, is an integral part of the same, both comprising the FNMT-RCM's Certification Practices Statement. However, these are only applicable for the group of Certificates described and identified in the corresponding Specific Certification Policies and Practices and they include in addition, as abovementioned specific items covered under the Issuance Law of the corresponding Certificate or group of Certificates should there be any specific characteristics or functionalities.

This document therefore comprises the *Specific Certification Policies and Practices* for the *Certificates* issued for:

1) Personnel working for the Public Administration,
2) Identification of electronic venues,
3) Electronic signature systems for automated administrative/legal actions.

4 ORDER OF PREVALENCE

13. The order of prevalence is as follows:

- These *Specific Certification Policies and Practices* for *Certificates* issued by the personnel working for the Spanish Public Administrations, as well as *Certificates* for identification of electronic venues and electronic signature systems for automated administrative/legal actions are a part of the *Certification Practices Statement* and will have prevalence as appropriate and in particular over each type of *Certificate,* over that set out in the main body of this *General Certification Practices Statement*.

  Therefore, in the event of any contradiction between this document and that stipulated in the *General Certification Practices Statement*, that formulated herein shall prevail.

- The *Issuance Law* of each *Certificate* or group of *Certificates* shall represent, as appropriate and given its singularity, a special standard with regard to that established in these *Specific Certification Policies and Practices* for the various public bodies or entities using the services of the FNMT-RCM, when thus required by the nature of their competences or functions. The

Issuance Law, if set up, shall be included in the binding document to be formalized between the FNMT-RCM and the Administrations, public bodies and entities, and/or in the conditions of use or issue contract, and/or in the *Certificate* itself.

- The electronic *Certificates* corresponding to this document and referring to: Personnel working for the Public Administration, identification of electronic venues, Electronic signature systems for automated administrative/legal actions through electronic Seals, the *Issuance Law* (without prejudice to what may be established in the agreements signed with the Subscribers Administrations, bodies and entities in accordance with the corresponding competence system), shall have the following fields, which may be included, totally or partially, in the *Certificate* itself or in the conditions of use document:
  - System for electronic identification of *Signatory* and authentication of electronic documents generated.
  - Scope of use, to match the *Signatory*'s competence system and which shall be universal across all the Public Administrations, bodies and entities.
  - Liability limitation, indicating as appropriate, financial limits for public acts and transactions.
  - Signatory/custodian, which shall be the same as the person in charge of the corresponding *Registry Office* or, as appropriate, the representative of the administrative body exercising these functions.
  - Validity, in the event it is different from the general duration set in this Statement.
  - Validation System. Common Platform.
  - Data Protection and Security Protocol.

5 DEFINITIONS

14. For the purposes contemplated in this document, specifically with regard to the definitions in the General Certification Practices Statement and only when the terms begin with capital letters or in italics, they shall be construed as follows:

- *Applicant*: Individual matching the *Signatory* and custodian of the *Signature Creation Data* and the person working for the Public Administration or dependent body or attached or dependent entity.
- *Applicant Body*: Public Administration or dependent body or attached or dependent entity, which for various reasons cannot create the necessary registry infrastructure for management of registration applications and delegates, totally or partially, processing of these applications to others. The future *Signatory* and custodian of the *Signature Creation Data* belongs to this Body and they shall be the applicant of the corresponding registration operation.
- *Centralized Registry Office*: Delegate Registry Office
- *Delegate Registry Office*: *Registry Office* which for the purposes of conducting registration operations acts before the FNMT-RCM on behalf of an *Applicant Body* within the

framework of the corresponding agreement and without detriment to the duties and responsibilities associated to the registry function and established in the *Certification Practices Statement*.

- *Delegate Body*: Public Administration or dependent body or attached or dependent entity where the *Delegate Registry Office* or *Centralized Registry Office* shall be located, where applications for certificate management from *Applicant Body* shall be processed.

6 LIFECYCLE MANAGEMENT OF THE KEYS OF THE CERTIFICATION SERVICES PROVIDER

15. The FNMT-RCM as Certification Services Provider, with relation to the encryption keys used to issue Certificates for the Certificates issued for the **personnel working for the Public Administration, identification of electronic venues**, electronic signature systems for **automated administrative actions** states they shall undertake the following:

6.1. LIFECYCLE MANAGEMENT OF KEYS

6.1.1. Generation of Keys of the Certification Services Provider

16. The Keys of the FNMT-RCM, as Certification Services Provider, are generated under completely controlled circumstances, in a physically secure environment and, at least, by two people authorized for this, using hardware and software systems that meet current regulations regarding encryption protection, as shown in the General Certification Practices Statement.

6.1.2. Storage, safeguarding and recovery of the Keys of the Certification Services Provider

17. The FNMT-RCM uses the necessary mechanisms to maintain its Key private and confidential and maintain its integrity as shown in the General Certification Practices Statement.

6.1.3. Distribution of Signature Verification Data of Certification Services Provider

18. The FNMT-RCM uses the necessary mechanisms to maintain the integrity and authenticity of its Public Key, as well as its distribution as shown in the General Certification Practices Statement.

19. The fields of the Root Certificate corresponding to the certification hierarchy of the Certificates for the personnel working for the Public Administration are shown in the annex (Table 1).

20. In addition, Certificates issued under the Certification Policies identified in this document are electronically signed with the Signature Creation Data of the Certification Services Provider.

21. For this purpose, the FNMT uses two possible sets of Signature Creation Data, each corresponding to its respective Certificate of Certification Authority (in any case, subordinated to the Root Certificate of the FNMT-RCM previously identified). Both Certificates are defined in the annex to this document (Tables 2 and 3).

6.1.4. Storage, safeguarding and recovery of the Private Keys of the user Administration, public Bodies and Entities

22. Under no circumstance shall the FNMT-RCM generate or store *Private Keys* for its *Signatories*. These shall be generated under their sole control and their custody is the responsibility of the various signatories, bodies and entities to which they are attached or they depend on.

6.1.5. Use of Signature Creation Data of the Certification Services Provider

23. The *Signature Creation Data* of the FNMT-RCM, as *Certification Services Provider*, shall be used solely and exclusively for the purposes of:

    1) Signing *Certificates*.

    2) Signing Lists of Revocation.

    3) Other uses contemplated in this *Statement* and/or applicable legislation.

6.1.6. End of lifecycle of the Keys of the Certification Services Provider

24. The FNMT-RCM shall have the necessary means to ensure that upon termination of the validity period of the *Keys* of the *Certification Services Provider*, these Keys are not used again, either destroying them or storing them properly.

6.1.7. Lifecycle of the encryption hardware used to sign Certificates

25. The FNMT-RCM shall have the necessary means to ensure the encryption hardware used to protect its *Keys* as *Certification Services Provider* is not tampered with in accordance with state-of-the-art technology throughout its lifecycle, and said component shall be located in a physically secure environment from the time it is received until it is destroyed, as appropriate.

7 OPERATION AND MANAGEMENT OF PUBLIC KEY INFRASTRUCTURE; NATIONAL INTEROPERABILITY PLAN AND NATIONAL SECURITY PLAN

7.1. OPERATION AND MANAGEMENT OF PUBLIC KEY INFRASTRUCTURE

26. The operations and procedures carried out to implement the *Certification Policies* described in this document follow the controls required by the standards recognized for this purpose. These actions are described in the "Safety, procedures and personnel controls" and "Technical security controls" sections of the *General Certification Practices Statement* of the FNMT-RCM.

27. For information purposes, it is noted that the FNMT-RCM has an *Information Security Management System* (hereinafter SGSI) for its CERES Department (*Spanish Certification*) with the ultimate objective of maintaining and ensuring information security of the members of the *Electronic Community*, as well as their own, so that the service provided by the FNMT-RCM-CERES meets the reliability levels required by the Market. The SGSI of the FNMT-RCM-CERES is applicable to the information assets defined in the Risk Analysis conducted for all the Areas comprising the Department, including as assets the services provided to the members of the *Electronic Community*.

28. The General Certification Practices Statement clarifies precisely all the aspects related to the following sections of the ETSI TS 101 456 Standard:

    1) Security management

    2) Asset classification and management

3) Personnel security
4) Physical and environmental security
5) Operations management
6) System Access Management
7) Trustworthy Systems Deployment and Maintenance
8) Business continuity management and incident handling
9) CA termination
10) Compliance with Legal Requirements
11) Recording of Information Concerning Qualified Certificates

8 DISSEMINATION OF TERMS AND CONDITIONS

29. The FNMT-RCM is making available to the *Electronic Community* and other interested parties, both this document and the *General Certification Practices Statement* document of the FNMT-RCM detailing:

1) The terms and conditions regulating the use of the Certificates issued by the FNMT-RCM, with relation, as appropriate, to the corresponding Issuance Law.
2) Certification Policy applicable to the Certificates issued by the FNMT-RCM.
3) Limits of use for the Certificates issued under this Certification Policy.
4) Obligations, guarantees and liabilities of the parties involved and issue and use of the Certificates.
5) Time for keeping information collected during the registration process and the events generated in the Certification Services Provider's systems related to management of the lifecycle of the Certificates issued under this Certification Policy.

9 PSEDUDONIMS

30. About the subscribers identification with the certificates issued under the current Certification Policy, FNMT-RCM does not admit pseudonyms use.

10 CERTIFICATES PROFILES

31. All certificates are released complying with this policy in accordance with the X.509 version 3 standard. The Annex II of this document shows out each complete profile certificate.

10.1. NAMING RESTRICTIONS

32. 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.

10.2. USING OF EXTENSION POLICY CONSTRAINS

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

10.3. SYNTAX AND SEMANTICS OF THE POLICY QUALIFIERS

34. The extension certificate Policies includes two fields of Policy Qualifiers:

- CPS Pointer: contains the URL where the *General Certification Practices Declaration* and the *Particular Certification Practices and Policies* applicable to certificates.
- User notice: contains a text that could be displayed in the screen by the user of the certificate during the verification.

10.4. SEMANTIC PROCESSING EXTENSION OF "CERTIFICATE POLICY"

35. 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.

11 RECOGNITION AND AUTHENTICATION OF TRADEMARKS

36. FNMT–RCM does not assume any commitment about the commercial brand use for the release of issued certificates beneath the current Certificate Policy. The use of distinctive signs which rights of use are not property of the owner, is not allowed, so FNMT-RCM is not obliged to previously verified the possession of trademarks and other distinctive signs before the certificate release although they were in public registry.

12 CERTIFICATES ISSUED FOR THE PERSONNEL WORKING FOR THE PUBLIC ADMINISTRATION

12.1. CERTIFICATION POLICY OF CERTIFICATES ISSUED FOR PERSONNEL WORKING FOR THE PUBLIC ADMINISTRATION

12.1.1. Identification

37. This *Certification Policy* of the FNMT-RCM to issue *Certificates* for personnel working for the Public Administration has the following identification:

Name: Certificate Certification Policy for personnel working for the Spanish Public Administration

Reference / OID[1]:

. 1.3.6.1.4.1.5734.3.3.4.4.1

. 1.3.6.1.4.1.5734.3.3.4.4.2

Version: 2.4

Issue Date: 24th June 2016

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

Related DPC: General Certification Practices Statement of the FNMT-RCM

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

12.1.2. Type of Certificate for personnel working for Public Administrations: (civil servants, employees, statutory personnel at their service and authorized personnel, hereinafter personnel working for Public Administrations).

38. The *Certificate* for personnel working for Public Administrations is the electronic certification issued by the FNMT-RCM that links the *Signatory* to *Signature Verification Data* and confirms, jointly:

- the identity of the Signatory and custodian of the *Keys* (personnel working for the Public Administrations that conduct electronic signatures using the *Certificate* on behalf of the acting Administration), personal identification number, position, job and/or authorization status and,
- The *Certificate Subscriber*, the body or entity of the Public Administration, whether it is General, regional, local or institutional, where they exercise their functions, provide services or conduct their activities.

39. This *Certificate* is issued by the FNMT-RCM on behalf of the corresponding Public Administration to which the FNMT-RCM lends any necessary technical, administrative and security services as Certification Services Provider.

40. The *Certificate* for personnel working for the Public Administration is developed by the FNMT-RCM with a specific and ad hoc PKI infrastructure, based on identification and registration actions carried out by the Registry Office network designated by the Certificate Subscriber body or entity. The "*Issuance Laws*" may establish, within the scope of action of the Public Administrations, common Registry Offices for this scope of action with standard effects for any Administrations, public bodies and/or entities.

---

[1] *Note*: The OID or policy identifier is a reference to be included in the *Certificate* in order for users to be able to determine the applicable practices and procedures to issue the *Certificate* in question.

Although this document describes a single policy for this type of *Certificates*, there may be three different references to the same to distinguish and identify specific elements in the *Certificate* format, the *Certificate* profiles, the *Certification Authority* used for issuing it or the relevant issue procedures.

Therefore, the *Certificate Certification Policy and Practices* for personnel working for the Public Administration shall be described singly, identifying any possible special features and associating them to the corresponding OID or references.

41. The *Issuance Law* shall provide, considering the various functionalities of the scope of action of the *Certificates*, elements or fields ordinarily shown in the *Certificate* itself, taking into account the specialized actions of the various public Administrations.

42. It is expressly noted that the *Certificate* issued under this policy, is a different *Certificate* from the one described in the *Certification Practices and Policy Statement* for natural person of the "AC FNMT Usuarios", regardless of the common and matching elements, for, in addition to its personal identity as personnel working for the Public Administrations (civil servants, employees, statutory personnel, professional staff, etc.), it shows the relationship, identification number, link, position or *Certificate Signatory* status with the body or entity of the Public Administration to which they belong and the identity of the Administration itself, either directly in the same *Certificate*, or in the *Issuance Law*.

12.1.3. Community and scope of application

43. This Certification Policy is applicable to issue electronic Certificates with the following characteristics:

a) They are issued by the FNMT-RCM as *Certification Services Provider* in compliance with the criteria established under Law 59/2003, of 19th December, abovementioned and the technical standards EESSI, namely ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified certificates" and ETSI TS 101 862 - "Qualified Certificate Profile". These electronic Certificates are issued only to personnel working for Public Administrations, and thus are not issued to the public.

b) The *Encryption Card* of the FNMT-RCM used as a *Secure Device to create a Signature*, complies with the technical criteria established under Law 59/2003, of 19th December, on Electronic Signatures for said devices. Nonetheless, within the scope of *Certificates* of this *Certification Policy*, there are other devices that work as *Secure Devices to create Signatures* compliant with the legal and technical regulations for such devices.

Certificates issued under this *Certification Policy* are issued for the Public Administrations, under scope of application of Law 11/2007, of 22nd June, on Citizens' Electronic Access to Public Services and of Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration, included in the *Electronic Community*, as defined in the ***Definitions*** section of the *General Certification Practices Statement* of the FNMT-RCM. Within the framework of this *Certification Policy*, the *target Users* are the personnel of the Public Administrations of the Kingdom of Spain, whether a body or entity of the General, Regional or Local Administration of Spain.

c) For the purposes of the *Specific Certification Practices* applicable to the certification and electronic signature services, within the scope of the organization and operation of the State General Administration and the rest of the Public Administrations, as well as attached or dependent bodies and entities, the scope of the Electronic Community definition shall refer, only, to the *Subscribers* and Signatories/custodians of the *Certificates* issued under a specific PKI (Public Key Infrastructure) of the corresponding body entrusted to the FNMT-RCM, to fulfil various public functions pertaining to the position, the civil servant relationship, the public employee functions or status of authorized person with relation to bodies endowed with an *electronic venue* to which these users belong to or relate with.

d) The *Certificates* issued under this *Certification Policy* are considered valid as an integral part of the electronic signature systems and, therefore, adequate for operations between administrations and for communications with citizens under Law 11/2007, of 22nd June, on Citizens' Electronic Access to Public Services and under Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration. In particular, they may be a part of electronic signature systems that comply with and/or are equal to that established under Law 59/2003, of 19th December, on Electronic Signatures and they are adequate to guarantee identification of participants in interactions between the administrations and with citizens and, as appropriate, the authenticity and integrity of the electronic documents, as well as their use to generate a recognized electronic signature.

e) The *Issuance Law* of these *Certificates* may determine, in the absence of any specific regulations, the conditions of use and system of these *Certificates* that shall allow attribution to the Administrations, bodies and entities the various actions conducted by the personnel at their service; all without any legal modifications or variations regarding the actions being carried out by these Public Administrations in traditional formats.

12.1.4. Liability and duties of the Parties

44. The obligations and liabilities expressed in this section are understood without prejudice to the corresponding derivatives of the legislation and rules of application, specifically those applicable to the FNMT-RCM as a provider of certification services and for such a condition established in the articles of law 59/2003, of 19 December, about Electronic Signature and its regulations.

45. For the purposes of this section the following subjects shall be considered Parties:

- The Administrations, bodies, public entities represented through the various competent bodies and which depending on the *Issuance Law* (if any) may be set up as liable *Subscribers*.
- Registry Offices, which, through the personnel designated by the competent Administration, shall be liable for the requirements and conditions related to the *Certificate Signatories* and signatories/custodians.
- The Signatories and custodians of the *Certificate* and its *Keys*, who are the personnel working for the public Administrations, bodies and entities.
- FNMT-RCM, as Certification Services Provider.
- If applicable, the rest of the Electronic Community and Third Parties.

46. The system of rights and obligations of the public Administrations, bodies, entities and the FNMT-RCM is governed by the corresponding agreement regulating certification services. In accordance with these agreements, it shall be possible to establish the *Issuance Law* of these *Certificates*. The *Issuance Law* may also be established with the contents and purpose contemplated in this Statement.

47. In addition to the obligations and liabilities of the Parties listed in this document and in the *General Certification Practices Statement*, the *Certificate Subscriber* Administration and/or person in charge of the *Registry Office* shall be obliged to:

- Not conduct any registrations or process any applications from personnel working for an entity other than the one represented by the *Registry Office*, without detriment to the creation of centralized *Registry Offices* or agreements between administrations to conduct registrations.

- Verify unequivocally the data of the personnel working for the Public Administrations as *Certificate* Users, to act as signatories and custodians of the same, with relation to their identity and status of the position, job, employment or any other data that shows or describes their relationship with the Administration, body or entity which it works for.
- Not use the *Certificate* in case the Signature Creation Data of the Subject may be threatened and / or compromised.
- Apply for revocation or suspension of the *Certificate* of the personnel working for the body represented by the *Registry Office* when any of the data related to the status of the position, job, employment or any other data that shows or describes their relationship as *Certificate* signatory and custodian user with the *Signatory*, or public body or entity where their services are provided, is inaccurate, incorrect, has changed, or must be revoked for security reasons.
- Request to FNMT-RCM, through the *Registry Office*, revocation of the *Certificate* when, directly or through communications with the personnel working for the Public Administrations and custodians of the *Certificate*, the *Certificate* card or format has been lost, or it is assumed to be lost.
- In the event the *Certificate* is in a card, download *Certificate* and its keys directly onto the encryption card provided to its personnel. In any case, no private keys associated to Certificates shall be kept in the *Registry Office* computers, in accordance with the FNMT-RCM guidelines described in the procedure manuals given to the *Registry Offices*, in these *Specific Certification Policies and Practices* and in the *General Certification Practices Statement*.
- Not use the *Certificate* in case the Trust Service Provider has ceased the activity as Certification Authority and it had not occurred subrogation under the Act. In any case, not use the *Certificate* in cases where the Signature Creation Data of the Trust Service Provider (TSP) may be threatened and / or compromised, and this has been communicated by the TSP or, where applicable, the subscriber has been informed of these circumstances.

48. The relationships between the FNMT-RCM with the *Subscriber* and the personnel working for the Public Administrations that shall conduct the electronic signatures with the *Certificate* provided by the abovementioned *Subscriber* shall be primarily determined, for the purposes of the use of the *Certificates*, through a document pertaining to the conditions of use or, if applicable, to the Certificate issue contract, and, secondly, by these *Specific Certification Policies and Practices* and by the *General Certification Practices Statement*, in compliance with the agreements or document on the relationship between the FNMT-RCM and the corresponding Public Administration.

49. Interaction of the *Certificate Subscriber* Public Administration and its personnel with the FNMT-RCM shall always be conducted through the *Registry Office* and its person in charge.

50. In addition to the obligations and liabilities of the Parties listed in the *General Certification Practices Statement*, the personnel working for the Public Administrations, as signatories and custodians of the *Certificate* and its *Keys*, are obliged to:

- Not use the *Certificate* when any of the data related to the position, job, employment or any other is inaccurate or incorrect or does not reflect or describe their relationship with the body or entity they serve; or whenever there are security reasons for this.
- Make proper use of the *Certificate* based on the functions and powers ascribed to the position, job or employment as personnel working for the Public Administrations.

- Inform the *Registry Office* manager of the loss or suspected loss of the *Certificate* card or format they are the user and custodian of, in order to initiate, as the case may be, revocation process.

51. The rest of the *Electronic Community* and Third Parties shall regulate their relationships with the FNMT-RCM through the *General Certification Practices Statement*, and, as the case may be, through these *Specific Certification Policies and Practices*; all of the above without prejudice to that stipulated in the regulations on electronic signatures and any other applicable regulations.

12.1.5. Limits of use of the *Certificates* for personnel working for the Public Administrations

52. The limits of use for this type of *Certificates* are the various functions pertaining to the Subscribers Public Administrations (acting through the personnel at their service as *signatories* and custodians of the *Certificates*), in accordance with their position, employment and, as the case may be, authorization conditions. The FNMT-RCM and the public Administration, bodies and entities may establish in the agreements, through the corresponding relationship document or, as the case may be, in the *Issuance Law* of these *Certificates*, other additional limits.

53. The FNMT-RCM shall have no control on the actions and uses of the *Certificates* by the personnel working for the Public Administrations on their behalf and by the Registry Offices, therefore the FNMT-RCM is exonerated from any liability for said uses, as well as from the consequences and effects that may be derive in claims or, where appropriate, any possible pecuniary liability of other third parties.

54. Regarding the activities of the Registration Office staff, FNMT-RCM shall be subject of obligations and responsibilities contained in Law 59/2003, December 19, about electronic signature, without prejudice of the specialties in the article 11 of RD 1317/2001, November 30, by which the article 81 Law 66/1997, December 30, about Financial measures, administrative and social order in security service provision of Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, in the communications throughout electronic, computer and telematic means with Public Administrations. In order to be able to use the *Certificates* for the personnel working for the Public Administration diligently, one must first belong to the Electronic Community and, the acting Administration must obtain *Subscriber* status.

55. In any case, if a Third Party wishes to trust the electronic signature made with one of these *Certificates* without accessing the services for verification of the validity of the *Certificates* issued under this *Certification Policy*, no coverage from these *Specific Certification Policies and Practices* shall be obtained, and they shall not be entitled to claim or initiate legal actions against the FNMT-RCM for damages or conflicts derived from the use or trustworthiness of a *Certificate*.

56. Furthermore, even within the *Electronic Community*, this type of *Certificates* may not be used, by any individual or entity other than the FNMT-RCM, to:

- Sign another *Certificate*, except in the cases expressly authorized in advance.
- Private use, except in interaction with such Administrations that may consent it.
- Sign software or components.
- Generate time stamps for *electronic dating* procedures.

- Provide services against payment or free of charge, except in the cases expressly authorized in advance, such as for example:
    - Provide *OCSP* services.
    - Generate Lists of Revocation.
    - Provide notification services.

12.2. SPECIFIC CERTIFICATION PRACTICES FOR CERTIFICATES ISSUED FOR PERSONNEL WORKING FOR THE PUBLIC ADMINISTRATION

57. The FNMT-RCM as *Certification Services Provider* and to prove the necessary reliability for providing said services, has developed a *Certification Practices Statement* with the purpose of providing public information on the general conditions for the provision of certification services by the FNMT-RCM as *Certification Services Provider*.

58. Of special note, in order to interpret in this Annex the "Definitions" section of the *General Certification Practices Statement*.

59. This Document is derived from and is an integral part of the *Certification Practices Statement* of the FNMT-RCM and defines all of the specific practices followed by the FNMT-RCM as *Certification Services Provider* to manage the lifecycle of the *Certificates* for the personnel working for the Public Administration, issued under the Certificate Certification Policy for personnel working for the Public Administration identified with OIDs 1.3.6.1.4.1.5734.3.3.4.4.1 or 1.3.6.1.4.1.5734.3.3.4.4.2.

12.2.1. Key Management Services

60. The FNMT-RCM shall not under any circumstance, generate or store *Private Signatory Keys*, which are generated under their exclusive control and with the intervention of the corresponding *Registry Office* and whose custody is the responsibility of the personnel working for the Public Administration. Thus, FNMT-RCM does not do key scrow. The applications only allow RSA key generation with size 2048 bits, both Electronic certificates generated with OID 1.3.6.1.4.1.5734.3.3.4.4.1 (in cryptographic card), as those generated with OID 1.3.6.1.4.1.5734.3.3.4.4.2 (software).

12.2.2. Preparation of Secure Signature Creation Devices

61. For *Certificates* generated with OID 1.3.6.1.4.1.5734.3.3.4.4.1 a *Secure Signature Creation Device* shall be used to generate keys and then make an *Electronic Signature*.

62. 63. In these cases, the FNMT-RCM shall provide the *Subscriber* Public Administrations for delivery to the personnel reporting to them, *Encryption Cards* to generate their *Private Keys* and store the *Certificates*.

63. The *Encryption Card* shall be delivered to *Users* and *Subscriber* Public Administrations with no content whatsoever; with the necessary software utilities to achieve integration with the most frequently used Browsers. At the same time, the necessary codes shall be provided to access said card and in order to be able to, subsequently, from the workstation or from the *Registry Office* itself, generate their *Keys* and insert the *Certificate* in the *Encryption Card*.

64. The FNMT-RCM provides this type of cards as it allows *Signatories* to have "exclusive control" on the *Signature Creation Data*.

12.2.3. *Certificate* Lifecycle Management

65. Herein is a definition of the aspects which although already pointed out in the *General Certification Practices Statement* which this document is a part of, contain certain special features which require greater details.

12.2.3.1. Certificate application procedure for personnel working for the Public Administration

66. Below is a description of the application procedure whereby the *Registry Office* collects the data of the personnel working for the Public Administration, confirms their identity, validity in their position or job and formalizes, before the abovementioned personnel and the Administration, public bodies or entities where the personnel provide their services , the document on the conditions of use or the issue contract, as appropriate according to the personnel position, as contemplated in the relationship document or agreement between the FNMT-RCM and the body and/or entity for the subsequent issue of a *Certificate* for the personnel working for the Public Administration.

67. It should be noted that the FNMT-RCM, according to the list of users amongst the personnel dependent on the Administration, public bodies or entities, shall consider, under the responsibility of the corresponding bodies and/or entities, acting through the *Registry Offices*, that the position of said personnel is still valid, that their Personal Identification number, job or authorization is authentic and in effect and, therefore, are empowered to obtain and use the *Certificate*. FNMT-RCM shall not be responsible, with this type of *Certificate*, for verifying the position or job of the abovementioned personnel, and these requirements shall remain throughout the lifecycle of the *Certificate*, since the FNMT-RCM has no legal, civil servant, administrative or employment relationship with said personnel aside from the document on the conditions of use or, as the case may be, the issue contract, whose effect is strictly an instrument to perform the functions pertaining to the position.

68. The above verification activities shall be carried out by the people in charge of the *Registry Offices* implemented by the body or entity of the Public Administration in question and which corresponds, in each case, to the body or entity where the personnel provide their services. Therefore and for these purposes, the *Registry Offices* shall not be delegate authorities or dependent on the FNMT-RCM.

69. The actions shall be the following, once the *Registry Office* has satisfactorily completed the above:

1) Obtain Encryption Card and software to generate or import the *Signature Creation and Verification Data* on the Card[2]

The *Encryption Card* is the *Secure Signature*[3] *Creation Device* that must be used to generate *Signature*[4] *Creation and Verification Data* or, as the case may be, import the corresponding *Certificate* and make electronic signatures.

[2] This step shall only be necessary if the *Certificate* issue is in accordance with OID 1.3.6.1.4.1.5734.3.3.4.4.1

The *Subscriber* shall, prior to the pre-application phase, obtain the above *Card* through the corresponding *Registry Office*. In addition to the *Encryption Card*, the *Subscriber* Public Administration shall obtain the necessary software to generate the *Keys* with the same *Card* or, as appropriate, to import the corresponding *Certificate*.

For the procedure to obtain the *Certificates*, the FNMT-RCM shall provide the necessary elements to enable, at the *Registry Office*, the pertinent software to generate the encryption *Keys* that allow protecting the security of their communications through encrypted mechanisms, as well as to authenticate themselves and sign electronically in accordance with Law 11/2007, of 22nd June, and with Law 18/2011, of 5th July, , being set up in the latter case as *Signature Creation and Verification Data*.

It should be noted that, for the necessary elements to enable the *Certificate*, the FNMT-RCM shall purchase them from the market seeking the maximum diversity of providers possible. The FNMT-RCM shall demand from the providers the necessary eligibility and industrial and intellectual property guarantees, as well as any other relevant ones for computer security. Notwithstanding the above, FNMT-RCM shall not be liable for any damages and/or faulty operation of these elements that may occur during their use, whether due to the interested users or due to any original defects of the elements, and the FNMT-RCM shall merely forward any claims or complaints to the various providers.

The *Signature Creation Data* in the *Encryption Card* shall always remain under the exclusive control of the *Signatory* and the personnel working for the Public Administration as user and custodian of such *Certificates*, and no copy of the same shall be kept by the FNMT-RCM, or by the *Registry Office*.

FNMT-RCM sall manufacture these cards for greater security during the process, either directly or through the collaborating entities. FNMT-RCM shall issue *Certificates* for *Encryption Cards* that have been duly approved as *Secure Signature Creation Devices* by the corresponding bodies and/or that are technically suitable to store the *Certificates* issued by the Entity.

Once this format and the necessary software have been obtained for the operation to be carried out, the interested party shall proceed as follows.

2) Pre-application

Interested Party is to go to the *Registry Office* in person or from the workstation where they perform their functions[45], provided this has been authorized by the *Registry Office*, and access the *website* of the *Certification Services Provider*, of the FNMT-RCM electronic office, through the address

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

---

[3] In this context, it is assumed that all cryptographic cards can be considered a Secure Device of Signature Creation since it meets the requirements set out in annex III of the Directive 1999/93/EC of the European Parliament. However, under the provisions of law 59/2003 only will reach such a condition for legal and practical purposes, those which are subject to a certification procedure under the technical standards whose reference numbers have been published in the "Official Journal of the European Union" and, exceptionally, approved by the Ministry of Science and Technology which will be published on the website of this Ministry.

[4] For Certificates issued under OID 1.3.6.1.4.1.5734.3.3.4.4.2, this operation **shall always** be carried out from the workstation where the interested parties perform their functions

where full instructions for the procedure are shown. You must enter your NIF o NIE (Tax Identification Number), at the relevant data entry point; and/or the civil servant or employment identification number. *Public* and *Private Keys* shall be generated (in *Encryption Card* if the *Certificate* is issued with OID 1.3.6.1.4.1.5734.3.3.4.4.1) which shall be linked to the *Certificate*, becoming signature verification and creation data respectively. Then, the Public Key generated and the supporting evidence of possessing the private key, are sent in a standard format (PKCS # 10 or SPKAC) to the FNMT-RCM using a secure channel. The FNMT-RCM links an unique request code to this pre- application, which is shown to the *Applicant*.

Previously, the personnel working for the Public Administration and the public body or entity shall consult the *General Certification Practices Statement*, and these *Specific Certification Policies and Practices* at:

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

with the conditions of use and obligation as Signatory and *Subscriber*, respectively, of the *Certificate*, to be included in the document of conditions of use or, as the case may be, the issue contract.

The FNMT-RCM, once the *Registry Office* have conducted all relevant checks, shall verifythe information in the signed pre-application and verifying only the possession and matching of the pair of encryption *Keys* by the applicant.

This information shall not generate a *Certificate* by the FNMT-RCM, until the latter receives the Certificate application completed by the *Subscriber* Administration signed by the *Registry Office*.

If the keys are generated inside the *Encryption Card*, the pre-application operation can be carried out at the corresponding *Registry Office*, without compromising at any time the confidentiality and exclusive control, by the *Signatory*, of the *Private Key*.

3) Confirmation of personnel identity, position or job

12.2.3.2. Appearance in person at Registry Offices

70. Appearance in person shall take place at the *Registry Office* designated for this purpose by the *Subscriber* public body or entity the personnel report to. This *Registry Office* is created by the *Subscriber* Administration, which notifies to the FNMT-RCM the relationship of persons authorized to perform such activities, in accordance with the procedures established for this purpose, and any variation in the structure of the Office.

71. For this purpose, the FNMT-RCM shall consider the functionalities contemplated by applicable legislation related to the DNIe (*Electronic National Identity Card*), as well as the systems for identification and verification of position, function or job applicable to Public Administrations, therefore the requirement to appear in person may be substituted by other procedures that allow identification, always provided they are covered by the intervention of the *Registry Office*. In these cases of special identification procedures specific to the public setting, appearance in person shall not be necessary when the competent body of the Administration certifies the requirements for identity, position validity and all other conditions to be communicated to the *Registry Office*, in accordance with that established in article 13.1 *in fine* of Law 59/2003 on Electronic Signatures and article 19 of Law 11/2007, and in article 21st of Law 18/2011.

12.2.3.3. Appearance and documentation

72. In the event the action entails appearance before the *Registry Office*, the personnel working for the Public Administration shall submit all the data requested, proving their personal identity and status as personnel working for the Public Administration, without detriment to application of that in the above paragraph. FNMT-RCM shall in any case accept the function and report conducted by the *Registry Office* designated by the Administration.

1. Submission of information to the FNMT-RCM

Once the *Registry Office* has confirmed *Applicant* identity, validity of position or job and subscribed the document of conditions of use or, as the case may be, the application contract of the above *Applicant* and the *Registry Office*, it shall proceed to validate the data and send them, together with the application code obtained in the pre-application phase. The FNMT-RCM shall collect from the *Applicants* only that information, received from the *Registry Office*, which is necessary to issue *Certificates* and for verification of identity, storing the information required by electronic signature legislation for a period of fifteen (15) years, treating it with due diligence in order to comply with applicable national legislation regarding personal data protection.

All processing of personal data shall be subject to applicable legislation.

Submission of information to the FNMT-RCM shall be conducted through secure communications established for this purpose between the *Registry Office* and the FNMT-RCM.

2. Extension of the registration and identification function to other *Certificates* issued by the FNMT-RCM.

Members of the *Electronic Community* may receive certification and electronic signature services from the FNMT-RCM, based on issuing electronic *Certificates* belonging to various *Issuance Laws* and in different formats, by acceptance of the conditions that shall be specifically presented at the request of the FNMT-RCM in the various websites and other service formats of the members of the *Electronic Community*, in accordance with that established by the corresponding sector legislation and the limitations established by the legislation regulating processing of personal data.

During provision of the services described in the above paragraph, the actions derived from registration and identification may be extended, with the time limitations contemplated in the electronic signature legislation, as well as regulations on the DNI-e, all without detriment to the special features that may apply to Public Administrations.

12.2.3.4. Issue of Certificate for personnel working for the Public Administrations

73. Once the FNMT-RCM receives the personal data of the Applicant, the information describing their relationship with the Public Administration, as well as the application code obtained in the pre-application phase, the *Certificate* shall be issued.

74. Issue of the *Certificates* entails generating electronic documents confirming personnel identity, their relationship, position or job with the Public Administration as well as their correspondence with the

associated *Public Key*. FNMT-RCM *Certificates* can only be issued by the former, as *Certification Services Provider*, and there is no other entity or body authorized to issue them. The FNMT-RCM Certification Authority only accepts certificate requests for issuance from authorized sources. In order to prevent forgery, all data contained in each request are protected by electronic signature mechanisms which are performed by using certificates issued to these authorized sources.

75. The FNMT-RCM, through its *Electronic Signature*, authenticates the *Certificates* and confirms the identity of the *Signatory*, as well as validity of the position or job of their personnel, in accordance with the information received by the *Registry Office*. On the other hand, and in order to prevent tampering of information included in the *Certificates*, the FNMT-RCM shall use encryption mechanisms that confirm the authenticity and integrity of the *Certificate*.

76. The FNMT-RCM shall in no case include in a *Certificate* information other than the one shown here, or circumstances or specific attributes of the signatories or limits other than those contemplated in the agreements and, as the case may be, those contemplated in the corresponding *Issuance Law*.

77. In any case, the FNMT-RCM shall efficiently:

- Check that the *Registry Office* or, as the case may be, the signatory personnel and custodians of the *Certificate* use the *Private Key* corresponding to the *Public Key* linked to the identity of its *Signatory*. For this purpose, the FNMT-RCM shall check that the *Private Key* and the *Public Key* match.
- Ensure that the information included in the *Certificate* is based on the information provided by the corresponding *Registry Office*.
- Not ignore evident facts that may affect the reliability of the *Certificate*.
- Ensure that the *DN* (Distinguished Name) assigned in the *Certificate* is unique in the whole *Public Key Infrastructure* of the FNMT-RCM.

78. To issue the *Certificate* the following steps shall be taken:

1. Composition of the Certificate Distinguished Name (DN) for personnel working for the Public Administration.

With the personal details of the above personnel collected during the *Certificate* application procedure, the Distinguished Name (*DN*) is made up in accordance with standard X.500, ensuring said name makes sense and is not ambiguous. Pseudonyms may not be used for identification.

The *DN* for the personnel working for the Public Administration shall be made up of the following elements:

DN=CN, OU, OU, OU, O, C

The attribute *CN* contains the identification data of the personnel working for the Public Administration.

2. Composition of the alternative identity of the Certificate.

The alternative identity of the personnel working for the Public Administration Certificate, as contemplated for this type of *Certificates* contains the same information as the *CN*, as well as the position, public body or entity where services are provided, which is the *Certificate Subscriber*, job and identification number, distributed in a series of attributes, in order to facilitate gathering of personal data of the personnel

working for the Public Administration. The subjectAltName extension defined in X.509 version 3 shall be used to obtain this information.

As part of this extension, the subfield directoryName shall be used to include a set of attributes defined by the FNMT-RCM, which shall include information on the personnel working for the Public Administration and the *Subscriber* Administration in question.

3. Generation of the *Certificate* in accordance with the Certificate Profile of the personnel working for the Public Administration.

The format of the *Certificate* for the personnel working for the Public Administration, issued by the FNMT-RCM under the *Certificate Certification Policy* for the personnel working for the Public Administration, by the FNMT-RCM, in line with standard UIT-T X.509 version 3 and in accordance with legally applicable regulations regarding *Recognized Certificates*, may be consulted in the annexes to this document.

They describe the *Certificates* distinguishing between the issuing *Certification Authority* (always subject to the *Root Certification Authority* of the FNMT-RCM), as well as the *Certificate* support.

In addition, as the case may be, the necessary extensions shall be included to be able to conduct the "login" process to the Windows Operating System with the Encryption Card:

Extension Name: extKeyUsage

Values: Client Authentication: 1.3.6.1.5.5.7.3.2

Smart Card Session Start: 1.3.6.1.4.1.311.20.2.2

12.2.3.5. Information about the released of the Certificate for personnel working for the Public Administration

79. If during the application process the personnel working for the Public Administration provided an e-mail address, they shall be sent a message indicating their *Certificate* is available for downloading.

12.2.3.6. Downloading and installation of Certificate of personnel working for the Public Administration

80. Not later than 24 hours since the personnel working for the Public Administration appear in person at the *Registry Office* to their identity is proved, validity of their position or job, and once the *Certificate* has been generated, a mechanism to download the *Certificate* is made available to them or to the *Registry Office* at:

https://registro20.cert.fnmt.es/AplicacionRegistroWEB/pages/frameset1.html by accessing the option "Download your Certificate".

81. During this guided process the personnel working for the Public Administration or the person in charge of the *Registry Office* shall be asked to enter the NIF or NIE with which the pre-application process was carried out, as well as the unique request code provided by the system at the end of said process. If the *Certificate* has not been generated yet for whatever reason, this shall be communicated when downloading is attempted.

82. If the *Certificate* has already been made available to the personnel working for the Public Administration or the *Registry Office*, it shall be entered in the format in which the *Keys* were generated during the Pre-Application process.

12.2.3.7. Validity of the Certificate of the personnel working for the Public Administration

12.2.3.7.1. Expiration

83. The *Certificates* of the personnel working for the Public Administration issued by the FNMT-RCM shall be valid for a period of three (3) years from the time the *Certificate* is issued, provided its validity is not terminated. After this period and if the *Certificate* is still active, it shall expire and whenever the Subscriber wishes to continue using the services of the Certification Services Provider it shall be necessary to issue a new one.

12.2.3.7.2. Termination of validity

84. The *Certificates* of the personnel working for the Public Administration issued by the FNMT-RCM shall become null in the following cases:

a) Termination of the *Certificate* validity period

b) End of activity as *Certification Services Provider* by the FNMT-RCM, unless, with the prior express consent from the *Signatory* the *Certificates* issued by the FNMT-RCM have been transferred to another *Certification Services Provider*.

In these two cases [a) and b)], the *Certificate* shall stop being effective the moment these circumstances occur.

c) Suspension or revocation of the *Certificate* for any of the reasons contemplated in this document

85. For the purposes listed above, it is noted that application for the issuance of a *Certificate* for personnel working for the Public Administration issued by the FNMT-RCM when there is another one in effect for the same *Signatory* and belonging to the same *Issuance Law* shall entail revocation of the first one obtained.

86. The effects of revocation or suspension of the *Certificate*, that is, termination of its validity, shall come into effect the moment the FNMT-RCM becomes aware of any of the circumstances causing the termination and it shall be duly noted in its *Information and Inquiry Service on the Status of Certificates*.

12.2.3.8. Revocation of the Certificate of personnel working for the Public Administration

12.2.3.8.1. Causes for revocation

87. The causes accepted for revocation of a *Certificate* are those described below, additionally taking into account what is included in the "*Certificate* Validity Termination" section regarding application for a

Certificate when there is another one in effect for the same *Signatory* and the same personnel and belonging to the same *Issuance Law*.

88. The *Issuance Law* may, in addition, establish other causes for revocation, suspension and cancellation of the suspension.

89. The FNMT-RCM shall only be responsible for the consequences derived from not having revoked a *Certificate* under the following circumstances:

- When revocation should have been made due to termination of the contract subscribed with the Subscriber
- When revocation has been requested by the corresponding *Registry Office* to the *Subscriber* entity or body following the procedure for this type of *Certificates*
- When the revocation request or cause for the same, has been notified by a judicial or administrative ruling.
- When the causes c) to f) in this section have been duly proven, after identification of revocation *Applicant*.

90. Taking into account the above, causes for revocation of a *Certificate* of personnel working for the Public Administration are:

a) Request for revocation by the authorized parties. In any case, this request shall be prompted by:

- Loss of the Certificate format.
- Use by a third party of the *Signature Creation Data* corresponding to the *Signature Verification Data* included in the *Certificate* and linked to the *Signatory*'s personal identity.
- Breach or jeopardizing of confidentiality of the *Signature Creation Data*.
- Non-acceptance of any new conditions that may require issuance of new *Certification Practices Statements*, within a month following their publication.

b) Judicial or administrative ruling requiring so.

c) Termination or dissolution of the legal entity status of the *Subscriber*.

d) Termination of the contractual relationship of the *Signatory* to the administrative body *Subscriber* of the *Certificate*.

e) Total or partial unforeseen disability of *Signatory*.

f) Inaccuracies in the data provided by the *Applicant* to obtain the *Certificate*, or alteration of data provided to obtain the *Certificate* or modification of the circumstances verified to issue the *Certificate*, such as those related to the position or power of representation, so that these are no longer in force.

g) Violation of a substantial obligation of this *Certification Practices Statement* by the *Subscriber*, *Certificate Applicant* or a *Registry Office* if, in the latter case, it may have affected the procedure to issue the *Certificate*.

h) Termination of the contract entered into by and between the *Subscriber* and the FNMT-RCM.

i) Violation or jeopardising of confidentiality of the *Signature Creation Data.*

91. In no case shall it be construed that the FNMT-RCM assumes any obligation whatsoever to verify the points described in letters c) to f) in this section.

92. Any crime or offense which the FNMT-RCM is not aware of carried out with relation to the data and/or *Certificate*, inaccuracies regarding the data or lack of diligence in their communication to the FNMT-RCM, shall exonerate the FNMT-RCM from any liability.

12.2.3.8.2. Effects of the revocation

93. The effects of the revocation or suspension of the *Certificate*, that is, termination of its validity, shall come into force on the date the FNMT-RCM becomes aware and confirms any of the determining circumstances and they state as much in their *Information and Inquiry Service on the Status of Certificates*.

94. The revocation of *Certificates* implies, aside from their termination, cancellation of the relationship and the system of use of the *Certificate* with the FNMT-RCM.

12.2.3.8.3. Procedure for revocation

95. The request for revocation of the *Certificates* of personnel working for the Public Administration may be carried out during the validity period indicated in the *Certificate*.

96. Revocation of a *Certificate* for personnel working for the Public Administration, may be requested by the *Subscriber* through of the corresponding *Registry Office* or by the *Signatory*, either through the *Registry Office*, either through the telephone prepared for that purpose (prior identification of the Applicant) whose number is made public on the website of the FNMT - RCM and will be operational on schedule 24x7. In this case the Applicant must report, among other data, the unique request code received in the pre-application proccess, in order to verify his/her identity.

97. Nonetheless, the FNMT-RCM may revoke the *Certificates* for personnel working for the Public Administration in the cases listed in the *Certification Practices Statement*.

98. Below is a description of the procedure to be followed by the *Registry Office* to formalize the request for revocation of a *Certificate*.

99. In any case, the FNMT-RCM shall receive from the Administration, bodies and/or entity, all relevant information regarding the effects of the revocation of a *Certificate*, through the *Certificate* revocation request form it is submitted, either on paper or electronically, by the Registry Office.

100. The *Registry Office* shall forward the processed registrations to the FNMT-RCM in order for the latter to revoke the *Certificate*. All personal data processing shall be subject to applicable legislation.

101. Likewise the FNMT-RCM shall consider that the person requesting revocation of a *Certificate* of this type shall have the corresponding authorization if the request is conducted through the corresponding *Registry Office*. The FNMT-RCM shall not assess the appropriateness of the revocation requested whenever it is conducted through the abovementioned *Registry Office*. As soon as the revocation is done, the *Signatory* will receive, through the e-mail address provided on the application, notification of Certificate's revocation.

102. Once the FNMT-RCM has revoked the *Certificate*, the corresponding *List of Revoked Certificates* shall be published in the secure *Directory* with the serial number of the revoked *Certificate*, and the date, time and cause for the revocation. Once a certificate is definitively revoked, it shall not be reinstated.

103. This service will be operational on schedule 24x7. The maximum delay between the receipt of revocation request and publishing of the revocation information on the *Information and Inquiry Service on the Status of Certificates* will be 24 hours.

12.2.3.9. Suspension of Certificate for personnel working for the Public Administration

104. Suspension of a *Certificate* leaves the Certificate without effect for the period and under the conditions set.

105. Suspension of a *Certificate* shall be considered a temporary revocation of *Certificate* validity therefore the procedures and entities empowered to request and process *Certificate* shall apply in the event of suspension.

12.2.3.9.1. Causes for suspension of the Certificate

106. The FNMT-RCM may suspend validity of *Certificates* upon request from the legitimate interested party or Legal Authority or if there is ground to suspect the existence of validity termination causes for the *Certificates* as contemplated in the "Causes for Revocation of Certificates for personnel working for the Public Administration" section.

107. Likewise, the request for suspension may be due to an ongoing investigation or legal or administrative procedure, whose conclusion may determine that the *Certificate* is indeed affected by a cause for revocation. In these cases the FNMT-RCM, at the request of the legitimate interested party, shall suspend the validity of the *Certificate* for the period requested and, after said period, shall revoke the *Certificate* unless the FNMT-RCM is unequivocally asked by the legitimate interested party to reactivate it.

12.2.3.9.2. Effects of suspension

108. Suspension of a *Certificate* leaves the *Certificate* without effect (terminating its validity) for a period of time and conditions set.

12.2.3.9.3. Procedure for suspension of Certificates

109. Suspension of *Certificates* may only be carried out through the corresponding *Registry Office*, at the request of the *Signatory* or the *Subscriber* of the *Certificate*.

110. The FNMT-RCM shall suspend the *Certificate* provisionally for a period of thirty (30) days, after which the *Certificate* shall terminate through direct revocation by the *Certification Services Provider* of FNMT-RCM, unless the suspension has been withdrawn. Notwithstanding the above, the period contemplated for suspension of the Certificate may change according to any legal or administrative proceedings that may affect it.

111. If during the *Certificate* suspension period it should expire or its revocation were requested, the same consequences shall apply as for non-suspended *Certificates* affected by expiry or revocation causes.

112. The *Registry Office* of the area corresponding to the public *Subscriber* body or entity will collect the suspension contract of the *Certificate* signed by the Applicant.

The *Registry Offices* shall forward the processed registrations to the FNMT-RCM in order for the latter to suspend the *Certificate*. Processing of all personal data shall be subject to applicable legislation.

Once the FNMT-RCM has suspended the *Certificate*, the corresponding *List of Revocation* shall be published in the secure *Directory* with the serial number of the suspended *Certificate*, and the date and time of suspension and as cause for revocation: "suspension".

In all the above situations of these *Specific Certification Practices* requiring identification and whenever electronic identification is possible, the FNMT-RCM shall consider the functionalities contemplated for the DNI-e, in accordance with applicable legislation and the use of another *Certificate* issued by the FNMT-RCM or recognized by them.

12.2.3.10. Cancellation of suspension of Certificate *for personnel working for the Public Administration*

113. Cancellation of suspension of *Certificates* issued by the FNMT-RCM may be requested by the person in charge or manager of the *Registry Office* of the *Signatory*'s area provided said request is conducted within thirty (30) days from the suspension. In this case, the *Registry Office* shall provide all data required and shall certify identity of its personnel whose identity is included in the *Certificate,* following the procedure described above to request issue of the *Certificate* for personnel working for the Public Administration. FNMT-RCM shall accept any validation report issued by the *Registry Office* as established in article 13.1, *in fine*, of the Law on Electronic Signatures.

The personal data of the personnel working for the Public Administration and the Public Administration *Subscriber*, once validated by the *Registry Office*, shall be sent to the FNMT-RCM through secure communications established for this purpose between the *Registry Office* and the FNMT-RCM. Processing of all personal data shall be subject to applicable legislation.

Once data validated by the *Registry Office* regarding withdrawal of suspension have been received, the FNMT-RCM shall proceed to withdraw the *Certificate* from the *List of Revocations*, and no technical action on the *Certificate* in question shall be conducted.

114. As in previous cases for identification purposes, the functionalities contemplated for the DNI-e shall be considered, in accordance with applicable legislation and others applicable to Public Administrations.

12.2.3.11. Certificate renewal of staff serving to Public Administration

115. The renewal of the certificate of staff serving to Public Administration is performed by emitting new keys, so the process is the same as the obtention of a new certificate.

12.2.3.12. Verification of status of Certificate for personnel working for the Administration

116. The *Certificate Subscriber* and the user Administrations, bodies and entities belonging to the *Electronic Community* may check status of a *Certificate* in the manner and under the conditions described in this section.

117. The status of the *Certificate* for personnel working for the Administration may be verified either by accessing the *Lists of Revocation*, or through the *Information and Inquiry Service on the Status of Certificates* through OCSP.

118. These services shall be available twenty-four (24) hours a day, every day of the year, except for circumstances beyond the control of FNMT-RCM or for maintenance operations. The FNMT-RCM shall notify of this situation at http://www.ceres.fnmt.es if possible at least forty-eight (48) hours in advance and shall try to resolve it within a maximum of twenty-four (24) hours.

119. The FNMT-RCM has an OCSP responder service to provide the *Information and Inquiry Service on the Status of Certificates* under the terms subscribed in the corresponding agreement, contract or *Issuance Law*.

120. The service works as follows: The OCSP server receives the OCSP request made by an OCSP Client registered in the system and it checks status of the *Certificates* included in it. If the request is valid, an OCSP response shall be issued informing on the current status of the *Certificates* included in the request. This OCSP response is signed with the *Signature Creation Data* of the FNMT-RCM to ensure its authenticity and integrity.

121. It shall be the *user Entity*'s responsibility to obtain an *OCSP Client* to operate with the OCSP server made available by the FNMT-RCM.

122. It is the *user Entity*'s responsibility applying for the OCSP service to obtain, as the case may be, consent from *Certificate Subscriber* for which OCSP service is being requested, as well as inform this of the corresponding conditions and limitations.

123. The above is understood with the scope and limits of legislation on automated processing of personal data and in accordance with the corresponding contracts, agreements or Issuance Laws regulating the electronic certification service of the FNMT-RCM.

124. The FNMT-RCM shall not provide an *Information and Inquiry Service on the Status of Certificates* of other *Subscribers* unless established as such in agreements and/or contracts with the corresponding consent from the members of the *Electronic Community* or under the terms contemplated in the *Issuance Law*.

12.2.4. Exclusions and additional requirements to ETSI TS 101 456

125. As these electronic Certificates are not issued to the public, shall be taken into account exclusions and additional ETSI TS 101 456 requirements, such as:

- In accordance with the standard in section 8.2 b), the points defined in section 7.5 h), i) are excluded.
- In accordance with the standard in section 8.2 d), the points defined in section 7.3.6 k) are excluded. In this regard, that contained in the "Verification of *Certificate* Status" section of this annex shall apply.

126. With regard to those *Recognized Certificates* using *Secure Signature Creation Devices*, that contained in the "Certificate Format" section of the *General Certification Practices Statement* of the FNMT-RCM shall apply, as well as that contained in the sections on "Certificate Lifecycle" in said document.

12.2.5. Maximum period time for remediation of system failure

127. The maximum period for remediation of system failure regarding to the services that FNMT-RCM provides twenty-four (24) hours a day, every day of the year, is twenty-four (24) hours, except for maintenance operations. The FNMT-RCM shall notify of this situation at http://www.ceres.fnmt.es if possible at least forty-eight (48) hours in advance.

13 CERTIFICATES ISSUED FOR IDENTIFICATION OF ELECTRONIC VENUES OF THE PUBLIC ADMINISTRATION, BODIES AND ATTACHED OR DEPENDENT PUBLIC ENTITIES

13.1. CERTIFICATION POLICY FOR CERTIFICATES ISSUED FOR IDENTIFICATION OF ELECTRONIC VENUES OF THE PUBLIC ADMINISTRATION, BODIES AND ATTACHED OR DEPENDENT PUBLIC ENTITIES

13.1.1. Identification

128. The electronic venues in the scope of action of Public Administrations are electronic addresses available to citizens. Establishing an electronic venue entails the responsibility of the Administration or acting body with regard to the integrity, truthfulness and update of the information and services that may be accessed. The conditions of official publicity of the electronic venues, as well as the principles applicable to the electronic venue shall be the responsibility of *Subscriber* Administration of the same. The FNMT-RCM shall only provide the necessary security and electronic certification services to meet the needs of each Administration.

129. This *Specific Certification Policy* of the FNMT-RCM to issue *Certificates* for identification of electronic venues of the Public Administration, bodies and attached or dependent public entities bears the following identification:

Name: *Certificate Certification Policy* for identification of electronic venues of the Public Administration, bodies and attached or dependent public entities

Reference / OID[5]:

- 1.3.6.1.4.1.5734.3.3.2.2.

Version: 2.4

Issue Date: 24th June 2016

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

Related DPC: General Certification Practices Statement of the FNMT-RCM

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

[5] *Note*: The OID or policy identifier is a reference to be included in the Certificate in order for users to be able to determine applicable practices and procedures to issue the Certificate in question.

Although this document describes a single policy for this type of Certificates, there may be two different references to distinguish or identify specific features in the Certificate profiles, Certification Authority used for issue or issue procedures.

Therefore, the Certificate Certification Policy and Practices for identification of venues shall be described singly, identifying any possible specific features and associating them to the corresponding OID or references.

13.1.2. Type of *Certificate* for identification of electronic venues of the Public Administration, bodies and attached or dependent public entities

130. The "*Certificates* for *electronic venue* identification", in accordance with the definition of an *electronic venue* in Law 11/2007, LAECSP are those *Certificates* issued by the FNMT-RCM under this certification policy and which link *Signature Verification Data* to the identification data of an *electronic venue* where there is an *individual* acting as signatory or custodian of the key and the *Certificate Subscriber* which is the administration, public body or entity which it belongs to and which is the holder of the electronic address and domain which provides access to the *electronic venue*. This *individual* has control over said *Certificate* and the *Signature Creation and Verification Data* and is responsible for their diligent custody.

131. The person in charge of the *Registry Office* shall be the signatory, custodian and, therefore, in control of the key and of the *electronic venue Certificate*.

132. Therefore, the Private Key associated to the Public Key and the Signature Creation and Verification Data are the responsibility of said signatory or custodian, who shall act as representative of the Public Administration entity (Legal Entity) and is in charge of management and administration of the corresponding electronic address.

133. The FNMT-RCM shall issue these *Certificates* whenever requested to do so by the *Electronic Community* subject to Law 11/2007 and to Law 18/2011, for the various relationships that may be established under the scope of the *electronic venue* and whose use is not forbidden or limited by applicable legislation.

134. The FNMT-RCM shall issue, suspend and/or revoke these *Certificates* whenever requested to do so by the person in charge of the corresponding *Registry Office*, who is assumed to have sufficient power and authority for this type of *Certificates*.

135. The above shall be construed without detriment to that ordered by an administrative or judicial ruling.

136. The FNMT-RCM shall not be responsible, as with all other *Certificates* issued, of any actions conducted with this type of *Certificates* whenever there is an abuse of powers or lack of the same and/or whenever decisions are made by a member of the *Electronic Community* who is the *Certificate Signatory* affecting the validity of their powers, resulting, as the case may, on pecuniary liability, so that any modification, revocation or restriction of the *Certificate* and its use cannot be opposed by the FNMT-RCM unless unequivocally notified by someone authorized to do so or, as the case may be, by the person in charge of the corresponding *Registry Office*.

137. Likewise, the FNMT-RCM shall not be liable for actions conducted with this type of *Certificates* when the identification data of the *electronic venue*, included in the *Certificate* and for which it was issued, are different from those associated to the *electronic venue* where it is being used, so that any modification, revocation or restriction of the *Certificate* and its use cannot be opposed by the FNMT-RCM unless it has been unequivocally notified. The FNMT-RCM is not competent to prove or assess title of the electronic venues and/or domains of the Administrations, public bodies or entities the electronic venue belongs to.

138. The FNMT-RCM, as *Certification Services Provider* reserves the right not to issue or revoke this type of *Certificates* of the signatory/custodian of the *Certificate* of the *electronic venue* where said *Certificate* is used, misuses the same, violating industrial or intellectual property rights of others related to applications, websites or *electronic venues* to be protected with these *Certificates*, or if their

use can lead to misinterpretation or confusion on the ownership of said applications, websites or *electronic venues* and, therefore, their contents. In particular, this reservation of rights may be executed by the FNMT-RCM when the use of said *Certificates* is a violation of the following principles:

a) Safeguarding of public order, criminal investigation, public security and national defense.

b) Protection of public health or of the individuals who are consumers or users, even when acting as investors.

c) Respect for human dignity and the principle of non-discrimination for reasons of race, sex, religion, creed, nationality, disability or any other personal or social circumstance, and

d) Protection of youth and children.

139. The FNMT–RCM, shall be held harmless by the subscribers or people in charge of the computers, applications or *electronic venues* not complying with that contemplated in this section and which is related to the *Certificate*, and they shall be exonerated from any claim derived from improper use of these *Certificates*.

140. This *Certificate* is issued by the FNMT-RCM on behalf of the corresponding Public Administration to which the FNMT-RCM provides the necessary technical, administrative and security services as *Certification Services Provider*.

141. The *Certificate* for identification of *electronic venues* of the Public Administration is developed by the FNMT-RCM with a specific PKI infrastructure, based on actions for identification and registration conducted by the *Registry Offices* designated by the body or entity of the Public Administration holding, managing and administering the electronic address of the *electronic venue*.

142. The *Issuance Laws* may establish, within the scope of action of the Public Administrations, common *Registry Offices* for this scope of action with standard effects for any Administration, public body and/or entity.

143. This *Certificate* is issued with the corresponding technical profile and/or equivalent to the so-called Recognized Certificates, based on the criteria established for such under Law of Electronic Signatures (Law 59/2003), in the special regulations of the FNMT-RCM and in the technical standards EESSI, namely ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified certificates" and ETSI TS 101 862 – "Qualified Certificate Profile", both referring to the *Certification Services Provider* and to the generation of *Signature Verification Data* and the contents of the *Certificate* itself; all without prejudice to the specific features within the scope of action of the Public Administrations.

144. Consequently, the *Certificate* issued for identification of *electronic venues* shall not be ruled by that established in Law 59/2003, of 19th December, on Electronic Signatures for the legal entity *Certificate* in accordance with that stipulated in article 7.6 of said Law, therefore the specific corresponding regulations shall apply and, failing this, the General and Specific Statements of the FNMT-RCM, in the absence, as already mentioned, of specific regulations derived among other assumptions from the national interoperability and/or security plan.

13.1.3. Community and scope of application

145. This *Certification Policy* is applicable to issue public *electronic venue Certificates*. These *Certificates* shall have the following characteristics:

a) They shall be issued as *Recognized Certificates* or with an equivalent effect to those termed as *Recognized Certificates* based on the criteria established for this purpose in Law 59/2003, of 19th December, on Electronic Signatures and EESSI technical standards ETSI TS 101 862 – "Qualified Certificate Profile".

b) They shall be issued by the FNMT-RCM as *Certification Services Provider* in compliance with the criteria established in Law 59/2003, of 19th December, above, and in the EESSI technical standards, namely ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified certificates".

c) The *Certificates* issued under this *Certification Policy* shall be issued for the bodies and entities fitting the legal concept of Public Administration, attached or dependent public bodies and which are a part of the *Electronic Community*, as defined in the ***Definitions*** section of the *General Certification Practices Statement* of the FNMT-RCM, and with the sole purpose of identifying an *electronic venue* held by any of these public subjects.

   Within the framework of this *Certification Policy*, the *Certificate Applicant* shall be the personnel with sufficient powers and working for the Public Administration of the Kingdom of Spain, either a body or entity of the General, Regional or Local Administration of the State and holding, managing and administering the electronic address used to access the *electronic venue*.

d) *Certificates* issued under this *Certification Policy* are considered suitable as an integral part of the electronic signature systems requiring specific levels of security and, in particular, to establish secure communications between an electronic address and the user connecting to it, as well as serving as a tool to authenticate and identify the electronic address for which they were issued. Therefore, *Certificates* issued under this policy are considered suitable for fulfilment of Law 11/2007, of 22nd June, on Citizens' Electronic Access to Public Services and of Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration, in order to identify *electronic venues* within the public scope and to establish secure communications with them, suitable to be used to generate an electronic signature recognized within said scope.

146. The *Issuance Law* of these *Certificates* may determine, in the absence of specific regulations, the conditions of use and specific or individualized system for these *Certificates* that allow identification of *electronic venues* and attribution to the Administrations, bodies and entities of said electronic venues and responsible for their contents in the various transactions carried out; all with no legal modification or variation regarding the actions conducted by the Administrations, bodies and entities in traditional paper formats and others.

13.1.4. Liability and obligations of the parties

147. The obligations and liabilities expressed in this section are understood without prejudice to the corresponding derivatives of the legislation and rules of application, specifically those applicable to the FNMT-RCM as a provider of certification services and for such a condition established in the articles of law 59/2003, of 19 December, about Electronic Signature and its regulations.

148. For the purposes of this section, the following subjects shall be considered Parties:

- The Administration, bodies and public entities represented by the various competent bodies. Unless indicated otherwise, representation shall be held by the *Registry Offices* through their person in charge.

- The *Subscribers*, who shall be:

  the bodies and entities of the Public Administration holding, managing and administering the electronic address to access the *electronic venue* or, as the case may be, the body upon which powers are delegated. The FNMT-RCM shall consider the *Registry Offices* delegate entities or bodies, unless indicated otherwise.

- The *Signatories*/Custodians, shall be:

  the personnel working for the public Administrations, bodies and entities requesting the *Certificate* and which, therefore, assume the role of signatories and custodians of the *Signature Creation Data*. The FNMT-RCM shall consider, unless indicated otherwise, that the person in charge of the *Registry Office* is the signatory and custodian of the *Certificate* and of the *Signature Creation Data* contained therein.

- FNMT-RCM, as Certification Services Provider.

- As appropriate, the rest of the *Electronic Community* and Third Parties.

149. The system of rights and obligations of the public Administrations, bodies, entities and the FNMT-RCM shall be ruled by the corresponding agreement regulating the certification services. These agreements may establish the *Issuance Law* of these *Certificates*; without detriment to that stipulated in this Statement regarding the characteristics or common requirements applicable to the *Issuance Law* for each type of *Certificate* established, in general and with subsidiary effect, for that not contemplated in the corresponding agreements.

150. In general and in addition to the obligations and liabilities of the Parties listed in the *General Certification Practices Statement*, the public *Subscribers* Administration, bodies, and entities represented by the various competent bodies, acting through the person in charge of the *Registry Office* to issue this type of *Certificates*, is obliged to:

- Not conduct registrations or process *Certificate* requests for identification of *electronic venues* for the personnel working at an entity other than the one represented by the *Registry Office*, unless another entity has been expressly empowered.

- Not conduct registrations or process *Certificates* issued under this policy and whose Subscriber corresponds to a Public Administration that has no authority over it or if it has no powers to act as a *Registry Office*.

- Not conduct registrations or process *Certificates* issued under this policy and whose *Subscriber* does not correspond to title of electronic address to access the electronic venue that identifies the *Certificate* subject of the request.

- Not conduct registrations or process *Certificates* issued under this policy and whose *Signatory*, and custodian of the *Signature Creation Data*, corresponds to an *individual* not working for the *Certificate Subscriber* entity and/or does not match any of the established contacts, in the corresponding databases, for management and administration of the electronic address to access the *electronic venue* that identifies the *Certificate* subject of the request.

- Verify unequivocally identification and competence data of the *Certificate Subscribers* (the Administration owning the *electronic venue* and the electronic address, domain or URL, to access said *venue*) and *Certificate Applicant* (the individual with sufficient authority to request an *electronic venue Certificate*) and verify they match the *Subscriber* and established contacts

in the corresponding databases, for management and administration of the electronic address to access the *electronic venue* to identify the *Certificate* subject of the request.

- Request revocation of *Certificate* for identification of *electronic venue* issued under this policy when any of the data referring to the *Subscriber* or *Signatory* of the *Certificate*
  - is either incorrect, inaccurate or has changed with relation to that included in the *Certificate* or
  - does not correspond to the *Subscriber*,and contacts established in the corresponding databases for the management and administration of the electronic address included in the *Certificate* subject to the revocation.
- Not to use the *Certificate* when any of the data referring to the position or job or any other related to signatory/custodian of the *Certificate* is inaccurate, incorrect or does not properly show their relationship with the body or entity they work for; or, there are security reasons for this.

151. The relationship between the FNMT-RCM and the *Subscriber* shall be primarily determined, for the purpose of use of the *Certificates* by the document related to the conditions of use or, as the case may be, issue contract of the *Certificate* and in compliance with the agreements or document of relationship between the FNMT-RCM and corresponding Public Administration.

152. The rest of the Electronic Community and Third Parties shall regulate their relations with the FNMT-RCM through the General Certification Practices Statement and; as the case may be, through these Specific Certification Policies and Practices; all without prejudice to that stipulated in the regulations on electronic signatures and other applicable regulations.

153. The FNM T-RCM shall not be responsible for verifying matching of *Subscriber*, Signatory and the electronic address included in the Certificate with the Subscriber and administrative contacts listed, for said electronic address, in the databases of the entities regulating assignment and management of the names of the electronic addresses, as this task is the responsibility of the Registry Office

154. The FNMT-RCM shall not be liable for the use of *Certificates* issued under this *Policy* when the electronic *Certificate Subscriber* through their representative or signatory/custodian conducts actions without authority or beyond it or does not match the Subscribers and contacts authorized for management of the electronic address for which the *Certificate* has been issued.

13.1.5. Limits of use of the Certificates for identification of electronic venues

155. The limits of use of this type of *Certificates* are the corresponding administrative competences of each *Subscriber* identified under the *electronic venues* of the Public Administration, public bodies and attached or dependent entities, in accordance with Law 11/2007 and with Law 18/2011, for identification of *electronic venues* and establishment of secure communications with them. The FNMT-RCM and the Administration, bodies and entities may set up in the agreements or through the corresponding document of relationship or, if contemplated in the *Issuance Law* of these Certificates, other additional limits.

156. The *Certificate* for the public electronic venue shall not be used by any individual or entity other than the FNMT-RCM, for:

- Signing another *Certificate*, unless previously and expressly authorized by the FNMT-RCM.

- Private use.
- Signing software or components.
- Generating *Lists of Revocation* as Certification Services Provider.
- Any other use exceeding the purpose of this type of *Certificates* without prior authorization from the FNMT-RCM.

13.2. SPECIFIC CERTIFICATION PRACTICES FOR CERTIFICATES ISSUED FOR IDENTIFICATION OF ELECTRONIC VENUES OF THE PUBLIC ADMINISTRATION, BODIES AND ATTACHED OR DEPENDENT PUBLIC ENTITIES

157. The FNMT-RCM as *Certification Services Provider* and to prove the necessary reliability to provide said services, has developed a *Certification Practices Statement* whose purpose is to provide public information on the general conditions for provision of certification services by the FNMT-RCM as *Certification Services Provider*.

158. Of particular note in order to interpret this annex is the "Definitions" section of the main text of the *General Certification Practices Statement*.

159. This document is derived from and is an integral part of the *General Certification Practices Statement* of the FNMT-RCM and it defines the set of specific practices adopted by the FNMT-RCM as *Certification Services Provider* for management of the lifecycle of the *Certificates for identification of electronic venues of the Public Administration*, issued under the *Certificate Certification Policy for identification of electronic venues of the Public Administration, bodies and attached or dependent public entities* identified with 1.3.6.1.4.1.5734.3.3.2.2.

13.2.1. *Key* Management Services

160. Under no circumstance shall the FNMT-RCM generate or store *Private Keys* for its *Signatories*, generated under their exclusive control and that of the person in charge of the *Registry Office* whose custody is under their responsibility or, as the case may be, under the responsibility of the person designated by the *Registry Office*.

13.2.2. Certificate Lifecycle Management

13.2.2.1. Registration of Subscribers of public electronic venue Certificates

161. Prior to establishing any institutional relationship with the *Subscribers*, the FNMT-RCM shall inform through the means and websites mentioned in these Specific Certification Practices and, subsidiarily, in the *General Certification Practices Statement*, on the service conditions as well as the obligations, guarantees and liabilities of the parties involved in the issue and use of the *Certificates* issued by them as *Certification Services Provider*.

162. The FNMT-RCM as *Certification Services Provider*, through the *Registry Offices* identifies applicants and future *Subscribers* applying for Certificates for identification of *electronic venues* through the procedures set up for this purpose. The FNMT-RCM is empowered to consider any application coming from the person in charge of the corresponding *Registry Office*, who shall be considered representative of the *Subscriber*.

163. The FNMT-RCM shall collect from the *Applicants* only that information, received from the *Registry Office*, which is necessary to issue *Certificates* and for verification of identity, legitimacy and competence of representatives, storing the information required by electronic signature legislation for a period of fifteen (15) years, treating it with due diligence in order to comply with applicable national legislation regarding personal data protection.

164. The FNMT-RCM, given that within its activity as *Certification Services Provider* does not generate the pair of *Keys* for the *Signatories*, provides all the mechanisms necessary during the *Certificate Application* process to enable the person in charge of the *Registry Office* and/or *Subscriber* representative to hold the *Private Key* associated to the *Public Key* to be certified.

13.2.2.2. Application Procedure for electronic venue identification Certificate

165. Below is a description of the application procedure for the *Certificate* taking the official name of the public Administration, body or entity, who shall be the *Subscriber* of the *Certificates*, the personal data of the *Subscriber* representative, confirming their identity, validity of the position or job and formalizing, between *Subscriber* and FNMT-RCM the document on the conditions of use or standard issue contract for the subsequent issue of a *Certificate* for identification of the *electronic venue*.

166. For the record, the FNMT-RCM, according to the list of the *Subscribers* submitted by the Administration, body or public entity, shall consider, under the responsibility of the corresponding bodies and/or entities acting through the *Registry Offices*, that these *Subscribers* fulfil the requirements established under this Statement and, therefore, have the necessary legitimacy and competence to request and obtain the *Certificate* for *electronic venue* identification. The FNMT-RCM shall assume the *Subscriber* representatives entrusted with responsibility over the *Registry Office* have sufficient powers and competence.

167. The FNMT-RCM, shall not be liable, for this type of *Certificate*, for verifying:

- The authority and competence of the *Registry Office* to request an *electronic venue* identification *Certificate* on behalf of the body or entity of the administration in question and *Certificate Subscriber*.
- Ownership by the body or entity of the administration of the electronic address and/or domain included in the *Certificate.*
- That the *Certificate Applicant* is personnel working for the *Subscriber* Public Administration with sufficient legitimacy and competence to initiate the application and act as signatory and/or custodian of the *Certificate*.

168. Therefore, all the verification activities shall be conducted by the *Registry Offices* set up by the body or entity of the Public Administration in question which shall correspond, in each case, to the body or entity holding the *Certificate* and the electronic address to access their *electronic venue*.

169. The public AC Key sending for the generation of the certificate is made following a standard format, PKCS#10 o SPKAC, through a secure cannel.

13.2.2.3. Pre-Application

170. The representative of the *Subscriber* who, usually, is the person in charge of the corresponding *Registry Office*, in the electronic signature system based on a secure device or equivalent medium, shall generate the *Public* or *Private Keys* linked to the *Certificate*, subsequently becoming signature *verification and creation* data respectively.

171. The representative and/or person in charge of the *Registry Office* prepares an electronic *Certificate* application, generally in PKCS#10 format, and enters the *Certification Services Provider*'s *website*, the FNMT-RCM, through

https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp

where a form shall be shown asking said representative to enter data of *Subscriber* body in charge of the *electronic venue* for which the *Certificate* is to be issued, and the data of the *individual* responsible for the diligent custody of the Signature Creation Data. In addition, the person in charge shall also enter the electronic application generated previously.

172. In response to submission of the form the FNMT-RCM shall assign and inform the person in charge of the application code to be used at the *Registry Office* upon application for the *Certificate*.

173. Previously, the representative and/or person in charge of the *Registry Office* and the *Subscriber* Administration shall consult the *General Certification Practices Statement* and these *Specific Certification Policies and Practices* at

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

with the conditions of use and obligations of the Parties, with the possibility of checking the scope of this Statement; all without detriment to the fact the *Subscriber* representative in charge of the *Registry Office* and the FNMT-RCM, must subscribe the document on conditions of use or, if appropriate, the issue contract. Under no circumstance shall continuation of the pre-application procedure imply completion of the process.

174. When carrying out this pre-application the FNMT-RCM shall be sent the *Public Key* generated, together with the corresponding proof of possession of the *Private Key*, for subsequent issue of the *Certificate*.

175. Upon receiving this information, the FNMT-RCM shall check with the applicant's *Public Key* the validity of the information of the signed pre-application, verifying possession and matching of the pair of encryption *Keys* by the representative and/or person in charge of the *Registry Office* and the size of keys generated.

176. This information shall not result in the generation of a *Certificate* by the FNMT-RCM, until they receive the *Certificate* application signed by the person in charge of the *Registry Office*.

13.2.2.4. Confirmation of Party identities and requirements

177. The person in charge of the *Registry Office* shall be identified with their national identity document or substitute identification document by the FNMT-RCM, with the corresponding registration application and use of their own *Recognized Certificate*. FNMT-RCM shall assume that the person in charge of the *Registry Office* is exercising their competence and has sufficient power to conduct the necessary transactions to obtain this type of *Certificates*.

13.2.2.5. Appearance in person of Applicant at Registry Offices

178. For cases other than intervention of the person in charge of the *Registry Office*, in order to obtain the *Certificate*, the person designated by the *electronic venue Certificate Subscriber* shall be considered an *Applicant* with sufficient authentication and competence.

179. In order to obtain the *Certificate*, the *Applicant* must appear in person at the *Registry Office* designated for this purpose by the *Certificate Subscriber* body or entity.

13.2.2.6. Appearance in person and documentation

180. For cases other than intervention of the person in charge of the *Registry Office*, in order to obtain the *Certificate*, the representative of the *Subscriber Applicant* shall appear in person and submit the data required and which prove, before the *Registry Office*:

- their personal identity,
- their status as personnel working for the body or entity of the *Certificate Subscriber* Administration and Subscriber of the electronic address to access the *electronic venue* subject of the *Certificate*
- their status as person empowered or designated to manage the electronic address to access the *electronic venue* subject of the *Certificate*

181. The FNMT-RCM shall in any case accept the function and report provided by the *Registry Office* designated by the Administration. If the above points have not been proven, the *Registry Office* shall not continue processing the *Certificate* application.

13.2.2.7. Submission of information to the FNMT-RCM

182. Once the *Applicant*'s identity has been confirmed as well as the validity of the authentication and competence conditions required, including but not limited to, ownership of the electronic address, the document of conditions of use shall be subscribed or, as the case may be, application contract by the *Applicant* on behalf of the *Subscriber* and/or person in charge of the *Registry Office*. The above information and documents shall be submitted, together with the application code collected during the pre-application phase, to the FNMT-RCM. Processing of all personal data shall be subject to applicable legislation.

183. This submission shall only take place if the *Registry Office* has legitimacy and competence to act as such on behalf of the body or entity of the Public Administration of the *electronic venue* identification *Certificate* and if this administration is the Subscriber of the electronic address to access the *electronic venue* subject of the *Certificate*.

184. Transmission of information to the FNMT-RCM shall be conducted through secure communications established for this purpose between the *Registry Office* and the FNMT-RCM.

13.2.2.8. Extension of the registration and identification function to other Certificates issued by the FNMT-RCM.

185. The members of the *Electronic Community* may receive from the FNMT-RCM certification and electronic signature services, based on the issue of electronic *Certificates* belonging to various

Issuance Laws and on various formats, by accepting the conditions that, specifically, shall be set forth at the request of the FNMT-RCM in the various websites and other service formats of the *Electronic Community* members, in accordance with that established in the corresponding sector legislation and with the limitations established in the legislation regulating personal data processing.

186. For provision of the services outlined in the above paragraph, the effects of the actions derived from registration and identification may be extended, with the time limits contemplated in electronic signature legislation, as well as that regulating the DNI-e; all without detriment to any specific features that may apply to the area of Public Administrations.

13.2.2.9. Issue of Certificate for electronic venue identification

187. Once the FNMT-RCM has received the *Subscriber* and *Applicant's* data, the information describing the relationship of the representative with the Public Administration (without prejudice to it being submitted by the person in charge of the *Registry Office*), as well as the application code obtained during the pre-application phase and, as the case may be, information describing ownership and management of the electronic address of the venue in question, the *Certificate* shall be issued.

188. Issuing a *Certificate* entails generating electronic documents confirming the identity and ownership of an electronic address to access an *electronic venue*, as well as its management by a body or entity of the Spanish Public Administration, as well as the link with the Signatory/custodian of the signature creation data and person in charge of any operations carried out with said *Certificate* within the framework of *electronic venue* identification and establishment of secure communications with them.

189. *Certificates* of the FNMT-RCM may only be issued by them, as *Certification Services Provider*, there being no other entity or body authorized to issue them.

190. The FNMT–RCM, by means of its *Electronic Signature*, authenticates the *Certificates* and confirms the identity and competence of the *Subscriber and Applicant*, as well as ownership of the electronic address of the venue and the contacts established to manage said address, in accordance with the information received by the *Registry Office*. Moreover and in order to avoid tampering of the information included in the *Certificates*, the FNMT-RCM shall use encryption mechanisms that ensure the authenticity and integrity of the *Certificate*.

191. The FNMT-RCM shall in no case include in a *Certificate* information other than that described herein, or any circumstance, specific attribute of signatories or limits other than those contemplated in the agreements and, as the case may be, those contemplated in the corresponding *Issuance Law*.

192. In any case, the FNMT-RCM shall exercise due diligence to:

- Check that the *Certificate Applicant* or person in charge of the *Registry Office* uses the *Private Key* corresponding to the *Public Key* linked to the identity of its *Signatory*. For this the FNMT-RCM shall check that the *Private Key* and the *Public Key* match.
- Ensure the information included in the *Certificate* is based on the information provided by the *Applicant* and/or the person in charge of the corresponding *Registry Office*.
- Not ignore evident facts that may affect the *Certificate*'s reliability.
- Ensure the *DN* (Distinguished Name) assigned in the *Certificate* is unique in the whole *Public Key Infrastructure* of the FNMT-RCM.

193. To issue the Certificate the following steps shall be taken:

1. Composition of Certificate Distinguished Name (DN).

The Distinguished Name (*DN*) is made up with the data of the venue electronic address collected during the *Certificate* application phase, in accordance with standard X.500, ensuring said name makes sense and is not ambiguous. Pseudonyms may not be used to identify the *Subscriber*.

The *DN* is made up of the following elements:

DN=CN, OU, OU, OU, O, C

The attribute *CN* contains the electronic address to access the electronic venue subject of the *Certificate*.

2. Composition of an alternative Cerficate identity

The Certificate alternative identity, as contemplated in this type of *Certificates* contains the identity of the electronic venue and the *Subscriber* distributed in a series of attributes. The subjectAltName extension defined in *X.509* version 3 is used to provide this information.

Within said extension, the subfield directoryName is used to include a set of attributes defined by the FNMT-RCM, which include information in question.

3. Generation of *Certificate* in accordance with the *electronic venue* identification *Certificate* Profile

The *Certificate* format for electronic venue identification issued by the FNMT-RCM under this policy, in line with standard UIT-T X.509 version 3 and in accordance with legally applicable regulations regarding *Recognized Certificates*, may be seen in the annexes to this document.

They describe the *Certificate* profiles distinguishing by issuing *Certification Authority* (always subordinated to the *Root Certification Authority* of the FNMT-RCM).

The necessary extensions shall also be included to be able to conduct venue identification through the access electronic addresses indicated in the *Certificate*.

Extension name: extKeyUsage

Values: Server Authentication: 1.3.6.1.5.5.7.3.1

13.2.2.10. Download and installation of the electronic venue identification Certificate

194. Not later than 72 hours from the document reception in the FNMT – RCM in order to make the pre reviews commented before the expedition of the *electronic office Certificate*, the FNMT-RCM shall make available for the person in charge of the corresponding *Registry Office* a mechanism to download the *Certificate*, at the address owned by the Administration or body, through the following link:

https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp

195. For this purpose, you must access the option “Download your Certificate”.

196. During this guided process the person in charge of the *Registry Office* in the *Subscriber*’s area shall be asked to enter the CIF (Tax Identification Code) of the public body or entity conducting the pre-application process as well as the application code provided by the system upon completion of said process. If the *Certificate* has not been generated yet for any reason, you shall be notified of this fact when you attempt to download it.

197. If the *Certificate* has already been made available to the personnel working for public administration or Registry Office, it shall be directly entered in the format in which the *Keys* were generated during the Pre-application process.

13.2.2.11. Validity of the Electronic Venue Identification Certificate

13.2.2.11.1. Expiry

198. The electronic venue identification *Certificates* issued by the FNMT-RCM shall have a validity of three (3) years from the moment the *Certificate* is issued, provided its validity is not terminated. After this period and if the *Certificate* is still active, it shall expire and whenever the Subscriber wishes to continue using the services of the Certification Services Provide a new one must be issued.

13.2.2.11.2. Termination of Certificate Validity

199. The electronic venue identification *Certificates* issued by the FNMT-RCM shall become null in the following cases:

a) End of *Certificate* validity period

b) Cessation of activity as *Certification Services Provider* by the FNMT-RCM, unless, with prior express consent from the *Subscriber* the *Certificates* issued by the FNMT-RCM have been transferred to another *Certification Services Provider*.

In these two cases [a) and b)], the loss of effect of the *Certificates* shall take place the moment these circumstances occur.

c) Suspension or revocation of the *Certificate* for any of the causes contemplated in this document.

200. For the purposes listed above, it is noted that application for issue of an electronic venue identification *Certificate* issued by the FNMT-RCM when there is another one in force for the same venue and Subscriber and belonging to the same *Issuance Law* shall entail revocation of the first one obtained.

201. The consequences of revocation or suspension of the *Certificate*, that is, termination of its validity, shall come into effect on the date the FNMT-RCM become aware of any of the determining facts and they state as such in their *Information and Inquiry Service on the Status of Certificates*.

13.2.2.12. Revocation of the electronic venue identification Certificate

13.2.2.12.1. Causes for revocation

202. The causes admitted for revocation of a *Certificate* are listed below. The *Issuance Law* may, in addition, establish other causes for revocation, suspension and cancellation of the suspension.

203. The FNMT-RCM shall only be liable for the consequences derived from not having revoked a *Certificate* in the following cases:

- When revocation should have been carried out due to termination of the contract subscribed with the *Subscriber*.
- When the revocation has been requested by the corresponding *Registry Office* to the *Signatory* entity or body following the procedure established for this type of *Certificates*.

- When the revocation request or the cause for the same has been notified by means of a judicial or administrative ruling.
- When causes c) to g) in this section are evidenced unequivocally, after identifying the revocation applicant.

204. Taking into account the above, causes for revocation of an electronic venue identification *Certificate* are:

a) Revocation request by authorized persons. In all cases, this request shall be based on:

- Loss of *Certificate* physical format.
- Use by a Third Party *Signature Creation Data*, corresponding to the *Signature Verification Data* included in the *Certificate* and linked to the *Signatory* personal identity.
- Violation or jeopardizing of confidentiality *Signature Creation Data.*
- Non-acceptance of new conditions that may lead to issue of new *Certification Practices Statements*, within a period of one month since its publication.

b) Judicial or administrative ruling ordering so.

c) Termination, dissolution or closure of electronic venue.

d) Termination or dissolution of legal entity status of *Subscriber*.

e) End of representation of *Certificate Subscriber* representative.

f) Total or partial unforeseen disability of *Subscriber, Signatory* or the Party being represented.

g) Inaccuracies in the data provided by the *Applicant* to obtain the *Certificate*, or alteration of the data provided to obtain the *Certificate* or modification of the circumstances verified to issue the *Certificate*, such as those related to the position or authority for representation, to the extent it were no longer in effect.

h) Violation of a substantial obligation in this *Certification Practices Statement* by the *Subscriber, Certificate Applicant* or by a *Registry Office* if, in the latter case, it may have had an impact on the *Certificate* issue procedure.

i) Cancellation of contract subscribed between *Subscriber, Certificate Subscriber* or their representative, and the FNMT-RCM.

j) Violation or jeopardizing of confidentiality of the *Signature Creation Data* of the FNMT-RCM, with which they sign the *Certificates* issued.

205. Under no circumstance shall it be construed that the FNMT-RCM assumes any obligation whatsoever to verify the points listed in letters c) to g) in this section.

206. Actions representing a crime or offense which the FNMT-RCM is not aware of related to the *Certificate* data, inaccuracies of the data or lack of diligence in their communication to the FNMT-RCM, shall exonerate the FNMT-RCM from liability.

13.2.2.12.2. Effects of the revocation

207. The effects of revocation or suspension of the *Certificate*, that is, termination of its validity, shall come into force on the date the FNMT-RCM has evidence of any of the determining facts and states as such in its *Information and Inquiry Service on the Status of Certificates*.

208. Revocation of the *Certificates* implies, aside from their termination, end of the relationship and system of use of the *Certificate* with the FNMT-RCM.

13.2.2.12.3. Procedure for revocation

209. The revocation request for the electronic venue identification *Certificates* may be carried out during the validity period indicated in the *Certificate*.

210. Revocation of the *Certificates* consists of cancellation of the guarantee of identity, authenticity or other properties of the *Subscriber* and their representatives and correspondence with the associated Public Key. It implies, aside from their termination, end of the relationship and system of use of the Certificate with the FNMT-RCM

211. The Parties authorized to request revocation of an electronic venue identification *Certificate*, based on inaccurate data, change of the same or any other cause to be assessed by the *Signatoy or Applicant* are:

- The Management board, body or public entity Subscriber of the *Certificate* or delegated person.
- The *Registry Office*, —through its person in charge— designated for this purpose, by the Administration, body or attached or dependent entity holding the *Certificate* to be revoked, when it detects that any of the data included in the *Certificate*
    - is either incorrect, inaccurate or has changed with regard to that entered in the *Certificate* or
    - the individual, signatory/custodian of the *Certificate* does not match the ultimate person in charge or designated person to manage and administer the electronic address included in the *Certificate* subject of the revocation always within the framework of the terms and conditions regarding the revocation of *Certificates* in the *Certification Practices Statement*.

212. Below is the procedure to be followed by the *Registry Office* to formalize the request of revocation of a *Certificate*. In any case the FNMT-RCM, shall assume the *Applicant* is duly authorized and empowered when it is the person in charge of the corresponding *Registry Office*.

1. Appearance in person of the *Applicant* before the *Registry Offices*

To revoke the *Certificate*, the *Applicant* with sufficient authority and competence, shall appear in person before a *Registry Office* designated for this purpose by the body or entity holding the *Certificate* to be revoked or it shall be conducted directly by the person in charge of the *Registry Office*.

2. Appearance in person and documentation

Applicant shall provide the data required and proving:

- their personal identity,
- their personal status as working for the body or entity of the *Certificate Subscriber* Public Administration and holder of the electronic address to access the electronic venue subject of the *Certificate* or their status as person in charge of the *Registry Office*.
- their status as person designated to manage the electronic address to access the electronic venue subject of the *Certificate* to be revoked or as personnel attached to the *Registry Office* designated for said purpose by the body or entity holding the *Certificate* to be revoked.

FNMT-RCM shall accept, in all cases, the function and report prepared by the *Registry Office* designated by the Administration. If the above points are not evidenced, the *Registry Office* shall not proceed with the request for the *Certificate* revocation.

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

Without evident causes of lack of competence by the person in charge of the *Registry Office* and/or having confirmed the *Applicant* identity, validity of the conditions required from them and the revocation request document having been subscribed, the *Registry Office* shall proceed to validate the data and send them to the FNMT-RCM for the effective revocation of the *Certificate*. Processing of all personal data shall be subject to applicable legislation.

This submission shall only take place if the *Registry Office* has the authority to act as such on behalf of the body or entity of the Public Administration holding the *Certificate* and if it is the Subscriber of the electronic address to access the electronic venue subject of the *Certificate*.

This information shall be transmitted to the FNMT-RCM through secure communications established for this purpose between the *Registry Office* and the FNMT-RCM.

213. In addition, the revocation requests can be done through the phone number 902 200 616, as a 24 x 7 telephone service. The communication will be recorded and registered, as a guarantee of the application for revocation.

214. The A*pplicant* of the revocation through the telephone service shall be the *Subscriber* or his representative, and must appear as such in the *Certificate* to be revoked. For the representative, it must be the same person who acted as such at the time for applying for the *Certificate*.

215. Once the FNMT-RCM has revoked the *Certificate*, it shall publish the corresponding *List of Revoked Certificates* in the secure *Directory* including the serial number of the revoked *Certificate*, the date and time and cause of revocation. *Subscriber* shall receive, through the email address used for the application, a notification about the change of the *Certificate's* validity status.

13.2.2.13. Suspension of electronic venue identification Certificate

216. Suspension of the *Certificate* leaves the Certificate without effect for a set period of time and conditions.

217. Suspension of a *Certificate* is considered a temporary revocation of the validity of the Certificate therefore the procedures and entities empowered to request and process a *Certificate* revocation shall apply in the event of a suspension.

13.2.2.13.1. Causes for suspension

218. The FNMT-RCM may suspend validity of *Certificates* upon request from the legitimate interested party or a Legal Authority or if there is ground to suspect the existence of validity termination causes for the *Certificates* as contemplated in the "Causes for Revocation of electronic venue identification Certificates" section.

219. Likewise, the request for suspension may be due to an ongoing investigation or legal or administrative procedure, whose conclusion may determine that the *Certificate* is indeed affected by a cause for revocation. In these cases the FNMT-RCM, at the request of the legitimate interested party, shall suspend the validity of the *Certificate* for the period requested and, after said period, shall revoke the *Certificate* unless the FNMT-RCM is unequivocally requested by the legitimate interested party to reactivate it.

13.2.2.13.2. Effects of the suspension

220. Suspension of the *Certificate* leaves the *Certificate* without effect (terminates its validity) for a set period of time and conditions.

13.2.2.13.3. Procedure for suspension

221. Suspension of *Certificates*, given their nature, may only be carried out by the person in charge of the corresponding *Registry Office*, although the *Signatory* may request it from the *Registry Office* in pertinent cases.

222. Below is a description of the procedure to be followed by the *Registry Office* whereby personal data are collected, their identity is confirmed and, if appropriate, the request for suspension of the *Certificate* is formalised by a legitimate interested party.

223. These tasks shall be carried out by the *Registry Office* of the entity or body which the *Signatory* belongs to.

224. The FNMT-RCM shall suspend the *Certificate* provisionally for a period of thirty (30) days, after which the *Certificate* shall terminate through direct revocation by the *Certification Services Provider* of the FNMT-RCM, unless the suspension has been withdrawn. Notwithstanding the above, the period contemplated for suspension of the *Certificate* may change according to any legal or administrative proceedings that may affect it.

225. If during the *Certificate* suspension period it should expire or its revocation were requested, the same consequences shall apply as for non-suspended *Certificates* affected by termination or revocation causes.

1. The *Registry Office* of the area corresponding to the public *Subscriber* body or entity may request suspension of the *Certificate* by signing the *Certificate* suspension request form submitted either on paper or electronically.

   The *Registry Offices* shall forward the processed registrations to the FNMT-RCM in order for the latter to suspend the *Certificate*. Processing of all personal data shall be subject to applicable legislation.

   Once the FNMT-RCM has suspended the *Certificate*, the corresponding *List of Revocation* shall be published in the *Directory* with the serial number of the suspended *Certificate*, and the date and time of suspension and as cause for revocation: “suspension".

   In all the above situations of the *Specific Certification Practices* requiring identification and whenever electronic identification is possible, the *Provider* FNMT-RCM shall consider the functionalities contemplated for the DNI-e, in accordance with applicable legislation and the use of another *Certificate* issued by the FNMT-RCM or recognized by them.

2. Cancellation of suspension of electronic venue identification *Certificate*

   Cancellation of suspension of *Certificates* issued by the FNMT-RCM may be requested by the *Subscribers*, through their representatives, provided said request is conducted within thirty (30) days from the suspension.

   The FNMT-RCM shall consider there is sufficient authority to act, for the purposes of this section, when the request is conducted through the person in charge of the corresponding *Registry Office*.

Without prejudice to the above, an in the event of operating through *Certificate Subscriber* representatives other than the person in charge of the *Registry Office*, appearance in person and/or the cancellation request shall be carried out through and/or at the *Registry Office* designated by the body or entity which the Signatory belongs to and in accordance with the FNMT-RCM criteria in force in order to ensure standardization in all cases.

For this transaction, the applicant representing the *Certificate Subscriber*, with sufficient competence for the request, shall provide all the data required and prove their personal identity, following the procedure described above for requesting issue of electronic venue identification *Certificate*.

The FNMT-RCM shall accept the proof issued by the *Registry Office* as established in article 13.1, *in fine*, of Law 59/2003, of 19th December, on Electronic Signatures.

The personal data of the person in charge of the *Registry Office* or the *Subscriber* representative, once validated by the *Registry Office*, shall be sent to the FNMT-RCM through secure communications established for this purpose between the *Registry Office* and the FNMT-RCM. Processing of all personal data shall be subject to applicable legislation.

Once the data validated by the *Registry Office* requesting withdrawal of suspension have been received, the FNMT-RCM shall withdraw this *Certificate* from the List of Revocation, and no technical action whatsoever shall be conducted on the *Certificate* in question.

As in previous cases for identification purposes, the functionalities foreseen for the DNI-e shall be taken into account, in accordance with applicable legislation and other contemplated for Public Administrations.

13.2.2.14. Identification certificate renewal of electronic office

226. The renewal of the identification certificate of electronic office is always done by releasing new keys, so the process is the same as the obtention of a new certificate.

13.2.2.15. Verification of electronic venue identification Certificate status

227. The *Certificate* Subscriber and the user Administrations, bodies and entities belonging to the *Electronic Community* may verify the status of a *Certificate* in the manner and conditions described in this section.

228. The status of the electronic venue identification *Certificate* may be verified either by accessing the Lists of Revocation, or through the *Information and Inquiry Service on the Status of Certificate*s through the OCSP protocol.

229. These services shall be available twenty-four (24) hours a day, every day of the year, except for circumstances beyond the control of FNMT-RCM or for maintenance operations. The FNMT-RCM shall notify of this situation at http://www.ceres.fnmt.es if possible at least forty-eight (48) hours in advance and shall try to resolve it within a maximum of twenty-four (24) hours.

230. The FNMT-RCM has an OCSP responder service to provide the *Information and Inquiry Service on the Status of Certificates* under the terms subscribed in the corresponding agreement, contract or *Issuance Law*.

231. The service works as follows: The OCSP server receives the OCSP request made by an *OCSP Client* registered in the system and it checks status of the *Certificates* included in it. If the request is valid, an

OCSP response shall be issued informing on the current status of the *Certificates* included in the request.

232. It shall be the *user Entity*'s responsibility to obtain an *OCSP Client* to operate with the OCSP server made available by the FNMT-RCM.

233. It is the *user Entity*'s responsibility applying for the OCSP service to obtain, as the case may be, consent from *Certificate Subscriber* for which OCSP service is being requested, as well as inform him of the corresponding conditions and limitations.

234. The above is understood with the scope and limits of legislation on automated processing of personal data and in accordance with the corresponding contracts, agreements or *Issuance Laws* regulating the electronic certification service of the FNMT-RCM.

235. The FNMT-RCM shall not provide a verification service of *Certificate*s of other *Subscribers* unless established as such in agreements and/or contracts with the corresponding consent from the members of the *Electronic Community* or under the terms contemplated in the *Issuance Law.*

236. In particular, for dissemination and reliability of the systems which have these *Certificate*s, the FNMT-RCM, may provide the possibility of a member of the *Electronic Community* or a third party verifying that the electronic venue identification *Certificate* is a valid *Certificate* issued by the FNMT-RCM, as well as other features of the same.

14 CERTIFICATES ISSUED FOR AUTOMATED ADMINISTRATIVE ACTIONS OF THE PUBLIC ADMINISTRATION, BODIES AND ATTACHED OR DEPENDENT PUBLIC ENTITIES

14.1. CERTIFICATION POLICY FOR CERTIFICATES ISSUED FOR AUTOMATED ADMINISTRATIVE ACTIONS OF THE PUBLIC ADMINISTRATION, BODIES AND ATTACHED OR DEPENDENT PUBLIC ENTITIES

14.1.1. Identification

237. For identification and authentication of exercise of administrative competences in automated processes, the FNMT-RCM offers this electronic certification service based on the consideration of the legal concept contemplated in Law 11/2007, of 22nd June on Citizens' Electronic Access to Public Services corresponding to article 18. a): Electronic Seals of the Public Administration, and other bodies and attached or dependent entities, also in Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration corresponding to article 19. a) Electronic Seal of the legal office,seal and based on an electronic *Certificate* under the terms contemplated in Law 59/2003, of 19th December, on Electronic Signatures.

238. This *Specific Certification Policy* of the FNMT-RCM to issue *Certificates* for automated administrative actions of the Public Administration, bodies and attached or dependent public entities bears the following identification

Name: *Certificate Certification Policy* for automated administrative actions of the Public Administration, bodies and attached or dependent public entities

Reference / OID[6]:

- 1.3.6.1.4.1.5734.3.3.3.2

Version: 2.4

Issue Date: 24th June 2016

Related DPC: General Certification Practices Statement of the FNMT-RCM

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

14.1.2. Type of Certificate for automated administrative actions of the Public Administration, bodies and attached or dependent public entities

239. The "*Certificate*s for automated administrative actions" with the electronic seal concept are *Certificate*s issued by the FNMT-RCM under this certification policy and which link *Signature Verification Data* to:

- the identification and authentication data of a specific Administration, body or entity and their respective organization units (unit conducting the automated administrative action: area, section, department and
- the *individual* in charge of the corresponding *Registry Office* and/or representative of the *Certificate* Subscriber Administration, body or entity and, as the case may be, delegated personnel for the automated administrative action.

240. The *individual* shall act as signatory of the automated administrative actions and custodian of the key and, therefore, in control of said *Certificate* and the *Signature Creation and Verification Data* and is in charge of their diligent custody, without prejudice to any delegations that may take place, in accordance with applicable legislation.

241. The FNMT-RCM shall issue these electronic stamp *Certificate*s whenever requested to do so by members of the *Electronic Community* under Law 11/2007, of 22nd June, ande under Law 18/2011, for the various relationships that may arise from the automated administrative/legal action and whose use is not prohibited or limited by applicable legislation.

242. The FNMT-RCM shall not be responsible for actions conducted with this type of *Certificate*s when there is an abuse of powers or lack thereof and/or when a *Certificate* Subscriber member of the *Electronic Community* makes a decision that may affect the validity of their powers, so that any

---

[6] *Note*: The OID or policy identifier is a reference to be included in the *Certificate* in order for users to be able to determine applicable practices and procedures to issue the *Certificate* in question.

Although this document describes a single policy for this type of *Certificates*, there may be two different references to distinguish or identify specific features in the *Certificate* profiles, *Certification Authority* used for issue or issue procedures.

Therefore, the Certificate Certification Policy and Practices for identification of venues shall be described singly, identifying any possible specific features and associating them to the corresponding OID or references.

modification, revocation or restriction of the *Certificate* and its use cannot be opposed by the FNMT-RCM unless it has been unequivocally and duly notified.

243. Likewise, the FNMT-RCM shall not be liable for actions conducted with this type of *Certificates* when the identification and authentication data of the organization unit of the administration indicated in the *Certificate* does not correspond to a unit dependent on said administration entity.

244. The FNMT-RCM, as *Certification Services Provider* reserves the right not to issue or revoke this type of *Certificates*, being exonerated from liability in this regard, if the *Certificate* user and/or the signatory/custodian and/or organization unit (conducting automated/legal administrative actions) where said *Certificate* is used, lacks competence, misuses the same, violating industrial or intellectual property rights of others related to applications and actions carried out or any other applicable legislation.

245. The FNMT–RCM, shall be held harmless by the *Subscriber* and the people in charge or their representatives regarding property of rights and/or flaws or defects of computers, applications or systems not complying with that contemplated in this section and related to the *Certificate*, and they shall be exonerated from any claim derived from improper use of these *Certificates*.

246. This *Certificate* is issued by the FNMT-RCM on behalf of the corresponding Public Administration to which the FNMT-RCM provides the necessary technical, administrative and security services as *Certification Services Provider*.

247. The electronic seal *Certificate* for automated administrative/legal actions of the Public Administration is developed by the FNMT-RCM with a specific PKI infrastructure, based on actions for identification, authentication and registration conducted by the *Registry Offices* designated by the body or entity of the Public Administration the organization unit conducting the automated administrative action indicated in the *Certificate* depends on.

248. The *Issuance Laws* may establish, within the scope of action of the Public Administrations, common *Registry Offices* for this scope of action with standard effects for any Administration, public body and/or entity.

249. This *Certificate* is issued with the corresponding technical profile for *Recognized Certificate*s or equivalent *electronic signature systems* as established in Law 59/2003, of 19th December, on Electronic Signatures as well as in the special regulations of the FNMT-RCM and in technical standards EESSI, namely ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified *Certificate*s" and ETSI TS 101 862 – "Qualified *Certificate* Profile", both referring to the *Certification Services Provider* and to the generation of *Signature Verification Data* and the contents of the *Certificate* itself.

14.1.3. Community and scope of application

250. This *Certification Policy* is applicable to issue electronic *Certificate*s suitable to operate as electronic seals, with the following characteristics:

a) They shall be issued as *Recognized Certificates* or with an equivalent effect to those termed as *Recognized Certificates* based on the criteria established for this purpose in Law 59/2003, of 19th December, on Electronic Signatures and EESSI technical standards ETSI TS 101 862 – "Qualified Certificate Profile".

b) They shall be issued by the FNMT-RCM as *Certification Services Provider* in compliance with the criteria established in Law 59/2003, of 19th December, above, and in the

EESSI technical standards, namely ETSI TS 101 456 - "Policy requirements for certification authorities issuing qualified certificates".

c) The *Certificates* issued under this *Certification Policy* shall be issued for the Public Administration, bodies and attached or dependent public entities which are a part of the *Electronic Community*, as defined in the ***Definitions*** section of the *General Certification Practices Statement* of the FNMT-RCM, and with the sole purpose of identifying and authenticating competence for automated administrative actions, by means of an *electronic Seal*.

d) Within the framework of this *Certification Policy*, the *Certificate Applicant* shall be the person in charge of the *Registry Office* and/or the representative of the *Subscriber* or delegated person of the organization unit conducting the automated administrative action and to be included in the *Certificate* working for a Public Administration of the Kingdom of Spain, either a body or entity of the General, Regional or Local Administration of the State which said organization unit reports to.

e) The *Certificate*s issued under this *Certification Policy* include the tax identification number and the name of the entity, body or unit of the Public Administration *Certificate* Subscriber.

f) *Certificates* issued under this *Certification Policy* are considered suitable as an integral part of the electronic signature systems for automated/legal administrative actions by the Public Administration. Specifically, these *Certificate*s meet the requirements established by legislation on Electronic Signatures and are valid for the creation of electronic seals of the Public Administration, body or public law entity. Therefore, *Certificates* issued under this policy are considered suitable for fulfilment of Law 11/2007, of 22nd June, on Citizens' Electronic Access to Public Services and of Law 18/2011, of 5th July, regulating the use of information and communications technology in the Justice Administration, for identification and authentication of competence for automated administrative/legal actions of the Public Administration.

251. The *Issuance Law* of these *Certificates* may determine, in the absence of specific regulations, the conditions of use and system of these *Certificate*s that allow attribution to Administrations, bodies and entities of the various actions and resolutions conducted by *Signatories*. All with no legal modification or variation regarding the actions conducted by *Signatories* in traditional paper formats and others.

14.1.4. Liability and obligations of the parties

252. The obligations and liabilities expressed in this section are understood without prejudice to the corresponding derivatives of the legislation and rules of application, specifically those applicable to the FNMT-RCM as a provider of certification services and for such a condition established in the articles of law 59/2003, of 19 December, about electronic signature and its regulations.

253. For the purposes of this section, the following subjects shall be considered Parties:

- The *Subscribers*: the Administration, bodies and public entities represented by the various competent bodies.
- The signatories/custodians of the *Certificate*s and of the *Signature Creation Data*: the personnel working for the Administrations, bodies and public entities requesting the *Certificate* and/or the person in charge of the corresponding *Registry Office*, indicated in the *Certificate* and which therefore assume the role of signatory and custodian of the *Signature Creation Data*.

- FNMT-RCM, as Certification Services Provider.
- As the case may be, the rest of the *Electronic Community* and third parties

254. The system of rights and obligations of the public Administrations, bodies, entities and the FNMT-RCM shall be ruled by the corresponding agreement regulating the certification services. These agreements may establish the *Issuance Law* of these *Certificate*s.

255. In general and in addition to the obligations and liabilities of the Parties listed in the *General Certification Practices Statement*, the public *Subscribers* Administration, bodies, and entities represented by the various competent bodies and the *Registry Office* acting to request issue of this type of *Certificate*s from the FNMT-RCM is obliged to:

- Not conduct registrations or process *Certificate* requests for automated administrative actions issued under this policy, by the personnel working for an entity other than the one represented by the *Registry Office*.
- Not conduct registrations or process *Certificates* issued under this policy and whose title, referred to the administration body, corresponds to a Public Administration entity it has no authority over or if it has no powers to act as a *Registry Office*.
- Not conduct registrations or process *Certificates* issued under this policy, for an organization unit not reporting to the *Certificate* Subscriber administration body.
- Not conduct registrations or process *Certificates* issued under this policy and whose title, referred to the signatory and custodian of the *Signature Creation Data*, and identity of the applicant does not correspond to the *individual* in charge of the organization unit to be indicated in the *Certificate*, unless it is the person in charge of the *Registry Office*.
- Verify unequivocally *Applicant* identification data, representative of *Certificate Subscriber*, and verify they belong to the organization unit as person in charge of the same.
- Revoke *Certificate* issued under this policy when any of the data referring to the *Subscribers* or signatories/custodians of *Certificate*
  - is incorrect or inaccurate
  - or the *individual* (signatory/custodian) representing the *Certificate* Subscriber, is not a manager with sufficient authority in the organization unit indicated in the *Certificate*
  - or the name of the organization unit in the *Certificate* is inaccurate or does not correspond to an operating unit or
- Not use the *Certificate* when the following are inaccurate or incorrect:
  - any of the data referring to their status as person in charge with sufficient authority in the organization unit indicated in the *Certificate* or
  - the data referring to their belonging to the *Certificate Subscriber* administrative body
  - any other data showing their relationship with the organization unit or administration body indicated in the *Certificate*

256. The relationship between the FNMT-RCM and the signatory/custodian shall be primarily determined, for the purpose of use of the *Certificates* by the document related to the conditions of use or, as the case may be, issue contract of the *Certificate* and in compliance with the agreements or document of relationship between the FNMT-RCM and body or public entity.

257. The rest of the *Electronic Community* and Third Parties shall regulate their relations with the FNMT-RCM through the *General Certification Practices Statement* and; as the case may be, through these *Specific Certification Policies and Practices*; all without prejudice to that stipulated in the regulations on electronic signatures and other applicable regulations.

258. The FNMT-RCM shall not be responsible for verifying that the organization unit to be indicated in the *Certificate* belongs to the Subscriber administration body of the *Certificate* or that the *Applicant* belongs to the organization unit as person in charge of it, as this task is the responsibility of the *Registry Office*. The FNMT-RCM shall consider it representative of the body or entity of the administration *Certificate* Subscriber, unless notified otherwise by the corresponding person in charge of the *Registry Office*.

259. The FNMT-RCM shall not be liable for the use of *Certificates* issued under this *Policy* when the electronic *Certificate Subscriber* representatives act without authority or exceeding it.

14.1.5. Limits of use of the Certificates for automated administrative actions with electronic seals

260. The limits of use of this type of *Certificate*s is the creation of electronic seals of the Public Administration, body or public law entity, in accordance with Law 11/2007, of 22nd June, and Law 18/2011, of 5th July, for identification and authentication of competence for automated administrative/legal actions by the organization unit belonging to an Administration, body or public entity.

261. The FNMT-RCM and the Administration, bodies and entities may establish in the agreements or through the corresponding binding document or, if applicable in the *Issuance Law* of these *Certificate*s, other additional limits.

262. In order to be able to use the *Certificate*s for automated administrative actions within the limits outlined above and diligently, one must previously belong to the *Electronic Community* and acquire the status of *User Entity*.

263. In any case, if a third party should wish to trust an electronic signature made with one of these *Certificate*s (seal for automated actions) without accessing the validity verification services of *Certificates* issued under this *Certification Policy*, they shall not be covered by these *Specific Certification Policies and Practices*, and shall have no legitimacy whatsoever to claim or pursue legal action against the FNMT-RCM for damages or conflicts derived from the use or trust in a Certificate.

264. Moreover, even within the *Electronic Community*, this type of *Certificate*s may not be used by any individual or entity other than the FNMT-RCM, for:

- Signing another *Certificate*, unless previously and expressly authorized by the FNMT-RCM.
- Private use.
- Signing software or components.
- Generating time seals for *electronic Dating* procedures without prior and express authorization from the FNMT-RCM
- Providing services, without prior and express authorization from the FNMT-RCM free of charge or against payment as, for example:
  - Provide *OCSP* services.
  - Generate Lists of Revocation.

- And, in general, any use exceeding those identified in this section.

14.2. SPECIFIC CERTIFICATION PRACTICES FOR CERTIFICATES ISSUED FOR AUTOMATED ADMINISTRATIVE ACTIONS OF THE PUBLIC ADMINISTRATION, BODIES AND ATTACHED OR DEPENDENT PUBLIC ENTITIES

265. The FNMT-RCM as *Certification Services Provider* and to prove the necessary reliability to provide said services, has developed a *Certification Practices Statement* whose purpose is to provide public information on the general conditions for provision of certification services by the FNMT-RCM as *Certification Services Provider*.

266. Of particular note in order to interpret this annex is the "Definitions" section of the main text of the *General Certification Practices Statement*.

267. This document is derived from and is an integral part of the *General Certification Practices Statement* of the FNMT-RCM and it defines the set of specific practices adopted by the FNMT-RCM as *Certification Services Provider* for management of the lifecycle of the *Certificates* for *automated administrative actions of the Public Administration, Bodies and attached or dependent public entities* issued under the *Certificate* Certification Policy for *automated administrative actions by the Public Administration, Bodies and attached or dependent public entities* identified with OID 1.3.6.1.4.1.5734.3.3.3.2

14.2.1. *Key* Management Services

268. Under no circumstance shall the FNMT-RCM generate or store *Private Keys* for *Signatories and/or representatives*, generated under their exclusive control and whose custody is under their responsibility.

14.2.2. Certificate Lifecycle Management

14.2.2.1. Registration of Subscribers

269. Prior to establishing any institutional relationship with the *Subscribers*, the FNMT-RCM shall inform through the means and websites mentioned in these *Specific Certification Practices* and, subsidiarity, in the *General Certification Practices Statement*, on the service conditions as well as the obligations, guarantees and liabilities of the parties involved in the issue and use of the *Certificates* issued by them as *Certification Services Provider*.

270. The FNMT-RCM as *Certification Services Provider*, through the *Registry Offices* identifies *applicants* and future *Subscribers* applying for *Certificates* for automated administrative actions of the Public Administration, Bodies and attached or dependent public entities through the procedures set up for this purpose. The FNMT-RCM shall consider competent any application coming from the person in charge of the corresponding *Registry Office*, who shall be considered a *Subscriber* representative.

271. The FNMT-RCM shall collect from the *Applicants* only that information, received from the *Registry Office*, which is necessary to issue *Certificates* and for verification of identity, legitimacy and competence of representatives, storing the legally required information for a period of fifteen (15) years, treating it with due diligence in order to comply with applicable national legislation regarding personal data protection.

272. The FNMT-RCM, given that within its activity as *Certification Services Provider* does not generate the pair of *Keys* for the *Subscribers*, provides all the mechanisms necessary during the *Certificate Application* process to enable the person in charge of the *Registry Office* and/or *Subscriber* representative to hold the *Private Key* associated to the *Public Key* to be certified.

14.2.2.2. Application Procedure for Certificate for automated administrative actions of the Public Administration

273. Below is a description of the application procedure for the *Certificate* taking the official name of the administrative units belonging to the public Administration, body or entity, who shall be the *Subscribers* of the *Certificates* for automated administrative actions, the personal data of the *Subscriber* representatives are taken, which for individuals is the same as the *Applicant*, and shall have sufficient authentication and competence to request and obtain the *Certificate*, their identity, validity of their position or job is confirmed and a document of conditions of use or a standard issue contract is formalized between the *Subscriber* representative and the FNMT-RCM, for the subsequent issue of a *Certificate* for automated administrative actions of the Public Administration.

274. For the record, the FNMT-RCM, according to the relationship of the *Applicants* submitted by the public Administration, body or entity, shall consider, under the responsibility of the corresponding bodies and/or entities acting through the *Registry Offices*, that these *Applicants* fulfil the requirements established under this Statement and, therefore, have the necessary legitimacy and competence to request and obtain the *Certificate* for automated administrative actions of the Public Administration.

275. The FNMT-RCM shall consider the persons in charge of the *Registry Office*s have sufficient authority and competence to request the *Certificate*, as well as to carry out the procedure described.

276. The FNMT-RCM, shall not be liable, for this type of *Certificate*, for verifying:

- The authority and competence of the *Registry Office* to request a *Certificate* for automated administrative actions on behalf of the body or entity of the administration in question and *Certificate Subscriber*.
- Ownership and dependence of the organization unit to be indicated in the *Certificate* on the body or entity of the *Certificate* Subscriber administration.
- That the *Applicant* of the *Certificate* for automated administrative actions works for the administrative unit belonging to the *Certificate Subscriber* Administration, body or public entity.
- The status of the *Applicant* in charge of the organization unit to be indicated in the *Certificate* belonging to the Administration to be the *Subscriber* with sufficient legitimacy and competence to conduct this request.

277. Given that the FNMT-RCM has no legal civil servant, administrative or employment relationship with the *Applicants*, beyond the document of conditions of use or, as the case may be, issue contract, all verification shall be conducted by the *Registry Offices* set up by the body or entity of the Public Administration in question which shall correspond, in each case, to the body or entity Subscriber of the *Certificate*.

1. Pre-application

The representative of the *Subscriber,* who, usually, is the person in charge of the corresponding *Registry Office*, shall generate the *Public* or *Private Keys* linked to the *Certificate*, subsequently becoming *Signature Verification and Creation Data* respectively.

The representative and/or person in charge of the *Registry Office* prepares an electronic *Certificate* application, generally in PKCS#10 format, and enters the *Certification Services Provider*'s *website*, the FNMT-RCM, through

https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp

where a form shall be shown asking said representative to enter data of *Subscriber* body for which the *Certificate* is to be issued and which the organization unit depends on and the specific data of the *individual* as person in charge of the diligent custody of the Signature Creation Data and who will therefore be the signatory/custodian. In addition, the person in charge shall also enter the electronic application generated previously.

In response to submission of the form the FNMT-RCM shall assign and inform the person in charge of the application code to be used at the *Registry Office* upon application for the *Certificate.*

Previously, the representative and/or person in charge of the *Registry Office* and the *Subscriber* Administration shall consult the *General Certification Practices Statement* and these *Specific Certification Policies and Practices* at

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

with the conditions of use and obligations of the Parties, with the possibility of checking the scope of this Statement; all without detriment to the fact the *Subscriber* representative and/or person in charge of the *Registry Office*, and the FNMT-RCM, must subscribe the document on conditions of use or, if appropriate, the issue contract. Under no circumstance shall continuation of the pre-application procedure imply completion of the process.

When carrying out this pre-application the FNMT-RCM shall be sent the *Public Key* generated, together with the corresponding proof of possession of the *Private Key*, for subsequent issue of the *Certificate*.

Upon receiving this information, the FNMT-RCM shall check with the applicant's *Public Key* possession and matching of the pair of encryption *Keys* by the representative and/or person in charge of the *Registry Office* and the size of keys generated.

This information shall not result in the generation of a *Certificate* by the FNMT-RCM, until they receive the *Certificate* application signed by the person in charge of the *Registry Office*.

2. Confirmation of Party identities and requirements

The person in charge of the *Registry Office* shall be identified with their national identity document or substitute identification document by the FNMT-RCM, with the corresponding registration application and use of their own personal *Certificate*. FNMT-RCM shall assume that the person in charge of the *Registry Office* is exercising their competence and has sufficient power to conduct the necessary transactions to obtain this type of *Certificate*s.

a) Appearance in person of Applicant at Registry Offices

For cases other than intervention of the person in charge of the *Registry Office*, in order to obtain the *Certificate*, the person designated by the *Certificate Subscriber* shall be considered an *Applicant* with sufficient authentication and competence.

The FNMT-RCM shall consider the person in charge of the *Registry Office* with sufficient authority and competence by having been designated by the *Subscriber*.

b) Appearance in person and documentation

For cases other than intervention of the person in charge of the *Registry Office*, in order to obtain the *Certificate*, the representative of the *Subscriber, Applicant* shall appear in person and submit the data required and which prove, before the *Registry Office*:

i. their personal identity,

ii. their status as personnel working for the body or entity of the *Certificate Subscriber* Administration for the automated administrative action

iii. their status as person empowered or designated with sufficient authentication and competence in the organization unit, body or public entity to be indicated in the *Certificate* and from where the automated administrative actions are carried out.

The FNMT-RCM shall in any case accept the function and report provided by the *Registry Office* designated by the Administration. If the above points have not been proven, the *Registry Office* shall not continue processing the *Certificate* application.

c) Submission of information to the FNMT-RCM

Once the *Applicant*'s identity has been confirmed as well as the validity of the authentication and competence conditions required, the document of conditions of use shall be subscribed or, as the case may be, application contract by the *Applicant* on behalf of the *Subscriber* and/or person in charge of the *Registry Office*. The above information and documents shall be submitted, together with the application code collected during the pre-application phase, to the FNMT-RCM. Processing of all personal data shall be subject to applicable legislation.

This submission shall only take place if the *Registry Office* has authority to act as such on behalf of the body or entity of the Public Administration *Certificate* Subscriber for the automated administrative actions and if they own the organization unit to be indicated in the *Certificate* and from where the automated administrative actions shall be carried out.

Transmission of information to the FNMT-RCM shall be conducted through secure communications established for this purpose between the *Registry Office* and the FNMT-RCM.

14.2.2.3. Issue of the Certificate for automated administrative actions of the Public Administration

278. Once the FNMT-RCM has received the data of the *Subscribers*, *Applicants* and signatories/custodians, the information describing their relationship with the Public Administration, organization unit from where the automated administrative actions subject of the *Certificate* are carried out, as well as the application code obtained during the pre-application phase, the *Certificate* shall be issued.

279. Issuing a *Certificate* entails generating electronic documents confirming identification and authentication of the *Subscriber* and signatory/custodian authorized personnel of the *Registry Office* and/or *organization unit* of the acting Administration, body or attached or dependent public entity and to which *signature verification data* are linked to univocally and unequivocally to *Signature Creation Data* under the custody of said signatory/custodian.

280. *Certificates* of the FNMT-RCM may only be issued by them, as *Certification Services Provider*, there being no other entity or body authorized to issue them. The FNMT–RCM, by means of its *Electronic Signature*, authenticates the *Certificates* and confirms the identity and competence of their *Subscribers*, as well as their *Certificate Signatory* status for automated administrative action (electronic seal) and the signatory/custodian personnel in charge of management of said *Certificate* and

electronic seal, in accordance with the information received by the *Registry Office*. Moreover and in order to avoid tampering of the information included in the *Certificates*, the FNMT-RCM shall use encryption mechanisms that ensure the authenticity and integrity of the *Certificate*.

281. The FNMT-RCM shall in no case include in a *Certificate* information other than that described herein, or any circumstance, specific attribute of signatories/custodians or limits other than those contemplated in the agreements and, as the case may be, those contemplated in the corresponding *Issuance Law*.

282. In any case, the FNMT-RCM shall exercise due diligence to:

- Check that the *Certificate Applicant* or person in charge of the *Registry Office* uses the *Private Key* corresponding to the *Public Key* linked to the identity of its *Signatory*. For this the FNMT-RCM shall check that the *Private Key* and the *Public Key* match.
- Ensure the information included in the *Certificate* is based on the information provided by the *Applicant* and/or the person in charge of the corresponding *Registry Office*.
- Not ignore evident facts that may affect the *Certificate*'s reliability.
- Ensure the *DN* (Distinguished Name) assigned in the *Certificate* is unique in the whole *Public Key Infrastructure* of the FNMT-RCM.

283. To issue the Certificate the following steps shall be taken:

1. Composition of Certificate Distinguished Name (DN).

The Distinguished Name (*DN*) is made up with the data collected during the *Certificate* application process, in accordance with standard X.500, ensuring said name makes sense and is not ambiguous. Pseudonyms may not be used to identify the *Subscriber*.

The *DN* is made up of the following elements:

DN=CN, OU, OU, OU, O, C

The attribute *CN* contains the name of the *Registry Office* and/or *organization unit* of the Administration, body or public entity conducting the automated administrative action it depends on.

2. Composition of an alternative Certificate identity

The alternative identity of the Certificate as contemplated in this type of *Certificates* contains the identity of the Subscriber and the component or seal system distributed in a series of attributes. The subjectAltName extension defined in X.509 version 3 is used to provide this information.

Within said extension, the subfield directoryName is used to include a set of attributes defined by the FNMT-RCM, which include the information in question.

3. Generation of *Certificate* in accordance with the *Certificate* Profile for automated administrative action.

The *Certificate* format for the automated administrative actions issued by the FNMT- RCM under this policy, in line with standard UIT-T X.509 version 3 and in accordance with legally applicable regulations regarding *Recognized Certificates*, may be seen in the annexes to this document.

They describe the *Certificate* profiles distinguishing by issuing *Certification Authority* (always subordinated to the *Root Certification Authority* of the FNMT-RCM).

14.2.2.4. Download and installation of Certificate for automated administrative actions

284. Not later than 72 hours since the *applicant* has appeared in person at the *Registry Office*s to submit the request and once the *Certificate* has been generated and made available to the person in charge of the corresponding *Registry Office* a mechanism to download the *Certificate* at the address owned by the Administration or body, through the following link:

https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp

285. For this purpose, you must access the option "Download your Certificate".

286. During this guided process the person in charge of the *Registry Office* in the *Subscriber*'s area shall be asked to enter the NIF (Tax Identification Number) of the public body or entity conducting the pre-application process as well as the application code provided by the system upon completion of said process. If the *Certificate* has not been generated yet for any reason, you shall be notified of this fact when you attempt to download it.

287. If the *Certificate* has already been made available to the personnel working for public administrations *or the Registry Office*, it shall be directly entered in the format in which the *Keys* were generated during the preapplication process.

14.2.2.5. Validity of the Certificate for automated administrative actions

14.2.2.5.1. Expiry

288. *Certificate*s for automated administrative actions issued by the FNMT-RCM shall have a validity of three (3) years from the moment the *Certificate* is issued, provided its validity is not terminated. After this period and if the *Certificate* is still active, it shall expire and whenever the Subscriber wishes to continue using the services of the Certification Services Provider a new one must be issued.

14.2.2.5.2. Termination of Certificate Validity

289. *Certificate*s for automated administrative actions issued by the FNMT-RCM shall become null in the following cases:

a) End of *Certificate* validity period.

b) Cessation of activity as *Certification Services Provider* by the FNMT-RCM, unless, with prior express consent from the *Subscriber*, the *Certificates* issued by the FNMT-RCM have been transferred to another *Certification Services Provider*.

In these two cases [a) and b)], the loss of effect of the *Certificates* shall take place the moment these circumstances occur.

c) Suspension or revocation of the *Certificate* for any of the causes contemplated in this document.

290. For the purposes listed above, it is informed that the application for a Certificate for automated administrative actions issued by the FNMT-RCM when there is another one existing in favor of the same Subscriber and belonging to the same Issue Law does not mean the revocation of the one firstly obtained.

291. The consequences of revocation or suspension of the *Certificate*, that is, termination of its validity, shall come into effect on the date the FNMT-RCM become aware of any of the determining facts and they state as such in their *Information and Inquiry Service on the Status of Certificates*.

14.2.2.6. Revocation of Certificate for automated administrative actions

14.2.2.6.1. Causes for Revocation

292. The causes admitted for revocation of a *Certificate* are listed below. The *Issuance Law* may, in addition, establish other causes for revocation, suspension and cancellation of the suspension.

293. The FNMT-RCM shall only be liable for the consequences derived from not having revoked a *Certificate* in the following cases:

- When revocation should have been carried out due to termination of the contract subscribed with the *Subscriber*.
- When the revocation has been requested by the corresponding *Registry Office* to the *Subscriber* entity or body following the procedure established for this type of *Certificates*.
- When the revocation request or the cause for the same has been notified by means of a judicial or administrative ruling.
- When causes c) to f) in this section are evidenced unequivocally, after identifying the revocation applicant.

294. Taking into account the above, causes for revocation of a *Certificate* for automated administrative actions are:

a) Revocation request by authorized persons. In all cases, this request shall be based on:

- Loss of *Certificate* physical format.
- Use by a Third Party of *Signature Creation Data*, corresponding to the *Signature Verification Data* included in the *Certificate* and linked to the *Signatory* personal identity.
- Violation or jeopardizing of confidentiality of *Signature Creation Data*.
- Non-acceptance of new conditions that may lead to issue of new *Certification Practices Statements*, within a period of one month since their publication.

b) Judicial or administrative ruling ordering so.

c) Termination or dissolution of *Subscriber* or *Signatory* legal entity.

d) End of representation of *Certificate Subscriber* representative

e) Total or partial unforeseen disability of *Subscriber*, *Signatory* or the Party being represented.

f) Inaccuracies in the data provided by the *Applicant* to obtain the *Certificate*, or alteration of the data provided to obtain the *Certificate* or modification of the circumstances verified to issue the *Certificate*, such as those related to the position or authority for representation, to the extent it were no longer in effect.

g) Violation of a substantial obligation in this *Certification Practices Statement* by the *Subscriber*, *Certificate Applicant* or by a *Registry Office* if, in the latter case, it may have had an impact on the *Certificate* issue procedure.

h) Cancellation of contract subscribed between Subscriber or their representative, and the FNMT-RCM.

i) Violation or jeopardizing of confidentiality of the *Signature Creation Data* of the FNMT-RCM, with which they sign the *Certificate*s issued.

295. Under no circumstance shall it be construed that the FNMT-RCM assumes any obligation whatsoever to verify the points listed in letters c) to f) in this section.

296. Actions representing a crime or offense which the FNMT-RCM is not aware of related to the data and/or *Certificate*, inaccuracies of the data or lack of diligence in their communication to the FNMT-RCM, shall exonerate the FNMT-RCM from liability.

14.2.2.6.2. Effects of the revocation

297. The effects of revocation or suspension of the *Certificate*, that is, termination of its validity, shall come into force on the date the FNMT-RCM has evidence of any of the determining facts and states as such in its information and inquiry Service on the status of *Certificate*s.

298. Revocation of the *Certificate*s implies, aside from their termination, end of the relationship and system of use of the *Certificate* with the FNMT-RCM.

14.2.2.6.3. Procedure for revocation of Certificates

299. The revocation request for the automated administrative action *Certificate*s may be carried out during the validity period indicated in the *Certificate*.

300. Revocation of the *Certificate*s consists of cancellation of the guarantee of identity, authenticity or other properties of the *Subscriber* and their representatives and correspondence with the associated Public Key. It implies, aside from their termination, end of the relationship and system of use of the *Certificate* with the FNMT-RCM

301. The Parties authorized to request revocation of an automated administrative action *Certificate*, based on inaccurate data, change of the same or any other cause to be assessed by the *Subscriber or the Signatory,* are:

- The Management board of the Administration, bodies or attached or dependent entities, or personas delegated. FNMT-RCM shall consider the signatories/custodians in charge of the organization unit indicated in the *Certificate* and belonging to the entity of the *Certificate Subscriber* administration, with sufficient authority and competence to request this revocation.
- The *Registry Office*, —through its person in charge— designated for this purpose, by the Administration, body or attached or dependent entity *Subscriber* of the *Certificate* to be revoked, when it detects that any of the data included in the *Certificate* is
  - incorrect, inaccurate or has changed with regard to that entered in the *Certificate* or
  - the individual, signatory/custodian of the *Certificate* does not match the ultimate person in charge or designated person of the organization unit, body or public entity included in the *Certificate* or
  - the organization unit included in the *Certificate* does not depend on the body or public entity the *Certificate Signatory* depends on.

  always within the framework of the terms and conditions regarding the revocation of the *Certificate Certification Practices Statement*.

302. Below is the procedure to be followed by the *Registry Office* to formalize the revocation request of a *Certificate*. In any case the FNMT-RCM, shall assume the Applicant is duly authorized and empowered when it is the person in charge of the corresponding *Registry Office*.

1. Appearance in person of the *Applicant* before the *Registry Office*s

   To revoke the *Certificate*, the *Applicant* with sufficient authority and empowerment, shall appear in person before a *Registry Office* designated for this purpose by the body or entity holding the *Certificate* to be revoked or it shall be conducted directly by the person in charge of the *Registry Office*.

2. Appearance in person and documentation

   Applicant shall provide the data required and proving:

   - their personal identity,
   - their personal status as working for the body or entity of the *Certificate Subscriber* Public Administration or their status as person in charge of the *Registry Office*.
   - their status as ultimate person in charge or person designated by the organization unit indicated in the *Certificate* and dependent on the administration *Subscriber* of the *Certificate* or as personnel attached to the *Registry Office* designated for said purpose by the body or entity *Subscriber* of the *Certificate* to be revoked.

   FNMT-RCM shall accept, in all cases, the function and report prepared by the *Registry Office* designated by the Administration. If the above points are not evidenced, the *Registry Office* shall not proceed with the request for the *Certificate* revocation.

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

   Without evident causes of lack of competence by the person in charge of the *Registry Office* and/or having confirmed the *Applicant* identity, validity of the conditions required from them and the revocation request document having been subscribed, the *Registry Office* shall proceed to validate the data and send them to the FNMT-RCM for the effective revocation of the *Certificate*.

   Processing of all personal data shall be subject to applicable legislation.

   This submission shall only take place if the *Registry Office* has the authority to act as such on behalf of the body or entity of the Public Administration *Subscriber* of the *Certificate* and if it is in charge of or has sufficient competence on the organisation unit included in the *Certificate*.

   This information shall be transmitted to the FNMT-RCM through secure communications established for this purpose between the *Registry Office* and the FNMT-RCM.

303. In addition, the revocation requests can be done through the phone number 902 200 616, as a 24 x 7 telephone service. The communication will be recorded and registered, as a guarantee of the application for revocation.

304. The A*pplicant* of the revocation through the telephone service shall be the *Subscriber* or his representative, and must appear as such in the *Certificate* to be revoked. For the representative, it must be the same person who acted as such at the time for applying for the *Certificate*.

305. Once the FNMT-RCM has revoked the *Certificate*, it shall publish the corresponding *List of Revoked Certificate*s in the secure Directory including the serial number of the revoked *Certificate*, the date and time and cause of revocation. *Subscriber* shall receive, through the email address used for the application, a notification about the change of the *Certificate's* validity status.

14.2.2.7. Suspension of automated administrative action Certificate

306. Suspension of the *Certificate* leaves the *Certificate* without effect for a set period of time and conditions.

307. Suspension of a *Certificate* is considered a temporary revocation of the validity of the *Certificate* therefore the procedures and entities empowered to request and process a *Certificate* revocation shall apply in the event of a suspension.

14.2.2.7.1. Causes for suspension

308. The FNMT-RCM may suspend validity of *Certificate*s upon request from the legitimate interested party or a Legal Authority or if there is ground to suspect the existence of validity termination causes for the *Certificate*s as contemplated in the "Causes for Revocation of automated administrative action *Certificate*s" section.

309. Likewise, the request for suspension may be due to an ongoing investigation or legal or administrative procedure, whose conclusion may determine that the *Certificate* is indeed affected by a cause for revocation. In these cases the FNMT-RCM, at the request of the legitimate interested party, shall suspend the validity of the *Certificate* for the period requested and, after said period, shall revoke the *Certificate* unless the FNMT-RCM is unequivocally requested by the legitimate interested party to reactivate it.

14.2.2.7.2. Effects of the suspension

310. Suspension of the *Certificate* leaves the *Certificate* without effect (terminates its validity) for a set period of time and conditions.

14.2.2.7.3. Procedure for Certificate suspension

311. Suspension of *Certificate*s, given their nature, may only be carried out by the person in charge of the corresponding *Registry Office*, although the *Signatory* may request it from the *Registry Office* in the pertinent cases.

312. Below is a description of the procedure to be followed by the *Registry Office* whereby personal data are collected, their identity is confirmed and the request for suspension of the *Certificate* is formalized by a legitimate interested party.

313. These tasks shall be carried out by the *Registry Office* of the entity or body which the *Signatory* belongs to.

314. The FNMT-RCM shall suspend the *Certificate* provisionally for a period of thirty (30) days, after which the *Certificate* shall terminate through direct revocation by the *Certification Services Provider* of the FNMT-RCM, unless the suspension has been withdrawn. Notwithstanding the above, the period contemplated for suspension of the *Certificate* may change according to any legal or administrative proceedings that may affect it.

315. If during the *Certificate* suspension period it should expire or its revocation were requested, the same consequences shall apply as for non-suspended *Certificate*s affected by termination or revocation causes.

1. The *Registry Office* of the area corresponding to the *Subscriber* body or public entity may request suspension of the *Certificate* by signing the *Certificate* suspension request form submitted either on paper or electronically.

The *Registry Office*s shall forward the processed registrations to the FNMT-RCM in order for the latter to suspend the *Certificate*. Processing of all personal data shall be subject to applicable legislation.

Once the FNMT-RCM has suspended the *Certificate*, the corresponding *List of Revocation* shall be published in the secure *Directory* with the serial number of the suspended *Certificate*, and the date and time of suspension and as cause for revocation: "suspension".

In all the above situations of the *Specific Certification Practices* requiring identification and whenever electronic identification is possible, the FNMT-RCM shall consider the functionalities contemplated for the DNI-e, in accordance with applicable legislation and the use of another *Certificate* issued by the FNMT-RCM or recognized by them.

2. Cancellation of suspension of automated administrative action *Certificate*s

Cancellation of suspension of *Certificate*s issued by the FNMT-RCM may be requested by the *Subscribers*, through their representatives, provided said request is conducted within thirty (30) days from the suspension.

The FNMT-RCM shall consider there is sufficient authority to act, for the purposes of this section, when the request is conducted through the person in charge of the corresponding *Registry Office*.

Without prejudice to the above, and in the event of operating through *Certificate Subscriber* representatives other than the person in charge of the *Registry Office*, appearance in person and/or the cancellation request shall be carried out through and/or at the *Registry Office* designated by the body or entity which the Signatory belongs to and in accordance with the FNMT-RCM criteria in force in order to ensure standardization in all cases.

For this transaction, the applicant representing the *Certificate Subscriber* with sufficient competence for the request, subject of the request, shall provide all the data required and prove their personal identity, following the procedure described above for requesting issue of *Certificate* for automated administrative actions. The FNMT-RCM shall accept the proof issued by the *Registry Office* considering that established in article 13.1, *in fine*, of Law 59/2003, of 19th December, on Electronic Signatures.

The personal data of the person in charge of the *Registry Office* or the *Subscriber* representative, once validated by the *Registry Office*, shall be sent to the FNMT-RCM through secure communications established for this purpose between the *Registry Office* and the FNMT-RCM. Processing of all personal data shall be subject to applicable legislation.

Once the data validated by the *Registry Office* requesting withdrawal of suspension have been received, the FNMT-RCM shall withdraw this *Certificate* from the *List of Revocation*, and no technical action whatsoever shall be conducted on the *Certificate* in question.

As in previous cases for identification purposes, the functionalities foreseen for the DNI-e shall be taken into account, in accordance with applicable legislation and other contemplated for Public Administrations.

14.2.2.8. Administrative automated Certificate Renewal

316. The renewal of the Certificate for the automated acting administrative is always developed releasing new keys, so the process is the same as the procurement of a new certificate.

14.2.2.9. Verification of Certificate status for automated administrative actions

317. The *Certificate Subscriber* and the user Administrations, bodies and entities belonging to the *Electronic Community* may verify the status of a *Certificate* in the manner and conditions described in this section.

318. The status of the *Certificate* for automated administrative actions may be verified either by accessing the *Lists of Revocation*, or through the *Information and Inquiry Service on the Status of Certificate*s through OCSP.

319. These services shall be available twenty-four (24) hours a day, every day of the year, except for circumstances beyond the control of FNMT-RCM or for maintenance operations. The FNMT-RCM shall notify of this situation at http://www.ceres.fnmt.es if possible at least forty-eight (48) hours in advance and shall try to resolve it within a maximum of twenty-four (24) hours.

320. The FNMT-RCM has an OCSP responder service to provide the *Information and Inquiry Service on the Status of Certificates* under the terms subscribed in the corresponding agreement, contract or *Issuance Law*.

321. The service works as follows: The OCSP server receives the OCSP request made by an *OCSP Client* registered in the system and it checks status of the *Certificates* included in it. If the request is valid, an OCSP response shall be issued informing on the current status of the *Certificates* included in the request.

322. It shall be the *user Entity*'s responsibility to obtain an *OCSP Client* to operate with the OCSP server made available by the FNMT-RCM.

323. It is the *user Entity*'s responsibility applying for the OCSP service to obtain, as the case may be, consent from *Certificate Subscriber* for which OCSP service is being requested, as well as inform you of the corresponding conditions and limitations.

324. The above is understood with the scope and limits of legislation on automated processing of personal data and in accordance with the corresponding contracts, agreements or Issuance Laws regulating the electronic certification service of the FNMT-RCM.

325. The FNMT-RCM shall not provide an *Information and Inquiry Service on the status of Certificate*s of other *Subscribers* unless established as such in agreements and/or contracts with the corresponding consent from the members of the *Electronic Community* or under the terms contemplated in the *Issuance Law*.

326. In particular, for dissemination and reliability of the systems which have these *Certificate*s, the FNMT-RCM, may provide the possibility of a member of the *Electronic Community* or a third party verifying that the *Certificate* for automated administrative actions is a valid *Certificate* issued by the FNMT-RCM, as well as other features of the same.

15. RATES

327. FNMT-RCM shall apply the rates of the Public Administrations approved by the Sub-secretary which certifications service provision depends on, or the rates agreed in the arrangement of management formalized for the purpose.

ANNEX I: IDENTIFICATION OF CERTIFICATION AUTHORITY CERTIFICATES

The Certification Authorities involved in the service use the certificates listed below for signature of certificates and CRLs:

Certification Authority Certificate "AC Public Administration"

- Distinguished Name: CN = AC Public Administration, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES

  - Hierarchy SHA1

- Serial Number: 01
- Validity Period From: Friday, 21 May 2010
- Validity Period Until: Saturday, 21 May 2022
- Digital Fingerprint (sha1): 1c:5b:fa:a3:dd:e8:c5:a4:a9:09:d1:10:37:a5:0a:ec:0b:4b:21:ec
- Digital Fingerprint (sha256):
  18:a4:3c:51:d0:81:74:c3:a6:d8:5f:1c:13:18:bd:29:09:75:3e:75:d9:1c:f6:59:9f:73:34:7b:00:70:28:90

  - Hierarchy SHA256

- Serial Number: 02
- Validity Period From: Friday, 21 May 2010
- Validity Period Until: Saturday, 21 May 2022
- Digital Fingerprint (sha1): 73:20:b5:52:7a:a9:d4:b0:26:e8:0f:9f:7a:92:e8:a4:a4:a7:24:62
- Digital Fingerprint (sha256):
  83:0f:f2:05:ae:69:48:50:59:c3:fb:23:76:a7:f2:f9:ee:1c:2a:61:de:25:9d:d0:9d:0b:b6:ad:69:f8:88:32

ANNEX II: CERTIFICATION AUTHORITY CERTIFICATE PROFILES

"AC PUBLIC ADMINISTRATION" CERTIFICATION AUTHORITY CERTIFICATE

Certification Authority certificate "AC Administración Pública"				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
1. Version		2	Yes	Integer:=2 ([RFC5280] describes certificate version. Value 2 is equal to saying that certificate is version 3 (X509v3)
2. Serial Number		Unique certificate identification number.	Yes	Integer. SerialNumber = eg: 111222. Established automatically by Certification Entity. [RFC5280]. This must be a positive "integer", not longer than 20 octets (1- 2159).
3. Signature Algorithm		Sha256withRsaEncryption	Yes	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish name		Certificate Issuing Entity (Subordinate CA)	Yes	
	4.1. Country	C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Name ("official" name of the organization) of certification services provider (certificate issuer).	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. Organization Unit	Organization unit within service provider, in charge of issuing certificate (Certification Entity) ou= FNMT-RCM ROOT AC	Yes	UTF8 String, maximum size 128 (rfc5280)
5. Validity		12 years	Yes	
6. Subject		Certificate issuing entity (Subordinate CA)	Yes	
	6.1. Country	C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements" PrintableString, size 2 (rfc5280)
	6.2. Organization	Name ("official" name of the organization) of certification services provider (certificate issuer). o=FNMT-RCM.	Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3. Organizational Unit	Organization unit within service provider, in charge of issuing certificate. ou=CERES	Yes	UTF8 String, maximum size 128 (rfc5280)
	6.4. Serial Number	Unique entity identification number, applicable according to country. In Spain, NIF (Tax Identification Number) of subscriber entity. serialNumber=Q2826004J	Yes	PrintableString, size 64 (X52G). In our case, size is 9

Certification Authority certificate "AC Administración Pública"					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	6.5. Common Name		cn=AC Administración Pública	Yes	UTF8 String, maximum size 128 (rfc528G)
7. Authority Key Identifier			Identifier of root entity public key. Means to identify public key corresponding to private key used by CA to sign certificate of this Subordinate CA	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of certificate issuer field subjectPublicKey (excluding tag, length and number of bits not used). Matches field Subject Key Identifier of root AC.
8. Subject Public Key Info			Subordinate CA public key for Public Administration, coded according to encryption algorithm. In this case RSA Encryption	Yes	Field to transport public key and identify algorithm with which key is used. Key length shall be 2048
9. Subject Key Identifier			Subordinate CA public key identifier. Means to identify certificates containing a specific public key and which helps build certification paths.	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of subject field subjectPublicKey (excluding tag, length and number of bits not used).
10. Key Usage			Use of certified keys allowed.	Yes	Standardized in standard X509 and RFC 5280
	10.1. Digital Signature		0	Yes	See X509 and RFC 5280
	10.2. Content Commitment		0	Yes	See X509 and RFC 5280
	10.3. Key Encipherment		0	Yes	See X509 and RFC 5280
	10.4. Data Encipherment		0	Yes	See X509 and RFC 5280
	10.5. Key Agreement		0	Yes	See X509 and RFC 5280
	10.6. Key Certificate Signature		1	Yes	See X509 and RFC 5280
	10.7. CRL Signature		1	Yes	See X509 and RFC 5280
11. Certificate Policies			Certification Policy	Yes	
	11.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	Yes	Complying with rfc5280: 'PolicyInformation SHOULD only contain an OID. 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/	Yes	IA5String String. URL of conditions of use

Certification Authority certificate "AC Administración Pública"					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
		11.2.2 User Notice	Subject to conditions of use included in Certification Practices Statement of FNMT-RCM (C/ Jorge Juan, 106-28009-Madrid-Spain)	Yes	UTF8 String. Maximum length 200 characters.
12. CRL Distribution Point				Yes	
	12.1. Distribution Point 1		Distribution point 1 of CRL (ARL) ldap://ldapfiimt.cert.fiimt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Yes	UTF8String Path where CRL is located (distribution point 1).
	12.2. Distribution Point 2		Distribution point 2 of CRL (ARL) http://ww.cert.fnmt.es/crls/ARLFNMTRCM.crl	Yes	UTF8String. Path of LDAP service where CRL is located (distribution point 2).
13. Authority Info Access					
	13.1. Access Method 1		Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	Protocol of certificate status online (1.3.6.1.5.5.7.48.1)
	13.2. Acces Location 1		http://ocspape.cert.fnmt.es/ocspape/OcspResponder	Yes	URL of OCSP service (not authenticated)
	13.3. Access Method 2		Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	Issuer of certificate issuing entity (Root CA) Of rfc 5280: *"the id-ad-calssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."*
	13.4. Access Location 2		http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt	Yes	Path to download additional certificates for validation of certification string. In this case the path for the FNMT-RCM root certificate.
14. Basic Constraints			This extension helps to identify whether the certification subject is a CA as well as maximum "depth" level allowed for certification strings.		
	14.1. Subject Type		CA		Subject type: Certification Authority.
	14.2. Path Length		0		A zero pathLenConstraint indicates none there may not be more intermediate CA certificates in the certification path.

Table 1 - "AC Public Administration" Certification Authority Certificate

ANNEX III: CERTIFICATE PROFILES FOR PUBLIC ADMINISTRATION PERSONNEL

"AC PUBLIC ADMINISTRATION" ON ENCRYPTION CARD FORMAT"

AP Personnel issued by the "AC Public Administration" Certification Authority in Encryption Card format and under OID 1.3.6.1.4.1.5734.3.3.4.4.1				
Field		**Content**	**Compulsory**	**Specifications**
1. Version		2	Yes	Integer:=2 ([RFC5280] describes certificate version. Value 2 equals saying the certificate is version 3 (X509v3)
2. Serial Number		Unique certificate identification number. This number is assigned randomly	Yes	Integer. SerialNumber = eg: 111222. Established automatically by the Certification Entity. [RFC5280] This shall be a positive "integer", not longer than 20 octets (1- 2159).
3. Signature Algorithm		Sha256withRsaEncryption	Yes	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Certificate issuing entity	Yes	
	4.1. Country	C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements" PrintableString, size 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). o=FNMT-RCM.	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. Organizational Unit	Organization unit within services provider, in charge of issuing certificate. ou=CERES	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.4. Serial Number	Unique entity identification number, applicable in accordance with country. In Spain, NIF of subscriber entity. serialNumber=Q2826004J	Yes	PrintableString, size 64 (X520). In our case, size is 9
	4.5. Common Name	cn=AC Administración Pública	Yes	UTF8 String, maximum size 128 (rfc5280)
5. Validity		3 años	Yes	Maximum validity limited by "Certificate Profile Identification and Signature Scheme"

AP Personnel issued by the "AC Public Administration" Certification Authority in Encryption Card format and under OID 1.3.6.1.4.1.5734.3.3.4.4.1				
Field		**Content**	**Compulsory**	**Specifications**
6. Subject		Identification/description of custodian/person in charge of certified keys	Yes	
	6.1. Country	State whose legislation rules name, which shall be "Spain" as these are public entities. C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements" PrintableString, size 2 (rfc5280)
	6.2. Organization	Name ("official" name of the organization) of Subscriber of certification services	Yes	UTF8 String, maximum size 128 (rfc5280). For example: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Description of certificate type. In this case: ou=public employee electronic certificate	Yes	
	6.4. Organizational Unit	Unit, within the Administration, where certificate subscriber works.	Optional	UTF8 String, maximum size 128 (rfc5280). For example: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN The organization unit shall be established if provided in the certificate application. Otherwise, this field shall not appear in certificate.
	6.5. Organizational Unit	Identification number of certificate subscriber (supposedly univocal) Public employee identifier.	Optional	UTF8 String, maximum size 128 (rfc5280). For example: ou=ADM5689 Identifier value of civil servant/public employee shall be established if provided in the certificate application. Otherwise this field shall not appear in certificate.
	6.6. Serial Number	DNI/NIE of public employee.	Yes	For example: serialNumber=99999999R PrintableString, size 64 (X520). In our case, size is 9
	6.7. Surname	Surnames as shown in identity document	Yes	UTF8String (rfc5280). For example: sn=ESPAÑOL ESPAÑOL
	6.8. Given Name	Given name, as shown in identity document (DNI/Passport)	Yes	UTF8String (rfc5280). For example: gn=JUAN
	6.9. Common Name	Given name and Surnames as shown in identity document and ID number	Yes	UTF8String (rfc5280). For example: cn=JUAN ESPAÑOL ESPAÑOL - DNI 99999999R

AP Personnel issued by the "AC Public Administration" Certification Authority in Encryption Card format and under OID 1.3.6.1.4.1.5734.3.3.4.4.1				
Field		**Content**	**Compulsory**	**Specifications**
7. Authority Key Identifier		Public key identifier of CA for Public Administration. Means to identify public key corresponding to private key used by CA to sign a certificate.	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of certificate issuer field subjectPublicKey (excluding tag, length and number of bits not used). Matches Subject Key Identifier field of issuing AC.
8. Subject Public Key Info		Public key associated to public employee, coded according to encryption algorithm. In this case RSA Encryption.	Yes	Field to transport public key and identify algorithm key is used with. Key length shall be 2048
9. Subject Key Identifier		Public key identifier of key subscriber or Subscriber. Means to identify certificates that contain a specific public key and helps build certification paths.	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of subject field subjectPublicKey (excluding tag , length and number of bits not used).
10. Key Usage				Standardized in standard X509 and RFC 5280
	10.1. Digital Signature	1		See X509 and RFC 5280
	10.2. Content Commitment	1		See X509 and RFC 5280
	10.3. Key Encipherment	1		See X509 and RFC 5280
	10.4. Data Encipherment	1		See X509 and RFC 5280
	10.5. Key Agreement	0		See X509 and RFC 5280
	10.6. Key Certificate Signature	0		See X509 and RFC 5280
	10.7. CRL Signature	0		See X509 and RFC 5280
11. Extended Key Usage		Improved or extended use of keys.	Yes	This extension indicates one or more purposes for which the public key certificate may be used, aside from or instead of the basic uses shown in the KeyUsage extension.
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Yes	E-mail protection
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Yes	Client authentication
	11.3. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Yes	*Necessary to conduct logon in Windows with card/token*
12. Qualified Certificate Statements				

AP Personnel issued by the "AC Public Administration" Certification Authority in Encryption Card format and under OID 1.3.6.1.4.1.5734.3.3.4.4.1					
Field			**Content**	**Compulsory**	**Specifications**
	12.1. QcCompliance		Certificate is qualified. (OID 0.4.0.1862.1.1)	Yes	Indicates that the certificate is qualified. Only if not explicit in policies shown in corresponding extension.
	12.2. QcEuRetentionPeriod		15 years (OID: 0.4.0.1862.1.3)	Yes	Number of years after certificate expiry that registry data and other relevant information is available. In this case, legislation stipulates: "Keep records in any secure medium of all information and documentation related to a recognised certificate and certification practices statements in force at the time, for at least 15 years from their issue date, in order to be able to verify signatures made with the same".
	12.3. QcSSCD		Keys generated in a DSCF (OID 0.4.0.1862.1.4)	No	Indicates that the private key corresponding to the certificate is stored in a secure signature creation device in accordance with Annex III of the European Parliament Directive 1999/93/EC, on a community framework for electronic signatures.
13. Certificate Policies			Certification Policy	Yes	
	13.1. Policy Identifier		Univocal identifier of certification policy associated to "public employee" type certificates. In this case: 1.3.6.1.4.1.5734.3.3.4.4.1	Yes	Identifier of Public Employee certificate policy -Mid-level (card)
	13.2. Policy Qualifier Id				
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	IA5String String. URL of conditions of use..
		13.2.2 User Notice	Public employee recognised certificate. Subject to conditions of use included in Certification Practices Statement of the FNMT-RCM (C/Jorge Juan 106-28009-Madrid-Spain)	Yes	UTF8 String. Maximum length 200 characters.
14. Subject Alternative Names			Identification/ description of Administrative Identity	Yes	

AP Personnel issued by the "AC Public Administration" Certification Authority in Encryption Card format and under OID 1.3.6.1.4.1.5734.3.3.4.4.1					
Field			**Content**	**Compulsory**	**Specifications**
	14.1. rfc822 Name		E-mail of public employee	Optional	For example: rfc822Name=jespanol@meh.es Contact e-mail value shall be established if provided in the certificate application. Otherwise this field shall not appear in the certificate.
	14.2. UPN		UPN (network login name) for smartcard logon.	Optional	Field devoted to include Windows smart card logon for person in charge of certificate. UPN value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.
	14.3. Directory Name		Administrative Identity	Yes	Specific fields defined by the Administration for LAECSP certificates..
		14.3.1 Type of certificate	Nature of certificate / type of certificate. ID Field/Value: 2.16.724.1.3.5.3.2.1 =public employee electronic certificate	Yes	UTF8 String.
		14.3.2 Subscriber entity	Name of entity holding the certificate. Id Field/Value: 2.16.724.1.3.5.3.2.2=< Subscriber Entity>	Yes	UTF8 String. For example: 2.16.724.1.3.5.3.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
		14.3.3 Entity NIF	Unique entity identification number (NIF) Id Field/Value: 2.16.724.1.3.5.3.2.3 =<NIF>	Yes	UTF8 String, tamaño 9. Por ejemplo: 2.16.724.1.3.5.3.2.3=Q2826004J
		14.3.4 Employee ID Card	Key subscriber-custodian identity identifier. (NIF). Id Field/Value: 2.16.724.1.3.5.3.2.4 =<NIF>	Yes	UTF8 String, size 9. For example: 2.16.724.1.3.5.3.2.4=99999999R
		14.3.5 Personnel identification number	Certificate subscriber identification number (supposedly univocal) Civil servant/public employee identification number Id Field/Value: 2.16.724.1.3.5.3.2.5 =<NRP>	Optional	UTF8 String. For example: 2.16.724.1.3.5.3.2.5=ADM12347 Civil servant/public employee identifier value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.
		14.3.6 Given name	Given name of certificate subscriber Id Field/Value: 2.16.724.1.3.5.3.2.6 =<Given name>	Yes	UTF8 String. For example: 2.16.724.1.3.5.3.2.6=JUAN

AP Personnel issued by the "AC Public Administration" Certification Authority in Encryption Card format and under OID 1.3.6.1.4.1.5734.3.3.4.4.1					
Field			**Content**	**Compulsory**	**Specifications**
		14.3.7 Surname 1	Primer apellido del suscriptor del certificado Id Campo/Valor: 2.16.724.1.3.5.3.2.7 =<Apellido 1>	Yes	UTF8 String. Por ejemplo: 2.16.724.1.3.5.3.2.7=ESPAÑOL
		14.3.8 Surname 2	Second surname of certificate subscriber Id Field/Value: 2.16.724.1.3.5.3.2.8 =<Surname 2>	Yes	UTF8 String. For example: 2.16.724.1.3.5.3.2.8=ESPAÑOL
		14.3.9 E-mail	E-mail of person in charge of the certificate. Id Field/Value: 2.16.724.1.3.5.3.2.9 =<contact e-mail>	Optional	UTF8 String, size 9. For example: 2.16.724.1.3.5.3.2.9=jespanol@meh.es Contact e-mail value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.
		14.3.10 Organization Unit	Unit, within the Administration, where certificate subscriber works. Id Field/Value: 2.16.724.1.3.5.3.2.10 =<Organization Unit>	Optional	UTF8 String. For example: 2.16.724.1.3.5.3.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Organization unit value shall be established if provided in certificate application Otherwise this field shall not appear in the certificate.
		14.3.11 Position / title	Position held by certificate subscriber in the administration. Id Field/Value: 2.16.724.1.3.5.3.2.11 =<Position/Title>	Optional	UTF8 String. For example: 2.16.724.1.3.5.3.2.11=ANALISTA DE INFORMATICA Position or title value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.
15. CRL Distribution Point			Distribution point (locator) of CRL	Yes	
	15.1. Distribution Point 1		Publication point of CRL1 http://www.cert.tfnmt.es/crls acape/CRL<xxx*>.crl *xxx: CRL identifier whole number (CRL partitioned)	Yes	UTF8String Path where CRL is located (distribution point 1)

AP Personnel issued by the "AC Public Administration" Certification Authority in Encryption Card format and under OID 1.3.6.1.4.1.5734.3.3.4.4.1				
Field		**Content**	**Compulsory**	**Specifications**
	15.2. Distribution Point 2	Publication point of CRL2. .dap://ldapape.cert.mmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMTRCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier whole number (CRL partitioned)	Yes	UTF8String. Path of LDAP service where CRL is located (distribution point 2).
16. Authority Info Access			Yes	
	16.1. Access Method 1	Access method identifier for revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	Access to OCSP service
	16.2. Acces Location 1	http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Yes	URL to access OCSP service. It is not necessary to sign OCSP requests
	16.3. Access Method 2	Access method identifier for information of additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	Certificate issuing entity issuer (Root CA) From rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Yes	Path to download additional certificates for validation of certification string. In this case the path of the FNMT-RCM root certificate.
17. Basic Contraints		This extension helps identify whether the certification subject is a CA as well as maximum "depth" level allowed for certification strings. It also helps distinguish a CA from end entities	Yes	Of rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. Subject Type	End entity (value FALSE)		No other certificate may be issued with this one

Table 2 - Certificate Profile of Personnel issued by the "AC Public Administration" Certification Authority in Encryption Card format and under OID 1.3.6.1.4.1.5734.3.3.4.4.1

"AC PUBLIC ADMINISTRATION" IN SOFTWARE FORMAT"

AP Personnel issued by the "AC Public Administration" Certification Authority in software format and under OID 1.3.6.1.4.1.5734.3.3.4.4.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
1. Version		2	Yes	Integer:=2 ([RFC5280] describes certificate version. Value 2 equals saying that the Certificate is version 3 (X509v3)
2. Serial Number		Unique certificate identification number This number is assigned randomly.	Yes	Integer. SerialNumber = eg: 111222. Established automatically by Certification Entity. [RFC5280] This must be a positive "integer", not longer than 20 octets (1- 2159).
3. Signature Algorithm		Sha256withRsaEncryption	Yes	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Certificate issuing entity	Yes	
	4.1. Country	C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements" PrintableString, size 2 (rfc5280)
	4.2. Organization	Name ("official" name of the organization) of certification services provider (certificate issuer). o=FNMT-RCM.	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. Organizational Unit	Organization Unit within services provider, in charge of issuing certificate. ou=CERES	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.4. Serial Number	Unique identification number of the entity, applicable according to the country. In Spain, NIF of subscriber entity. serialNumber=Q2826004J	Yes	PrintableString, size 64 (X520). In our case, size is 9
	4.5. Common Name	cn=AC Administración Pública	Yes	UTF8 String, maximum size 128 (rfc5280)
5. Validity		3 years	Yes	Maximum validity limited by "Certificate Profile Identification and Signature Scheme"
6. Subject		Identification/description of custodian/person in charge of certified keys	Yes	
	6.1. Country	State whose legislation rules name, which shall be "Spain" as these are public entities C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements" PrintableString, size 2 (rfc5280)

AP Personnel issued by the "AC Public Administration" Certification Authority in software format and under OID 1.3.6.1.4.1.5734.3.3.4.4.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	6.2. Organization	Name ("official" name of the organization) of Subscriber of certification services	Yes	UTF8 String, maximum size 128 (rfc5280). For example: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Description of certificate type. In this case: ou=public employee electronic certificate	Yes	
	6.4. Organizational Unit	Unit, within the Administration, where certificate subscriber works..	Optional	UTF8 String, maximum size 128 (rfc5280). For example: ou=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Organization Unit value shall be established if provided in certificate application. Otherwise this field shall not appear in certificate.
	6.5. Organizational Unit	Identification number of certificate subscriber (supposedly univocal) Public employee identifier.	Optional	UTF8 String, maximum size 128 (rfc5280). For example: ou=ADM5689 Identifier value of civil servant/public employee shall be established if provided in the certificate application. Otherwise this field shall not appear in certificate.
	6.6. Serial Number	DNI/NIE of public employee.	Yes	For example: serialNumber=99999999R PrintableString, size 64 (X520). In our case, size is 9
	6.7. Surname	Surnames as shown in identity document	Yes	UTF8String (rfc5280). For example: sn=ESPAÑOL ESPAÑOL
	6.8. Given Name	Given name, as shown in identity document (DNI/Passport)	Yes	UTF8String (rfc5280). For example: gn=JUAN
	6.9. Common Name	Given name and Surnames as shown in identity document and ID number	Yes	UTF8String (rfc5280). For example: cn=JUAN ESPAÑOL ESPAÑOL - DNI 99999999R
7. Authority Key Identifier		Public key identifier of CA for Public Administration. Means to identify public key corresponding to private key used by CA to sign a certificate.	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of certificate issuer field subjectPublicKey (excluding tag, length and number of bits not used). Matches Key Identifier Subject field of issuing AC.

AP Personnel issued by the "AC Public Administration" Certification Authority in software format and under OID 1.3.6.1.4.1.5734.3.3.4.4.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
8. Subject Public Key Info		Public key associated to public employee, coded according to encryption algorithm. In this case RSA Encryption.	Yes	Field to transport public key and identify algorithm key is used with. Key length shall be 2048
9. Subject Key Identifier		Public key identifier of key subscriber or Signatory. Means to identify certificates that contain a specific public key and helps build certification paths.	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of subject field subjectPublicKey (excluding tag, length and number of bits not used).
10. Key Usage				Standardized in standard X509 and RFC 5280
	10.1. Digital Signature	1		See X509 and RFC 5280
	10.2. Content Commitment	1		See X509 and RFC 5280
	10.3. Key Encipherment	1		See X509 and RFC 5280
	10.4. Data Encipherment	1		See X509 and RFC 5280
	10.5. Key Agreement	0		See X509 and RFC 5280
	10.6. Key Certificate Signature	0		See X509 and RFC 5280
	10.7. CRL Signature	0		See X509 and RFC 5280
11. Extended Key Usage		Improved or extended use of keys.	Yes	This extension indicates one or more purposes for which the public key certificate may be used, aside from or instead of the basic uses shown in the KeyUsage extension.
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Yes	E-mail protection
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2	Yes	Client authentication
	11.3. Microsoft Smart Card Logon	1.3.6.1.4.1.311.20.2.2	Yes	*Necessary to conduct logon inWindows with card/token*
12. Qualified Certificate Statements				
	12.1. QcCompliance	Certificate is qualified. (OID 0.4.0.1862.1.1)	Yes	Indicates that the certificate is qualified. Only if not explicit in policies shown in corresponding extension..

AP Personnel issued by the "AC Public Administration" Certification Authority in software format and under OID 1.3.6.1.4.1.5734.3.3.4.4.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	12.2. QcEuRetentionPeriod		15 years (OID: 0.4.0.1862.1.3)	Yes	Number of years after certificate expiry that registry data and other relevant information is available. In this case, legislation stipulates: "Keep records in any secure medium of all information and documentation related to a recognised certificate and certification practices statements in force at the time, for at least 15 years from their issue date, in order to be able to verify signatures made with the same".
13. Certificate Policies					
	13.1. Policy Identifier		Univocal identifier of certification policy associated to "public employee" type certificates. In this case: 1.3.6.1.4.1.5734.3.3.4.4.2	Yes	Identifier of Public Employee certificate policy Mid-level (software)
	13.2. Policy Qualifier Id				
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	IA5String String. URL of conditions of use.
		13.2.2 User Notice	Public employee recognised certificate. Subject to conditions of use included in Certification Practices Statement of the FNMT-RCM (C/Jorge Juan 106-28009-Madrid-Spain)	Yes	UTF8 String. Maximum length 200 characters.
14. Subject Alternative Names			Identification/ description of Administrative Identity	Yes	
	14.1. rfc822 Name		E-mail of public employee	Optional	For example: rfc822Name=jespanol@meh.es Contact e-mail value shall be established if provided in the certificate application. Otherwise this field shall not appear in the certificate.
	14.2. UPN		UPN (network login name) for smartcard logon.	Optional	Field devoted to include Windows smart card logon for person in charge of certificate. UPN value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.
	14.3. Directory Name		Administrative Identity	Yes	Specific fields defined by the Administration for LAECSP certificates.

AP Personnel issued by the "AC Public Administration" Certification Authority in software format and under OID 1.3.6.1.4.1.5734.3.3.4.4.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
		14.3.1 Type of certificate	Nature of certificate / type of certificate. ID Field/Value: 2.16.724.1.3.5.3.2.1 = public employee electronic certificate	Yes	UTF8 String.
		14.3.2 Subscriber entity	Name of entity holding the certificate. Id Field/Value: 2.16.724.1.3.5.3.2.2=< Subscriber Entity>	Yes	UTF8 String. For example: 2.16.724.1.3.5.3.2.2=MINISTERIO DE ECONOMÍA Y HACIENDA
		14.3.3 Entity NIF	Unique entity identification number (NIF) Id Field/Value: 2.16.724.1.3.5.3.2.3 =<NIF>	Yes	UTF8 String, size 9. For example: 2.16.724.1.3.5.3.2.3=Q2826004J
		14.3.4 Employee ID Card	Key subscriber-custodian identity identifier. (NIF). Id Field/Value: 2.16.724.1.3.5.3.2.4 =<NIF>	Yes	UTF8 String, size 9. For example: 2.16.724.1.3.5.3.2.4=99999999R
		14.3.5 Personal identification number	Certificate subscriber identification number (supposedly univocal) Civil servant/public employee identification number Id Field/Value: 2.16.724.1.3.5.3.2.5 =<NRP>	Optional	UTF8 String. For example: 2.16.724.1.3.5.3.2.5=ADM12347 Civil servant/public employee identifier value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.
		14.3.6 Given name	Given name of certificate subscriber Id Field/Value: 2.16.724.1.3.5.3.2.6 =<Given name>	Yes	UTF8 String. For example: 2.16.724.1.3.5.3.2.6=JUAN
		14.3.7 Surname 1	First surname of certificate subscriber. Id Field/Value: 2.16.724.1.3.5.3.2.7 =<Surname 1>	Yes	UTF8 String. For example: 2.16.724.1.3.5.3.2.7=ESPAÑOL
		14.3.8 Surname 2	Second surname of certificate subscriber. Id Field/Value: 2.16.724.1.3.5.3.2.8 =<Surname 2>	Yes	UTF8 String. For example: 2.16.724.1.3.5.3.2.7=ESPAÑOL
		14.3.9 E-mail	E-mail of person in charge of the certificate. Id Field/Value: 2.16.724.1.3.5.3.2.9 =<contact e-mail>	Optional	UTF8 String, size 9. For example: 2.16.724.1.3.5.3.2.9=jespanol@meh.es Contact e-mail value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.

AP Personnel issued by the "AC Public Administration" Certification Authority in software format and under OID 1.3.6.1.4.1.5734.3.3.4.4.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
		14.3.10 Organization Unit	Unit, within the Administration, where certificate subscriber works. Id Field/Value: 2.16.724.1.3.5.3.2.10 =<Organization Unit>	Optional	UTF8 String. For example: 2.16.724.1.3.5.3.2.10=SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN Organization unit value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.
		14.3.11 Position / title	Position held by certificate subscriber in the administration. Id Field/Value: 2.16.724.1.3.5.3.2.11 =<Position/Title>	Optional	UTF8 String. For example: 2.16.724.1.3.5.3.2.11=ANALISTA DE INFORMATICA Position or title value shall be established if provided in certificate application. Otherwise this field shall not appear in the certificate.
15. CRL Distribution Point			Distribution point (locator) of CRL	Yes	
	15.1. Distribution Point 1		Publication point of CRL1 ittpy/www.cert.fnmt.es/crlsacape/CRL<xxx*>.crl *xxx: CRL identifier whole number (CRL partitioned)	Yes	UTF8String Path where CRL is located (distribution point 1).
	15.2. Distribution Point 2		Publication point of CRL2. dap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;bmary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier whole number (CRL partitioned)	Yes	UTF8String. Path of LDAP service where CRL is located (distribution point 2).
16. Authority Info Access				Yes	
	16.1. Access Method 1		Access method identifier for revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	Access to OCSP service
	16.2. Acces Location 1		http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Yes	URL to access OCSP service. It is not necessary to sign OCSP requests

AP Personnel issued by the "AC Public Administration" Certification Authority in software format and under OID 1.3.6.1.4.1.5734.3.3.4.4.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	16.3. Access Method 2	Access method identifier for information of additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	Certificate issuing entity issuer (Root CA) Of rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Yes	Path to download additional certificates for validation of certification string. In this case the path of the FNMT-RCM root certificate.
17. Basic Contraints		This extension helps identify whether the certification subject is a CA as well as maximum "depth" level allowed for certification strings. It also helps distinguish a CA from end entities.	Yes	Of rf5280: "*This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	17.1. Subject Type	End entity (value FALSE)		No other certificate may be issued with this one

Table 3 - Certificate Profile: APE Personnel issued by the "AC Public Administration" Certification Authority in Software format and under OID 1.3.6.1.4.1.5734.3.3.4.4.2

ANNEX IV: CERTIFICATE PROFILES FOR IDENTIFICATION OF ELECTRONIC VENUSES

Electronic venue issued by the "AC Public Administration" Certification Authority under OID 1.3.6.1.4.1.5734.3.3.2.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
1. Version		2	Yes	Integer:=2 ([RFC5280] describes certificate version. Value 2 is equal to saying certificate is version 3 (X509v3)
2. Serial Number		Unique certificate identification number. This number is assigned randomly.	Yes	Integer. SerialNumber = eg: 111222. Established automatically by Certification Entity. [RFC5280]. This must be a positive "integer", no longer than 20 octets (1- 2159).
3. Signature Algorithm		Sha256withRsaEncryption	Yes	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entity issuing certificate (Subordinate CA)	Yes	
	4.1. Country	C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements" PrintableString, size 2 (rfc5280)
	4.2. Organization	Name ("official" name of the Organization) of certification services provider (certificate issuer). o=FNMT-RCM.	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. Organizational Unit	Organization Unit within services provider, in charge of issuing certificate. ou=CERES	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.4. Serial Number	Unique entity identification number, applicable according to the country. In Spain, NIF of subscriber entity. serialNumber=Q2826004J	Yes	PrintableString, size 64 (X520). In our case, size is 9
	4.5. Common Name	cn=AC Administración Pública	Yes	UTF8 String, maximum size 128 (rfc5280)
5. Validity		3 years	Yes	Maximum validity limited by "Certificate Profile Identification and Signature Scheme"
6. Subject		Identification/description of custodian/person in charge of certified keys	Yes	
	6.1. Country	State whose legislation rules name, which shall be "Spain" as these are public entities C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements" PrintableString, size 2 (rfc5280)
	6.2. LocalityName	Subscribers locality name (organization)	Yes	UTF8String (rfc5280). For example: L=Madrid

Electronic venue issued by the "AC Public Administration" Certification Authority under OID 1.3.6.1.4.1.5734.3.3.2.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	6.3. Organization	Name ("official" name of organization) of certification services subscriber (certificate custodian)	Yes	UTF8 String, maximum size 128 (rfc5280)
	6.4. Organizational Unit	Description of type of certificate. In this case: ou=electronic venue	Yes	UTF8 String, maximum size 128 (rfc5280)
	6.5. Organizational Unit	Name describing venue.	Yes	For example: ou=Virtual Office of MEH.UTF8 String, maximum size 128 (rfc5280)
	6.6. Serial Number	Unique identification number of certification services subscriber. In this case the NIF.	Yes	For example: serialNumber=Q2826004J PrintableString, size 64 (X520). In our case, size is 9
	6.7. Common Name	Domain name (DNS or IP) where certificate is to be located and which identifies venue	Yes	For example: cn=www.meh.es UTF8 String (rfc5280)
7. Authority Key Identifier		PSC public key identifier. Means to identify public key corresponding to private key used by CA to sign a certificate.	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of certificate issuer field subjectPublicKey (excluding tag, length and number of bits not used). Matches field Subject Key Identifier of issuer AC.
8. Subject Public Key Info		Public key of venue, coded according to encryption algorithm. In this case RSA Encryption.	Yes	Field to transport public key and identify algorithm key is used with. Key length shall be 2048
9. Subject Key Identifier		Identifier of public key of key subscriber or holder Means to identify certificates containing specific private key and helps build certification paths..	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of subject field subjectPublicKey (excluding tag, length and number of bits not used).
10. Key Usage		Use of certified keys allowed.	Yes	Standardized in standard X509 and RFC 5280
	10.1. Digital Signature	1		See X509 and RFC 5280
	10.2. Content Commitment	0		See X509 and RFC 5280
	10.3. Key Encipherment	1		See X509 and RFC 5280
	10.4. Data Encipherment	0		See X509 and RFC 5280
	10.5. Key Agreement	0		See X509 and RFC 5280
	10.6. Key Certificate Signature	0		See X509 and RFC 5280
	10.7. CRL Signature	0		See X509 and RFC 5280
11. Extended Key Usage		Improved or extended use of keys	Yes	This extension indicates one or more purposes for which the public key certificate may be used, aside from or instead of the basic uses shown in the KeyUsage extension.

Electronic venue issued by the "AC Public Administration" Certification Authority under OID 1.3.6.1.4.1.5734.3.3.2.2					
Campo			**Contenido**	**Obligatoriedad**	**Especificaciones**
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Yes	Authentication TSL web Server
12. Qualified Certificate Statements			Qualified extensions.		ETSI TS 101 862 defines inclusion of certain statements for qualified certificates
	12.1. QcCompliance		Certificate is qualified. (0.4.0.1862.1.1)	Yes	Indicates that the certificate is qualified. Only if not explicit in policies shown in corresponding extension
	12.2. QcEuRetentionPeriod		15 years (OID: 0.4.0.1862.1.3)	Yes	Number of years after certificate expiry that registry data and other relevant information is available. In this case, legislation stipulates: "Keep records in any secure medium of all information and documentation related to a recognised certificate and certification practices statements in force at the time, for at least 15 years from their issue date, in order to be able to verify signatures made with the same".
	12.3. QcSSCD		Keys generated in a DSCF (OID: 0.4.0.1862.1.4)	No	Indicates that the private key corresponding to the certificate is stored in a secure signature creation device in accordance with Annex III of the European Parliament Directive 1999/93/EC, on a community framework for electronic signatures
13. Certificate Policies			Certification Policy	Yes	
	13.1. Policy Identifier		Univocal identifier of certification policy associated to "Electronic venue" type certificates. In this case: 1.3.6.1.4.1.5734.3.3.2.2	Yes	Identifier of Venue certificate policy - Mid-level.
	13.2. Policy Qualifier Id			Yes	
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	IA5String String. URL of conditions of use.
		13.2.2 User Notice	Electronic venue recognised certificate. Subject to conditions of use included in Certification Practices Statement of the DPC of the FNMT-RCM (C/Jorge Juan 106-28009-Madrid-Spain)	Yes	UTF8 String. Maximum length 200 characters.
14. Subject Alternative Names			Identification / description of Administrative Identity	Yes	

Electronic venue issued by the "AC Public Administration" Certification Authority under OID 1.3.6.1.4.1.5734.3.3.2.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	14.1. DNS Name	Domain Name (DNS) of Venue	Yes	UTF8 String, maximum size 128. Domain Name where Venue is located. For example: DNSName = www.sede.meh.gob.es
15. CRL Distribution Point		Reports how to get information on CRL associated to certificate.	Yes	
	15.1. Distribution Point 1	Publication Point of CRL1c ittpy/www.cert.fnmt.es/crls acape/CRL<xxx*>.crl*xxx: CRL identifier whole number (CRL partitioned)	Yes	UTF8String Path where CRL is located (distribution point 1).
	15.2. Distribution Point 2	Publication point of CRL2.dap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier whole number (CRL partitioned)	Yes	UTF8String. Path of LDAP service where CRL is located (distribution point 2).
16. Authority Info Access			Yes	
	16.1. Access Method 1	Access method identifier for revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	16.2. Acces Location 1	http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Yes	
	16.3. Access Method 2	Access method identifier for information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	Issuer of entity issuing certificates (Root CA) Of rfc 5280: "*the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.*"
	16.4. Access Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Yes	Path to download additional certificates for validation of certification string. In this case the FNMT-RCM root certificate path.
17. Basic Contraints		This extension allows identifying whether certification subject is a CA as well as maximum level of "'depth"' allowed for certification strings.		Of rf5280: " This extension MAY appear as a critical or non-critical extension in end entity certificates.

Electronic venue issued by the "AC Public Administration" Certification Authority under OID 1.3.6.1.4.1.5734.3.3.2.2				
Campo		**Contenido**	**Obligatoriedad**	**Especificaciones**
	17.1. Subject Type	End Entity (value FALSE)		No other certificate may be issued with this one

Table 4 - Certificate Profile of Electronic venue issued by the "AC Public Administration" Certification Authority and under OID 1.3.6.1.4.1.5734.3.3.2.2

ANNEX V: CERTIFICATE PROFILES FOR AUTOMATED ADMINISTRATIVE/LEGAL ACTIONS

Automated Administrative/Legal Action issued by the "AC Public Administration" Certification Authority and under OID 1.3.6.1.4.1.5734.3.3.3.2				
Field		**Content**	**Compulsory**	**Specifications**
1. Version		2	Yes	Integer:=2 ([RFC5280] describes certificate version. Value 2 is equal to saying certificates is version 3 (X509v3).
2. Serial Number		Unique certificate identification number. This number is assigned randomly.	Yes	Integer. SerialNumber = ej: 111222. Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1-2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption	Yes	OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Certificate issuing entity	Yes	
	4.1. Country	C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements" PrintableString, size 2 (rfc5280)
	4.2. Organization	Name ("official" name of the organization) of certification services provider (certificate issuer). o=FNMT-RCM.	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. Organizational Unit	Organization unit within services provider, in charge of issuing certificate. ou=CERES	Yes	UTF8 String, maximum size 128 (rfc5280)
	4.4. Serial Number	Unique entity identification number, applicable in accordance with country. In Spain, NIF of subscriber entity. serialNumber=Q2826004J	Yes	PrintableString, size 64 (X520). In our case, size is 9
	4.5. Common Name	cn=AC Administración Pública	Yes	UTF8 String, maximum size 128 (rfc5280)
5. Validity		3 years	Yes	Maximum validity limited by "Certificate Profile Identification and Signature Scheme"
6. Subject		Identification/description of custodian/person in charge of certified keys	Yes	
	6.1. Country	State whose legislation rules name, which shall be "Spain" as these are public entities. C=ES	Yes	To be coded according to "ISO 3166-1 -alpha-2 code elements". PrintableString, size 2 (rfc5280)

	6.2. Organization	Name ("official" name of organization) of certification services subscriber (custodian of certificate)	Yes	UTFS String, maximum size 12S (rfc52SG). For example: o=MINISTERIO DE ECONOMÍA
	6.3. Organizational Unit	Description of type of certificate. In this case: ou=electronic seal	Yes	UTFS String, maximum size 12S (rfc52SG)
	6.4. Serial Number	Unique identification number of Entity subscribing certification services. In this case NIF.	Yes	For example: serialNumber=Q2826004J PrintableString, size 64 (X520). In our case, size is 9
	6.5. Common Name	Name of automatic process system or application. This name must make sense and not be ambiguous.	Yes	UTF8String (rfc5280). For example: cn=SERVICIO DE REGISTRO DEL MEH
7. Authority Key Identifier		PSC public key identifier. Means to identify public key corresponding to private key used by CA to sign a certificate.	Yes	RFC 5280: hash SHA-1 of 20 bytes calculated on BIT STRING value of certificate issuer field subjectPublicKey (excluding tag, length and number of bits not used). Matches field Subject Key Identifier of issuer AC.
8. Subject Public Key Info		Public key of venue, coded according to encryption algorithm. In this case RSA Encryption.	Yes	Field to transport public key and identify algorithm key is used with. Key length shall be 2048.
9. Subject Key Identifier		Public key identifier of key subscriber or holder. Means to identify certificates that contain a specific public key and helps build certification paths.	Yes	RFC 5280: hash SHA-1 of 20 bytes value of subject field subjectPublicKey (excluding tag, length and number of bits not used).
10. Key Usage		Use of certified keys allowed.		Standardized in standard X509 and RFC 5280
	10.1. Digital Signature	1		See X509 and RFC 5280
	10.2. Content Commitment	1		See X509 and RFC 5280
	10.3. Key Encipherment	1		See X509 and RFC 5280
	10.4. Data Encipherment	1		See X509 and RFC 5280
	10.5. Key Agreement	0		See X509 and RFC 5280
	10.6. Key Certificate Signature	0		See X509 and RFC 5280
	10.7. CRL Signature	0		See X509 and RFC 5280
11. Extended Key Usage		Improved or extended use of keys	Yes	This extension indicates one or more purposes for which the public key certificate may be used, aside from or instead of the basic uses shown in the KeyUsage extension.
	11.1. Email protection	1.3.6.1.5.5.7.3.4	Yes	E-mail Protection
	11.2. Client Authentication	1.3.6.1.5.5.7.3.2		Client Authentication

12. Qualified Certificate Statements			Qualified Extensions.		ETSI TS 101 862 defines inclusion of certain statements for qualified certificates
	12.1. QcCompliance		Certificate is qualified (OID 0.4.0.1862.1.1)	Yes	Indicates that the certificate is qualified. Only if not explicit in policies shown in corresponding extension
	12.2. QcEuRetentionPeriod		15 years (OID: 0.4.0.1862.1.3)	Yes	Number after certificate expiry that registry data and other relevant information is available. In this case, legislation stipulates: "Keep records in any secure medium of all information and documentation related to a recognised certificate and certification practices statements in force at the time, for at least 15 years from their issue date, in order to be able to verify signatures made with the same"
	12.3. QcSSCD		Keys generated in a DSCF (OID: 0.4.0.1862.1.4)	No	Indicates that the private key corresponding to the certificate is stored in a secure signature creation device in accordance with Annex III of the European Parliament Directive 1999/93/EC, on a community framework for electronic signatures. This value shall only be entered when it is certain that the private key has been generated in a DSCF unequivocally (guaranteed by a technical mechanism or audited process)
13. Certificate Policies			Certification Policy	Yes	
	13.1. Policy Identifier		Univocal identifier of certification policy associated to "electronic seal " type certificates In this case: 1.3.6.1.4.1.5734.3.3.3.2	Yes	Identifier of seal certificate policy - Mid-Level.
	13.2. Policy Qualifier Id				
		13.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	IA5String String. URL of conditions of use.
		13.2.2 User Notice	Electronic seal recognised certificate of Administration, body or public law entity. Subject to conditions of use included in DPC of FNMT-RCM (C/Jorge Juan 106-28009-Madrid-Spain)	Yes	UTF8 String. Maximum length 200 characters.
14. Subject Alternative Names			Identification/ description of Administrative Identity	Yes	

	14.1. rfc822 Name		Venue contact e-mail (subscriber entity)	Optional	For example: rfc822Name=sellomeh@meh.es Subscriber Entity contact e-mail value shall be established if provided in the certificate application. Otherwise this value shall not be filled in.
	14.2. Directory Name		Administrative Identity	Yes	Specific fields defined by the Administration for LAECSP certificates.
		14.2.1 Type of certificate	Nature of certificate / Type of certificate. ID Field/Value: 2.16.724.1.3.5.2.2.1 =electronic seal	Yes	UTF8 String.
		14.2.2 Subscriber Entity	Name of certificate subscriber entity. Id Field/Value: 2.16.724.1.3.5.2.2.2=< Subscriber Entity>	Yes	UTF8 String. For example: 2.16.724.1.3.5.2.2.2=Ministerio de Economía y Hacienda
		14.2.3 Entity NIF	Unique entity identification number (NIF) Id Field/Value: 2.16.724.1.3.5.2.2.3 =<NIF>	Yes	UTF8 String, size 9. For example: 2.16.724.1.3.5.2.2.3=Q2826004J
		14.2.4 Name of system or component	Brief description of component associated to seal certificate. 2.16.724.1.3.5.2.2.5 =<System Name>	Yes	UTF8 String, maximum size 128. For example: 2.16.724.1.3.5.2.2.5= SERVICIO DE REGISTRO DEL MEH
15. CRL Distribution Point			Reports how to get information on CRL associated to certificate.	Yes	
	15.1. Distribution Point 1		Publication point of CRL1 http://www.cert.fnmt.es/crlsacape/CRL<xxx*>.crl *xxx: CRL identifier whole number (CRL partitioned)	Yes	UTF8String Path where CRL is located (distribution point 1).
	15.2. Distribution Point 2		Publication point of CRL2. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Administraci%F3n%20P%FAblica,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: identifier whole number (CRL partitioned)	Yes	UTF8String. Path of LDAP service where CRL is located (distribution point 2).
16. Authority Info Access				Yes	
	16.1. Access Method 1		Access method identifier for revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	Access to OCSP service
	16.2. Acces Location 1		http://ocspap.cert.fnmt.es/ocspap/OcspResponder	Yes	URL to access OCSP service. It is not necessary to sign OCSP requests

	16.3. Access Method 2	Access method identifier for information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	Issuer of certificate issuing entity (Root CA) Of rfc 5280: "the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user."
	16.4. Acces Location 2	http://www.cert.fnmt.es/certs/ACAP.crt	Yes	Path to download additional certificates for validation of certification string. In this case the path for the FNMT-RCM root certificate.
17. Basic Contraints		This extension helps to identify whether the certification subject is a CA as well as maximum "depth" level allowed for certification strings.	Yes	Of rf5280: "This extension MAY appear as a critical or non-critical extension in end entity certificates.
	17.1. Subject Type	End entity (value FALSE)		No other certificate may be issued with this one.

Table 5 - Certificate Profile of Automated Administrative Action issued by the "AC Public Administration" Certification Authority and under OID 1.3.6.1.4.1.5734.3.3.3.2