Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PARTICULAR CERTIFICATE POLICIES AND PRACTICE STATEMENT APPLICABLE TO THE CERTIFICATION AND ELECTRONIC SIGNATURE SERVICES IN THE SCOPE OF THE EUROPEAN COMMISSION

	NAME	DATE
Prepared by:	FNMT-RCM / v1.5	22/10/2014
Revised by:	FNMT-RCM / v1.5	22/10/2014
Approved by:	FNMT-RCM / v1.5	22/10/2014

HISTORY OF THE DOCUMENT			
Version	**Date**	**Description**	**Author**
1.0	15/11/2010	Creation of the document	FNMT-RCM
1.1	21/12/2010	Inclusion of new definitions. The concept of centralised *Registration Office* and *Competent Bodies are* also included	FNMT-RCM
1.1	21/12/2011	Modifications are made in order to accept names of departments in the CN of the lightweight certificates, as well as generic addresses or of groups associated with these entities	FNMT-RCM
1.1	21/02/2011	The information relating to the management of the certification policies is eliminated given that it is in the G-CPS	FNMT-RCM
1.1	21/06/2011	Updated the AIA info for the end entity certificates. New value: http://www.cert.fnmt.es/certs/ISACA.crt	FNMT-RCM
1.2	3/2/2012	Updated the tables of profiles: Certificates serial number are randomly generated	FNMT-RCM

1.3	16/4/2013	Breakdown of the server certificate policy into two large groups: web server and automated action certificates. Inclusion of two new types within the server certificate policy: - qualified certificate without a secure signature creation device for signing documents - Normalised Certificate for signing or encrypting documents Replacement of the term Holder by the term Signatory or Subscriber.	FNMT-RCM
1.4	26/09/2013	Minor corrections	FNMT-RCM
1.5	22/10/2014	Removal two types of certificates included in version 1.3	FNMT-RCM

Reference: DPC/PCPCE0105/SGPSC/2014
Document classified as: *Public*

TABLE OF CONTENTS

List of Tables:

1. DEFINITIONS AND ABBREVIATIONS

In this document the following terms shall have the following definitions:

- *Competent Authorities:* Bodies designated by any of the Member States of the European Union, any country of the EFTA (European Free Trade Association) or other country, for the exchange of information in a certain context.
- *Local Registry Authority (LRA)*: The Organization performing identification and authentication duties of the *Users* on behalf of the *Certification Services Provider.*
- *Application:* Application based on client/server technologies which require security mechanism in the "application layer" for the exchange of information between the *Competent Authority* and the institutions, agencies and entities.
- *Server Certificate*: This is the certificate used for machines to be able to act without the need for any direct intervention of a human operator in each of their operations. It contemplates two types depending on the need: *Web Server Certificates* and *Automated Action Certificates.*
- *Web server certificate:* That *Certificate* which allows a web server or a URL to be identified and authenticated.

  Within this category of *Server certificate*, the FNMT-RCM (*The Royal Spanish Mint*) issues a special type of ***Server Certificate* called a *Wildcard,*** which allows its *Subscribers*, members of the *EU Electronic Community*, to identify and authenticate all of the sub-domains associated with a certain domain, without the need to acquire and manage multiple *Certificates.*

- *"Common name" type web Server Certificate: Web Server Certificate* issued under [RFC5246] and which allows a web Server or URL to be identified and authenticated.

- *"Wildcard" type web Server Certificate: Web Server Certificate* which allows the Signatory to identify and authenticate all of the subdomains associated or derived from a certain domain name.

- *Lightweight Certificate*: *Certificate* issued under a *Certification Policy* which offers a **less burdensome** service quality than the *Certification Policy* for the issue of *Qualified Certificates* (QCP) defined in ETSI 101 456
- *Normalised Certificate*: *Certificate* issued under a *Certification Policy* which offers a quality service **equivalent** to the *Certification Policy* for the issue of *Qualified Certificates* (QCP) defined in ETSI 101 456
- *Qualified Certificate*: *Certificate* issued under a *Certification Policy* which **incorporates the requirements identified in appendix I and II** of Directive 1999/93/EC
- *OCSP Client*: Tool necessary in order to make information requests on the state of validity of the *Certificates* following the *OCSP* protocol.
- *EU Electronic Community:* Group of persons and *User Entities* which are related with *Certificates* or which trust in them and in the *Electronic Certificate* of the FNMT-RCM, under the general framework of the G-CPS (General Certification Practice Statement) and these *Certification Policies* and the specific framework, if any, of the

corresponding relationship documents (agreements, contracts, forms, etc.) which have been signed. This concept can also be referred to as “ISA (closed) Group”.

The concept of *EU Electronic Community* is exclusive of these *Policies* and is exclusive with the Electronic Community defined in G-CPS

- *G-CPS*: General Certification Practice Statement
- *User Entity*: That *Organization* which has acquired the Framework Contract formalised with the European Commission and which leads to the provision of certification services object of this document.
- *Signatory (Certificate holder)*: The individual who possesses and keeps a signature creation device and who acts (makes the signature) on behalf of the *Certificate Subscriber* in accordance with their powers.
- *FNMT-RCM (The Royal Spanish Mint)*: In the context of these *Certification Policies*, it is the *Certification Services Provider.*
- *Local Registration Authority Offices (LRA Office)*: Offices installed by the *Organization* which are set up in order to facilitate to the *Users* the presentation of applications relating to the *Certificates*, with the objective of confirming their identity and the delivery of the corresponding certificates proving personal qualities, powers of representation and other requirements required for the type of *Certificate* which is requested.
- *Organization:* The European Commission (EC) and institutions, agencies and bodies of the European Union which participate in it, as well as any other executive agency that the European Commission decides to establish in Brussels or Luxembourg.
- *QCP*: *Certification* policy for the issue of Qualified Certificates in accordance with [ETSI456]
- *Local Registration Authority Referent (LRA Referent)*: This is the person responsible for the registration operations performed by the *Organization* as *Local Registration Authority*
- *Local Registration Authority Officer (LRA Officer)*: Personnel member of the *Local Registration Authority Office (LRA Office)* expressly designated by the *Local Registration Authority Referent (LRA Referent)* to perform the registration tasks of *Certificate Users* and to manage the requests relating to them (issue, revocation, suspension and cancellation of the suspension). The activities performed by the *Local Registration Authority Officers (LRA Officer)* can also be performed by the *Local Registration Authority Referent (LRA Referent).*
- *Representatives of the Organization*: Individual who due to the position bind an *Organization* with the content of the certification provision agreement signed with the FNMT-RCM.
- *Party responsible for the server certificate:* Individual or legal entity entrusted with the management, control and safekeeping of the *server certificate,* as well as the associated *Signature Creation or Decrypting Data.*
- *SMSI*: Security Management System
- *Subject*: Contracting person with the FNMT-RCM who signs the terms and conditions of the service on behalf of the *Certificate Subscriber*
- SSL: Secure Sockets Layer

- *Subscriber* of a Certificate: This is the Organization or Competent Body whose identity is linked to the Signature certification data (Public Key) of the Subscriber and issued by the Certification Services Provider. As such the identity of the Subscriber is linked to that signed electronically using the Signature creation data (Private Key) associated to the Certificate.
- *TSL: Transport Security Layer*
- *User* of the *Information and consultation services of the state of the certificates;* Person who, not being a *User Entity,* trusts in the FNMT-RCM to provide information about the state of the *Certificates* and which accesses said services for such purpose.
- User of a *Certificate: Signatory*

2. ORGANIZATION OF THE DOCUMENTATION

1. The FNMT-RCM structures its *Certification Practice Statement* in various documents:

   - The [G-CPS] which is to provide public information about the general conditions and characteristics of the certification services by the FNMT-RCM as *Certification Services Provider*.

   - All appendices considered appropriate in order to provide public information about the conditions of use, limitations, responsibilities, properties and any other information considered specific for each type of *Certificate*. These appendices shall be considered *Particular Certificate Policies and Practice Statement* of the type of *Certificate* in question.

2. As such, the *Certification Practice Statement* of a certain type of *Certificate* issued by the FNMT-RCM is considered the set of documents made up of the G-CPS and all appendices which specify and develop the issues relating to the type of *Certificate* in question, i.e. the Particular Certificate Policies and Practice Statement of said type of *Certificate*

3. The object of this document is to provide public information about the set of practices, conditions and characteristics of the certification services provided by the FNMT-RCM as *Certification Services Provider* in relation to the lifecycle of the electronic *Certificates* for their use in the scope of competences of the *Organizations* and in the framework of the *EU Electronic Community*.

4. As such, this appendix forms an integral part of the *Certification Practice Statement* of the FNMT-RCM in relation to the *Certificates* for their use in the scope of competences of the *Organizations* and in the framework of the *EU Electronic Community*, and the *Certification Practices* used in their lifecycle.

5. In conclusion, these *Certification Policies and Practices* specify that set out in the main body of the G-CPS, with both documents making up the *Certification Practice Statement* of the FNMT-RCM in relation to the *Certificates* for their use in the scope of competences of the *Organizations* and in the framework of the *EU Electronic Community*. That described in this document is only applicable to the set of *Certificates* characterised and identified in these *Particular Certificate Policies and Practice Statement*.

3. INTRODUCTION AND SCOPE

6. This document contain the obligations and procedures that parties undertake to fulfil in relation to the provision by FNMT-RCM of services relating to a *Public Keys Infrastructure* within the scope of competences of the *Organizations* and in the framework of the *EU Electronic Community*.

7. These services, including the issue of *Certificates*, make it possible for the *User Entities, Subscribers and Users* of the *Certificates*, directly or indirectly and in certain contexts, to perform the following operations: encrypting, authentication, *Electronic Signature*, non-repudiation and identification.

8. In order that the *User Entities, Subscribers and Users* of the *Certificates* can develop remote services with the appropriate security guarantees and on the other hand benefit from anything that may be established or available, the FNMT-RCM will issue different types of *Certificates*, whose requirements, limits on use and responsibilities, scope of application and related procedures will be declared as sections in this document and are listed below:

- Certification policy for the issue of "*Lightweight Certificates*"[1]
- Certification policy for the issue of "*Normalised Certificates*"[2]
- Certification policy for the issue of "*Qualified Certificates*"[3]
- Certification policy for the issue of "*Server Certificates*"[4]

9. In particular, the "Definitions" section of the G-CPS must be taken into account in order to interpret this *Particular Certificate Policies and Practice Statement.*

[1] *Certification Policy* which offers a **less burdensome** service quality than the *Certification Policy* for the issue of *Qualified Certificates* (QCP) defined ETSI 101 456

[2] *Certification Policy* which offers an **equivalent** service quality than the *Certification Policy* for the issue of *Qualified Certificates* (QCP) defined ETSI 101 456

[3] *Certification Policy* which **incorporates the requirements identified in appendix I and II** of Directive 1999/93/EC

[4] The name "*Server Certificates*" includes the server *Certificates* of a specific domain or wildcard (various sub-domains within the same domain)

4. REFERENCES

[G-CPS] General Certification Practice Statement

[D99/93EC] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures

[D9546EC] Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[CD3602] Commission Decision of 16 August 2006 C(2006) 3602 concerning the security of information systems used by the European Commission

[ETSI456] ETSI TS 101 456: Policy requirement for certification authorities issuing qualified certificates

[ETSI042] ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates

[ETSI903] ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)

[ETSI733] ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES)

[ETSI861] ETSI TS 101 861: Time Stamping Profile

[ETSI862] ETSI TS 101 862: Qualified Certificate Profile

[ETSI158] ETSI TS 102 158: Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates

[ETSI023] ETSI TS 102 023: Policy requirements for time-stamping authorities

[ISO9594] ISO/IEC 9594-8:2005: The Directory: Public-key and attribute certificate frameworks

[RFC5280] IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC3647] IETF RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

[RFC5246] IETF RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2

5. ORDER OF PREVALENCE

10. These *Particular Certificate Policies and Practice Statement* for the *Certificates* issued for their use within the scope of competences of the *Organizations* and in the framework of the *EU Electronic Community* shall have priority, as corresponds and in particular in relation to each type of *Certificate*, over that stated in the main body of the G-CPS. As such, in the event of a contradiction between this document and the provisions of the G-CPS, that set out herein shall have preference.

11. Notwithstanding the above, the contracts, agreements, forms and conditions that are signed between the *Organization* and the FNMT-RCM or in the scope of the relations between the members of the *EU Electronic Community*, can define special features which shall have priority in the event of a disagreement.

6. Management of the lifecycle of the keys of the certification services providers

12. The FNMT-RCM in its activity as *Certification Services Provider*, in relation to the cryptographic keys used for the issue of *Certificates* and in the framework of the *EU Electronic Community*, states that it will perform the following management:

6.1. Management of the keys' lifecycle

6.1.1. Generation of the *Keys* of the *Certification Services Provider*

13. 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 authorised persons, using hardware and software systems which comply with the current cryptographic protection regulations, as shown in the G-CPS.

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

14. The FNMT-RCM uses the mechanisms necessary in order to keep its *Private key* confidential and to maintain its integrity as shown in the G-CPS.

6.1.3. Distribution of the Signature verification date of the Certification Services Provider.

15. The FNMT-RCM uses the mechanisms necessary in order to maintain the integrity and authenticity of its *Public key,* as well as its distribution as shown in the G-CPS.

16. The fields of the *Root Certificate* correspond to the certification hierarchy of the *Certificates* for their use in the scope of competences of the *Organizations* and in the scope of the *EU Electronic Community,* can be seen in appendix G-CPS.

17. On the other hand, the *Certificates* issued under the *Certification Policies* identified in this document shall be electronically signed with the *Signature Creation Data* of the *Certification Services Provider.*

18. For said issue, the FNMT-RCM uses *Signature Creation Data* which corresponds *with* its respective *Certification Authority Certificate* (in any event, subordinated to the *Root Certificate* of the FNMT-RCM identified before). This *Certificate* is defined in the appendix to this document (**Table 1 – FNMT-RCM *Root Certificate* for the issue of certificates for the European Commission (Subordinated hierarchy to the *Root Certificate* of the FNMT-RCM)**.

6.1.4. Storage, safekeeping and recovery of the Private Keys of the public user Administrations, Bodies and Entities

19. Under no circumstances does the FNMT-RCM generate or store the *Private Keys* of its *Signatories,* which are generated under their exclusive control, and are kept under the

responsibility of the different signatories and entities to which they are linked or on which they depend.

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

20. The *Signature Creation Data* of the FNMT-RCM, in its activity as *Certification Services Provider*, is used only and exclusively in order to:

1) Sign Certificates.
2) Sign Revocation Lists.
3) Other uses set out in this *Declaration* and/or in the applicable legislation.

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

21. The FNMT-RCM shall have the necessary measures in order to achieve that after the end of the valid period of the *Keys* of the *Certification Services Provider,* these *Keys* are not reused and are either destroyed or duly stored for such purpose.

6.1.7. Lifecycle of the cryptographic hardware used to sign Certificates

22. The FNMT-RCM shall have the means necessary in order to make it possible that the cryptographic hardware used to protect its *Keys* as *Certification Services Provider* does not undergo manipulation in accordance with the state of the technique on the date during its entire lifestyle, with said component being located in a secure physical environment from its reception until it is destroyed.

7. OPERATION AND MANAGEMENT OF THE PUBLIC KEY INFRASTRUCTURE

7.1. AVAILABILITY OF THE SERVICES

23. The services object of this declarative document (certificate application, registration, revocation and renewal) are monitored and control by the corresponding availability management systems.

24. The service level which is established for the activities related with the *Public Keys Infrastructure* included in this document will be:

- Twenty-four (24) hours a day, every day of the year, except due to circumstances not due to FNMT-RCM or maintenance operations which will be regularly carried out in order to ensure the continuity of the service for the *Information and consultation service of the state of validity of the Certificates* and
- For the other services on working days between 9.30 am and 5.30 pm, according to the official calendar and timetable of the *Certification Services Provider*.

25. The FNMT-RCM shall notify the infrastructure maintenance operations to the *Organizations*, agreeing with them the dates and times for its performance. It shall also report at http://www.ceres.fnmt.es, if possible at least forty-eight (48) hours in advance, and shall seek to solve it in a period of no longer than twenty-four (24) hours.

7.2. INFORMATION AND CONSULTATION SERVICE ON THE STATE OF VALIDITY OF THE CERTIFICATES

26. The FNMT-RCM shall provide the interested parties with a service to consult and obtain information about the state of the *Certificates* issued under the policies defined in this document.

27. The members of the *EU Electronic Community* can check the state of a *Certificate* as stated in this section.

28. It is understood that the *User* of the *Information and consultation service of the state of validity of the Certificates*, merely be accessing the service, accepts the conditions of the *Certification Practice Statement* and their obligations and responsibilities as parties relying on the *Certificates* issued by the FNMT-RCM and its *Electronic signature*. The FNMT-RCM, before the *User* accesses said service, shall provide them with the aforementioned conditions.

29. The *Information and consultation service of the state of validity of the Certificates* shall be offered by providing the interested party with the relevant *Revocation Lists* and via the *OCSP protocol*.

30. The FNMT-RCM has a response service as stated in the OCSP responder protocol which works as follows: The OCSP server receives the OCSP request made by an *OCSP Client* and checks the state of the *Certificates* included therein. With the information on the state of the *Certificates* it prepares a response according to the protocol and sends it to the client.

31. It is the responsibility of the interested party to obtain an *OCSP Client* in order to operate with the *OCSP* server provided by the FNMT-RCM.

7.3. MANAGEMENT OF THE SECURITY OF THE INFORMATION AND SECURITY CONTROLS

32. The operations and procedures performed in order to put into practice the *Certification Policies* contained in this document are performed following the controls required by the standards recognised for such purpose. These actions are described in the sections "Controls of physical security, procedures and personnel" and "Controls of technical security" of the G-CPS.

33. By way of information, it should be stated that the FNMT-RCM has an *Information Security Management System* (hereinafter SGSI) for its CERES Department with the end objective of maintaining and guaranteeing the security of the information so that the service provided by the FNMT-RCM has sufficient levels of reliability required by the market. The SGSI of the FNMT-RCM is applicable to the information assets defined in the Risk Analysis performed for all of the Areas in the department, including as assets the services provided and described in this document.

34. The G-CPS specifically responds to those aspects referring to the following sections of the ETSI TS 101 456 regulation:

- Security Management..
- Classification and Management of Assets.
- Personnel Security.
- Physical security and of the setting.
- Management of the Operations.
- Access Management to the System.
- Incident management and business continuity system.
- Termination of the FNMT-RCM as *Certification Services Provider*.
- Storage of the information relating to the *Qualified Certificates*.

8. DISCLOSURE OF TERMS AND CONDITIONS

35. The FNMT-RCM provides the *EU Electronic Community* and other interested parties with both this document and the G-CPS:

1) The terms and conditions which regulate the use of the *Certificates* issued by the FNMT-RCM.
2) The *Certification Policy* applicable to the *Certificates* issued by the FNMT-RCM.
3) The user limit for the *Certificates* issued under these *Certification Policies.*
4) The obligations, guarantees and responsibilities of the parties involved in the issue and use of the *Certificates*.
5) The conservation periods for the information gathered in the registration processes and from the events produced in the *Certification Services Provider* systems relating to the management of the lifecycle of the *Certificates* issued under these *Certification Policies.*
6) Legal summary of interest, with reference to the rules relating to claims and conflict resolution.

9. LIGHTWEIGHT CERTIFICATES

9.1. CERTIFICATION POLICY FOR THE ISSUE OF LIGHTWEIGHT CERTIFICATES

9.1.1. Identification

36. This *Certification Policy* of the FNMT-RCM for the issue of *Lightweight Certificates* for their use in the scope of the competences of the *Organizations* and in the framework of the *EU Electronic Community*.

Name: Certification Policy for the issue of Lightweight Certificates

Reference / OID[5]:

- 1.3.6.1.4.1.5734.3.4.3

Version: 1.0
Issue date: 15th November 2010
Location: http://www.cert.fnmt.es/dpcs/
Related DCP: General Certification Practice Statement of the FNMT-RCM
Location: http://www.cert.fnmt.es/dpcs/

9.1.2. Type of Lightweight Certificate

37. The *Lightweight Certificate* is the electronic certificate issued by the FNMT-RCM which links its *Signatory* with *Signature Verification Data* and jointly confirms:

- The identity of the signatory and safekeeping of the *Keys* and their condition of personnel in the service of the *Organization* which makes electronic signatures using the *Certificate* on behalf of the acting entity and,
- to the *Subscriber* of the *Certificate*, that it is the *Organization* or *Competent Body*.

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

39. The processes necessary for the management of this *Certificate* (issue, revocation, renewal, etc.) are performed by the FNMT-RCM via a specific PKI infrastructure, based on identification and registration actions for the network of *Registry Offices* designated by the *Organizations* who are *Subscribers* of the *Certificates.*

40. [ETSI042] identifies a series of requirements for the *Certification Policies* which, amongst others, issue *Certificates* called “Lightweight Certificate” as used in this document.

[5] *Note*: The OID or policy identifier is a reference which will be included in the *Certificate* so that the users can determine the applicable practices and procedures for the issue of the *Certificate* in question.

41. Due to the above, the requirements identified in [ETSI042] for the *Certification Policies* which issue "*Lightweight Certificates*" are satisfied in this *Policy*. It should also be indicated that the *Certificates* issued under this policy are issued with the technical profile corresponding to the *Lightweight Certificates* based on the criteria established for such *Certificates* in the [ETSI042] regulation, both as regards the *Certification Services Provider*, and to the generation of the *Signature Creation and Verification Data* and the content of the *Certificate* itself.

42. On the other hand, [ETSI042] defines the *Lightweight Certificates* as those which are issued by a *Certification Policy* which offers a **less burdensome** service quality than the *Certification Policy* for the issue of *Qualified Certificates* (QCP) defined in [ETSI456].

43. The FNMT-RCM has opted to reduce the guarantees of these *Certification Policy* for the issue of *Lightweight Certificates* as regards those defined for the *Qualified Certificates* in [ETSI046] introducing a registration service based on the authentication, at least remotely, of the *Signatory* and custody of the *Signature Creation Data*, without requiring the physical presence at the *Local Registration Authority Office (LRA Office).*

44. The details of the registration service for this *Certification Policy* are contained below in the corresponding section.

9.1.3. Community and scope of application

45. This *Certification Policy* is applicable to the issue of electronic *Certificates* which have the following characteristics:

a) They are issued by the FNMT-RCM as *Certification Services Provider* complying with the criteria established in the Spanish Electronic Signature Act 59/2003, of 19th December and in the European Electronic Signature Directive [D99/93EC]

b) They are issued as *Lightweight Certificates* based on the criteria established for them in the EESSI technical regulations, specifically in the Certification Policy for the issue of *Lightweight Certificates* identified in regulation [ETSI042] – LCP (Lightweight Certificate Policy)

c) The *Certificates* issued under this *Certification Policy* are issued for the *Organizations* which form part of the *EU Electronic Community* as defined in the Definitions section of this document. Within the framework of this *Certification Policy*, the *Users* and safe keepers of the *Signature Creation Data* correspond to the personnel of the *Organizations* in the exercise of their competences and public functions of the position, of the employee relationship, of the functions of public employee, or of the condition of person authorised by the *Organization*, in relation to the entity to which they belong or with which these *Users* are related.

9.1.4. Responsibility and obligations of the parties

46. For the purposes of this section the following shall be parties:

- The *Organizations* and *Competent Bodies* represented through the different competent bodies and who are the *Subscribers* responsible for the *Certificates*.

- *Local Registration Authority Office (LRA Office)*, which, through the personnel designated by the *Organization*, are responsible for checking the requirements and conditions held by the *Users* of the *Certificate*.
- The *Users* of the *Certificate* and its *Keys*, who will be the personnel in the service of the *Organizations*.
- FNMT-RCM, as Certification Services Provider.
- The rest of the EU Electronic Community.

47. The rights and obligations regime of the *Organization* and the FNMT-RCM is governed by the corresponding agreements regulating the certification services.

48. As well as the obligations and responsibilities of the parties listed in this document and in the G-CPS, the *Organization* as *Local Registration Authority*, the *Local Registration Authority Referent (LRA Referent)* and the *Local Registration Authority Officer (LRA Officer)* are bound to:

- Comply with the registration procedures provided by the FNMT-RCM.
- To refrain from registering or processing requests from personnel who provide their services in an *Organization* other than that which represents as *Local Registration Authority Office (LRA Office),* without prejudice to the creation in the European Commission of centralised *Local Registration Authority Offices (LRA Office)* which have been established. .
- To reliably check the data of the personnel in the service of the *Organization* regarding their identity and that they belong to said *Organization* to which it provides its services and, if applicable, any other data that reflects or characterises this belonging.
- To request the revocation or suspension of the *Lightweight Certificate* for the personnel in the service of the *Organization* which represents the *Local Registration Authority Office (LRA Office),* when any of the data in the *Certificate* is incorrect, has varied or needs to be reviewed for security reasons. It must also request the revocation or suspension under the circumstances set out in the applicable legislation.
- To request the FNMT-RCM to revoke the *Certificate* when the circumstances which affect the condition of the office, job or any other detail which reflects or characterises the relationship between the *User* of the *Certificate* with the Organization where they provide their services, are inaccurate, incorrect, have varied or must be revoked on grounds of security.
- To request from the FNMT-RCM, through the *Local Registration Authority Office (LRA Office)*, the revocation or suspension of the *Certificate* when, directly or through communication from the personnel in the service of the *Organization*, there is a loss of the support of the *Certificate* or of its confidentiality or presumption thereof.
- To safe keep the documentation provided by any of those taking part in the management processes of the *Certificates* (requests for issue, suspension, cancellation of the suspension, revocation and any others of a similar nature) as well as the documents generated in said processes (receipts, contracts of issue, revocation, etc.)

49. The relationship between the FNMT-RCM and the *Organization* and the *Users* of the *Certificates* shall be determined, for the purposes for the *Certificates'* use regime, by the following documents: conditions of use or contract of issue of the *Certificate*, and of a

subsidiary nature by these *Particular Certificate Policies and Practice Statement* and by the G-CPS, according to the relationship agreements or documents between the FNMT-RCM and the *Organizations*.

50. The relations between the *Organization or Competent Body Subscribing the Certificate* and its personnel with the FNMT-RCM shall always be performed through the *Local Registration Authority Office (LRA Office)* and its *Referent.*

51. As well as the obligations and responsibilities of the parties listed in the G-CPS, the *User of the Certificate* is bound:

- Not to use the *Certificate* when any of the details referring to the position, job or any other which led to the issue of the *Certificate* is inaccurate, incorrect or does not reflect their relationship with the *Subscribing Organization or Competent Body.*
- To perform a proper use of the *Certificate* based on the competences and powers attributed by the position, job or employment as personnel in the service of the *Organization*.
- To maintain at all times exclusive control over the *Signature Creation Data* and to take reasonable precautions in order to prevent its unauthorised loss, revelation, modification or use.
- Communicate to the corresponding *Local Registration Authority Referent (LRA Referent)* the loss, or suspicion thereof, of the support of the *Certificate* or of its confidentiality, of which it is *User* in order to start, if appropriate, the *Certificate* revocation process.

52. The rest of the *EU Electronic Community* and the third parties shall regulate their relations with the FNMT-RCM through the G-CPS and this *Particular Certificate Policies and Practice Statement*, all without prejudice to that set out in the electronic signature regulations and other applicable regulations.

9.1.5. Limits on the use of the *Lightweight Certificates*

53. Limits on the use of this type of *Certificates* are the electronic messaging systems (email) of the *Subscribing Organizations or Competent Bodies* and the data authentication and encrypting operations which may be done within them. These *Certificates* cannot be used outside of the functionality set out above.

54. The FNMT-RCM and the *Organizations* can fix additional limits in the corresponding agreements.

55. The FNMT-RCM will not have control of the acts and uses of the *Certificates* performed by the *Subscriber, User or the Local Registration Authority Office (LRA Office)*, and as such the FNMT-RCM shall be exempt from liability for such uses and the exceeding in the aforementioned use, as well as for the consequences and effects which may derive due to claims or possible asset liability performed by any member of the *EU Electronic Community* or by third parties.

56. In order that the *User* can diligently use the *Lightweight Certificates* and associated *Keys*, the *Organization* which represents the user must previous form part of the *EU Electronic Community* and having been constituted as *Subscriber of the Certificate.*

57. In any event, if a third party wishes to trust the *Electronic signature* performed with one of these *Lightweight Certificates* without accessing the *Information and consultation services on the state of validity of the certificates* issued under this *Certification Policy*, no cover shall be obtained from these *Particular Certificate Policies and Practices* and shall lack any legitimacy to claim or start legal actions against the FNMT-RCM for damages or conflicts due to using or trusting a *Certificate*.

58. Furthermore, even within the scope of the *EU Electronic Community,* this type of *Certificate* cannot be used by a person or entity other than the FNMT-RCM, to:

- Sign another *Certificate*, unless expressly authorised in advance.
- Particular or private uses
- To sign software or components
- To generate time stamps for *Time-stamping* procedures
- To prevent free or onerous services, unless expressly authorised in advance, like for example:
    - Providing OCSP services
    - Generate Revocation Lists
    - Provide notification services
- To use the *Certificate* for uses other than those initially set out for the *Lightweight Certificates*

9.2. PARTICULAR CERTIFICATION PRACTICES FOR THE LIGHTWEIGHT CERTIFICATES

59. The FNMT-RCM in its work as *Certification Services Provider* and in order to demonstrate the necessary reliability for the provision of said services, has developed a *Certification Practice Statement* with the aim of providing public information about the general conditions for the provision of certification services by the FNMT-RCM as *Certification Services Provider*.

60. The “Definitions” sector of the G-CPS and of this document must be taken into special account in order to interpret this appendix.

61. This document forms an integral part of the *Certification Practice Statement* of the FNMT-RCM and defines the set of particular practices adopted by the FNMT.RCM as *Certification Services Provider* for the management of the lifecycle of the *Lightweight Certificates* issued by the *Certification Policy* identified with the OIDs 1.3.6.1.4.1.5734.3.4.3

9.2.1. *Key* Management Services

62. Under no circumstances does the FNMT-RCM generate or store the *Private Keys* of the *Signatories,* which are generated under their exclusive control and, if applicable, with the

intervention of the corresponding *Local Registration Authority Office (LRA Office)* and whose safekeeping is under the responsibility of the *User* of the *Certificate*.

9.2.2. Management of the lifecycle of the *Certificates*

63. Here are defined those aspects which, although some have been indicated in the G-CPS, have certain special characteristics which require greater detail.

9.2.2.1. Application and issue procedure for the Lightweight Certificate

64. Below is a description of the application procedure for which the *Local Registration Authority Officer (LRA Officer)* takes the details of the personnel in the service of the *Organization*, confirms their identity and formalises, between said personnel and the FNMT-RCM, the conditions of use document or the issue contract, as set out in the agreement between the FNMT-RCM with the *Organization* for the subsequent issue of a *Lightweight Certificate*.

65. It is stated that the FNMT-RCM, according to the list of *Subscribers* and dependent *User* personnel sent by the *Local Registration Authority Office (LRA Office)*, shall consider, under the responsibility of the corresponding *Organizations or Competent Bodies* that they shall act through the *Local Registration Authority Office (LRA Office)* as *Local Registry Authority*, that this personnel has their position in force, that their personal details are authentic and in force, and therefore authorised to obtain and use the *Certificate*.

66. The European Commission can establish, within the scope of action of its competences, central or common *Registration Offices* with uniform effects for any of the different entities of the Member States.

67. FNMT-RCM, shall not have, in this type of *Certificate*, the responsibility to check the position or employment of the *User*, or that these requirements are maintain throughout the life of the *Certificate*. The FNMT-RCM does not have a functional, administrative or employment legal relationship with the *User* beyond the conditions of use document or, if applicable, the issue document.

68. The above checking activities shall be performed by the personnel of the *Local Registration Authority Office (LRA Office)* introduced by the *Organization*, which is the entity where the *User* provides their services. As such, and for these purposes, the *Local Registration Authority Office (LRA Office)* shall not be delegate or dependent authorities of the FNMT-RCM.

69. This *Certificate* shall be requested by the *Subscribing Organization or Competent Body* which shall act as applicant without prejudice to the fact that the operations necessary in order to request and obtain the *Certificate* are performed by the *Referent* or the *Local Registration Authority Officer (LRA Officer)* or, in an instrumental manner, by the *Users* themselves.

70. The three steps to be performed in order to obtain the *Certificate* are:

9.2.2.1.1. Pre-application (Step 1)

71. Beforehand, the *User* and the *Subscriber* must consult the G-CPS and these *Particular Certificate Policies and Practice Statement* at http://www.cert.fnmt.es/dpcs/ with the conditions of use and obligations as *Users* and *Subscriber*, respectively, of the *Certificate*, which are in the conditions of use document or, if applicable, the issue contract.

72. The *User* must access https://ec.fnmt.es which shows the instructions for generating *Keys.* At this webpage they must introduce their name, first surname and email address in the part for collecting data.

73. In the case that a *Lightweight Certificate* is wanted for a dependant organisational unit of the *Certificate Subscriber*, the *User* can introduce in these fields the data relating to the name of said unit. Furthermore, the mail address provided can be a generic – not personal - mailbox of said unit.

74. The *Public and Private Keys* shall then be generated and shall be linked to the *Certificate,* becoming at this time *Signature Verification and Creation Data* respectively.

75. On making this pre-application the *Public Key* generated is sent to the FNMT-RCM, together with the corresponding possession tests of the *private Key*, for the subsequent issue of the *Certificate.*

76. After the FNMT-RCM receives this information, it shall check via the *User's Public Key* the validity of the information from the signed pre-application, only checking the possession and correspondence of the pair of cryptographic *Keys by it.*

77. If everything is correct, the FNMT-RCM shall assign an application code for the request made by the *User* and shall indicate it in a response webpage.

78. This information shall not give rise to the generation of a *Certificate* by the FNMT-RCM, until the *Local Registration Authority Office (LRA Office)* receives the signed application for the *Certificate.*

9.2.2.1.2. Accreditation of the identity and application (Step 2)

79. Once the *User* has obtained the application code in the “Pre-application” sub-process it must make the corresponding *Certificate* issue request via the corresponding *Local Registration Authority Office (LRA Office)* (that which represents the *Organization* before the FNMT-RCM in the *Certificates* management operations and in which the *User* provides its services).

80. This application can be made either by physically attending or remotely. In any event, the *Local Registration Authority Officer (LRA Officer)* shall authenticate the *User* by requesting that they provide

    - Personal details (at least the name, surname, email and distinctive number of the official document) and data linked to the request in question (application code) and
    - The corresponding documentation and consisting of the official document which proves the identity of the *User.*

Note: In the case of having entered generic data in the name, surname and email address fields referring to a *Subscriber's* dependant organisational unit, the *User* must also provide documentation proving sufficient powers of representation in order to make said request on behalf of the organisational unit in question.

81. Additionally, the *Local Registration Authority Officer (LRA Officer)* shall request that the *User* provides (in person, by email or fax) a photocopy of the official document proving their identity and which contains the data referring to the identity of the *User*. These documents shall be kept by the *Local Registration Authority Office (LRA Office)* as part of the application.

82. The *Local Registration Authority Officer (LRA Officer)* shall check the *User's* condition as employee of the *Organization or Competent Body Subscribing the Certificate* and in force, as well as the accuracy of the email, all via the means available and in view of the fact that the *Local Registration Authority Office (LRA Office)* acts in representation of the *Organization* in question and therefore reliably knows this information.

83. The FNMT-RCM, shall not be responsible for checking the personal details, the condition of employee, or the email of the *User*, or that these requirements or conditions are maintained during the life of the *Certificate*, as there is no functional, administrative or employment legal relationship with the *User*, beyond the conditions of use document or, if applicable, issue contract, whose effect is strictly instrumental for the performance of the functions corresponding to the position.

84. Providing these details and documents shall guarantee the identity of the *User* and shall be a necessary and sufficient condition in order to establish the link between identity and *Signature Creation Data* which is created at the time of issue of the *Certificate*.

85. The interested party does not have to personally attend the *Local Registration Authority Office (LRA Office)* given that this *Certification Policy* has less burdensome issue conditions that those contained in [ETSI456] and also because the *Local Registration Authority Office (LRA Office)* has prior record of the data identifying the *User* as they belong to the same *Organization*. Furthermore, this form of accreditation is completely in line with the requirements established by the *Certification Policies* for the issue of "Lightweight Certificates" or LCP defined in [ETSI042].

86. Once the *Local Registration Authority Officer (LRA Officer)* confirms the identity of the *User*, that their position or employment in the *Organization* is in force and having accepted the conditions of use document or, if applicable, the application contract by the *User* and the *Local Registration Authority Office (LRA Office)*, it shall validate the data and send it to the FNMT-RCM together with the application code obtained in the pre-application step.

87. The *Local Registration Authority Office (LRA Office)* shall receive a receipt with the details of the application made and which is must keep.

88. The personal data and its processing shall be subject to the specific legislation.

89. This transfer of information to the FNMT-RCM shall be made by secure communications established for such purposes between the *Local Registration Authority Office (LRA Office)* and the FNMT-RCM.

9.2.2.1.3. Issue of the Certificate (Step 3)

90. Once the FNMT-RCM has received the personal details of the *User*, the information describing their relationship with the *Organization or Competent Body Subscribing the Certificate*, as well as the application request obtained in the pre-application step, the *Certificate* shall be issued.

91. The issue of the *Certificate* involves the generation of electronic documents which confirm the identity of the *Signatory*, their relationship with the *Organization* and their correspondence with the associated *Public Key*.

92. The issue of the *Certificates* subject to these *Policies* can only be made by the FNMT-RCM as *Certification Services Provider*, and there is no other body or entity capable of issuing them.

93. Through its *Electronic signature* the FNMT-RCM authenticates the *Certificate* and confirms the identity of the *Subscriber*, and its relationship with the *User*, in accordance with the information received by the *Local Registration Authority Office (LRA Office)*. On the other hand, and in order to avoid the manipulation of the information contained in the *Certificate*, the FNMT-RCM shall use the cryptographic mechanisms which provide authenticity and integrity to the *Certificate*.

94. In any event, the FNMT-RCM shall act effectively in order to:

- Check that the *User* of the *Certificate* uses the *Private Key* corresponding to the *Public Key* linked to the identity of its *Signatory*. For this purpose, the FNMT-RCM shall check the correspondence between the *Private* Key and the *Public Key*.
- Achieve that the information included in the *Certificate* is based on the information provided by the corresponding *Local Registration Authority Office (LRA Office)*.
- Not ignore notorious events which could affect the reliability of the *Certificate*.
- Achieve that the *DN* (distinctive name) assigned in the *Certificate* is unique throughout the *Public Keys Infrastructure* of the FNMT-RCM.

95. In order to issue the *Lightweight Certificate* the following steps shall be followed:

1. Composition of the distinctive name (DN) of the *Lightweight Certificate*

With the personal details of the *User* collected during the *Certificate* application process, the distinctive name (DN) is composed according to the *X 500* standard, ensuring that said name makes sense and does not lead to any ambiguities. Pseudonyms are not considered as a form of identification.

The *DN* for this type of *Certificates* is made up of the following elements:

DN≡CN, O, C

The attributes O, C represent the branch of the directory containing the entry corresponding to the *Lightweight Certificates* issued to the *User* in the service of the *Organization* in question.

The *CN* attribute contains the identification details of the *User* or, if applicable, the identification data of the *Certificate Subscriber's* dependant organisational unit.

The O attribute contains the name of the *Organization*.

The C attribute contains the code of the country of the *Organization*.

Once the distinctive name (*DN*) has been composed, the corresponding entry is created in the *Directory*, ensuring that the distinctive name is unique through the *Public Key Infrastructure* of the *Certification Services Provider*.

2. Composition of the *User's* alternative identity

The User's alternative identity, as considered in this type of *Certificates*, contains the email address that it provided during the pre-application and identity accreditation steps. The subjectAltName extension defined in X 509 is used to offer this information.

3. Generation of the *Certificate* according to the profile of the *Lightweight Certificate*.

The *Lightweight Certificate* format shall be in accordance with the UIT-T X.509 version 3 format and in accordance with the applicable regulations.

The profile of this type of *Certificates* can be consulted in **Table 2 – *Lightweight Certificate* Profile** attached to this document.

9.2.2.2. Publication of the Lightweight Certificate

96. Once the *Certificate* is generated by the *Certification Services Provider*, it will be published in the *Directory*, specifically in the entry corresponding to the *Organization*.

97. A communication that the *Certificate* is available for downloading will be sent to the email provided by the *User*.

9.2.2.3. Downloading and installation of the Lightweight Certificate

98. Once the *Certificate* has been generated, a downloading mechanism is made available to the *User* at

https://ec.fnmt.es

Accessing the option "Descarga de su Certificado/Download your Certificate".

99. In this guided process the interested party will be asked to enter their name, first surname and email used to process the pre-application, as well as the application code returned by the system at the end of the process.

100. If the *Certificate* has not for any reason been generated, this will be indicated when trying to download. Otherwise it will be provided to the interested party who will introduce it into the support in which the *Keys* were generated during the pre-application process.

9.2.2.4. Validity of the Lightweight Certificate

9.2.2.4.1. Expiry

101. The *Lightweight Certificates* issued under this *Certification Policy* by the FNMT-RCM shall be valid for a period of four (4) years counting from the time of issue of the *Certificate*, provided that their validity is not extinguished. After that period and if the *Certificate*

continues active, it will expire, and it shall be necessary to issue a new one if the *Subscriber* wishes to continue using the services of the *Certification Services Provider.*

9.2.2.4.2. Extinction of the validity

102. The *Lightweight Certificates* issued by the FNMT-RCM under this policy shall become without effect under the following circumstances:

a) Termination of the period of validity of the *Certificate*

b) The FNMT-RCM ceases its activity as a *Certification Services Provider*, unless, with the express prior consent of 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 when these circumstances occur.

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

103. For the purposes listed above, it is stated that the application to issue a *Lightweight Certificate* when there is another in force in favour of the same *User and Subscriber* and under the same *Certification Policy* shall lead to the revocation of the first one obtained.

104. The effects of the revocation or suspension of the *Certificate*, i.e. the extinction of its validity, shall take effect from the date on which the FNMT-RCM becomes reliably aware of any of the determining events and it is recorded in its *information and consultancy services about the state of validity of the certificates*.

9.2.2.5. Revocation of the Lightweight Certificate

9.2.2.5.1. Grounds for revoking the Lightweight Certificate

105. The following are grounds for revoking a *Lightweight Certificate:*

a) Revocation request by the authorised persons. The following shall under all circumstances lead to this request:

- The loss of the support of the *Certificate* or suspicion that its confidentiality has been compromised.
- The use by a third party of the *Signature Creation Data*, corresponding to the *Signature Verification Data* contained in the *Certificate* and linked to the identity of the *Signatory.*
- The violation or putting in danger the secrecy of the *Signature Creation Data.*
- The non-acceptance by the *Organization or Competent Body* of the new conditions which may involve the issue of new *Declarations of Certification Practices,* during the period of one month following their publication.

b) Judicial or administrative decision which orders it, as well as the cases set out in the applicable legislation.

c) Extinction or dissolution of the legal status of the *Subscriber.*

d) Termination of the relationship between the *User* and the *Organization or Competent Body Subscribing the Certificate.*

e) Clear total or partial incapacity, or death of the *User.*

f) Inaccuracies or alterations in the data provided by the *User* in order to obtain the *Certificate* or modification of the verified circumstances for its issue, as well as those relating to the position or the powers of representation, so that they are not now in accordance with the reality.

g) Breach of a substantial obligation in this *Certification Practice Statement* by the *User, the Certificate Subscriber* or the personnel of the *Local Registration Authority Office (LRA Office)* if it may affect the *Certificate* issue procedure.

h) Cancellation of the contract signed between the *Organization* and the FNMT-RCM.

i) Violation or putting in danger the secrecy of the *Signature Creation Data* of the FNMT-RCM. with which it signs the *Certificates* that it issues.

106. Under no circumstances shall it be considered that the FNMT-RCM accepts any obligation to check the points mentioned in letters c) to g) of this section.

107. The actions constituting an offence of which the FNMT-RCM becomes aware performed in relation to the data or *Certificates*, the inaccuracies in the data or lack of diligence in its communication, including the grounds mentioned above, to the FNMT-RCM, shall exempt the FNMT-RCM from liability.

9.2.2.5.2. Effects of the revocation

108. The effects of the revocation or suspension of the *Certificate*, i.e. the extinction of its validity, shall take effect from the date on which the FNMT-RCM becomes reliably aware of any of the determining events and this is thus recorded in its *Information and consultation service on the state of the validity of the certificates.*

109. The revocation of *Certificates* involves, apart from its extinction, the end of the relationship and regime of use of the *Certificate* with the FNMT-RCM.

9.2.2.5.3. Procedure for the revocation

110. The revocation application for the *Lightweight Certificates* can be made during the validity period recorded in said *Certificate.*

111. The revocation of a *Lightweight Certificate* can be requested by the *Subscriber* through the *Local Registration Authority Referent (LRA Referent)* or the *Local Registration Authority Officer (LRA Officer).* Furthermore, the *User* can request from the *Local Registration Authority Office (LRA Office)* to revoke or suspend it there are justifying grounds, under the terms contained in this *Particular Certification Policy and Practices.*

112. Without prejudice to the above, the FNMT-RCM can revoke the *Lightweight Certificates* in the cases contained in the *Certification Practice Statement* and in the applicable legislation.

113. The *User* or the *Subscriber* through a representative with sufficient capacity can request the revocation operation either personally at the corresponding *Local Registration Authority Office (LRA Office)*, or remotely. The Local Registration Authority Officer (LRA Officer)

must check the sufficient capacity of the applicant in order to carry out the revocation application.

114. In any of the cases, the applicant must prove the identity of the *User* of the *Certificate* to be revoked by providing its personal data (at least the name, first surname and email).

115. The Local Registration Authority Officer (LRA Officer) shall formalise the revocation request via registration application, which will generate two forms with the application contract, to be printed.

116. After the *Local Registration Authority Officer (LRA Officer)* confirms the identity of the applicant, that their position or employment is in force in the *Organization* and having signed the contractual forms, the *Local Registration Authority Officer (LRA Officer)* shall validate the data and send it to the FNMT-RCM.

117. The *Local Registration Authority Office (LRA Office)* must look after the forms supporting the application as part of it.

118. The FNMT-RCM shall receive that relevant information for the purposes of the revocation of a *Certificate* through the revocation application model that is presented, on paper or electronically, by the *Local Registration Authority Office (LRA Office).*

119. The *Local Registration Authority Office (LRA Office)* shall transfer the requests to the FNMT-RCM so that it can revoke the *Certificate.* The personal data and its handling shall be subject to the specific legislation.

120. FNMT-RCM shall consider that the applicant to revoke a *Certificate* of this type has sufficient capacity if the request is made through the corresponding *Local Registration Authority Office (LRA Office).* FNMT-RCM shall not assess the appropriateness of the revocation request when it is made through the aforementioned *Local Registration Authority Office (LRA Office).*

121. Once the FNMT-RCM has revoked the *Certificate,* the corresponding *List of Revoked Certificates* shall be published in the secure *Directory,* containing the series number of the revoked *Certificate,* the date and time of revocation and the reason for the revocation. Similarly, this information shall also be available via the OCSP protocol in the corresponding *Information service on the state of validity of the Certificates.*

9.2.2.6. Suspension of the Lightweight Certificate

122. The suspension of the *Certificates* shall be considered a temporary revocation of the validity of the *Certificate* and as such the authorised procedures and entities for the application and processing of the revocation of the *Certificate* are applicable in the case of suspension.

9.2.2.6.1. Grounds for the suspension of the Lightweight Certificate

123. The FNMT-RCM can suspend the validity of the *Certificates* in the event of a request from the same authorised persons and under the same conditions as for the revocation request.

124. Furthermore, the suspension request may be due to the existence of a ongoing investigation or judicial or administrative proceedings, which could conclude that the *Certificate* is effectively affected by a ground for revocation. In these cases, the FNMT-RCM, on request

from a legitimate interested party, shall suspend the validity of the *Certificate* for the requested period and, after said period has passed, shall revoke the *Certificate* unless the FNMT-RCM is reliably request by the legitimate interested party to reactivate it.

9.2.2.6.2. Effects of the suspension

125. The suspension of *Certificates* leaves the *Certificate* without effect (extinguishes its validity) during a certain period of time and under certain conditions.

9.2.2.6.3. Procedure for the suspension of Certificates

126. The procedures and authorised persons for the *Certificate* revocation application and process are applicable in the case of suspension.

127. The *Local Registration Authority Office (LRA Office)* shall transfer the applications to the FNMT-RCM so that it can proceed to the suspension of the *Certificate*. The personal data and its processing shall be subject to the specific legislation.

128. The FNMT-RCM shall suspend the *Certificate* provisionally for a period of fifteen (15) days, after which the *Certificate* shall be extinguished by its direct revocation by the *Certification Services Provider*, unless the suspension has been cancelled. Notwithstanding the above, the period established for the suspension of the *Certificate* may be altered according to the duration of the investigations or judicial or administrative proceedings which may affect it.

129. Once the FNMT-RCM has suspended the *Certificate*, the corresponding *List of Revoked Certificates* shall be published in the secure *Directory*, containing the series number of the revoked *Certificate*, the date and time of revocation and the reason for the revocation. Similarly, this information shall also be available via the OCSP protocol in the corresponding *Information service on the state of validity of the Certificates.*

130. If during the *Certificate's* suspension period it expires or its revocation is requested, the same consequences will occur as for the non-suspended *Certificates* which expire or are revoked.

9.2.2.6.4. Cancelation of the suspension of the Lightweight Certificate

131. The same legitimate persons for the suspension request can request the cancellation of the suspension of the *Lightweight Certificates*, and under the same conditions and following the same procedures.

132. The *Local Registration Authority Office (LRA Office)* shall transfer requests to the FNMT-RCM so that it can cancel the suspension of the *Certificates*, The personal data and its processing shall be subject to the specific legislation.

133. Once the data validated by the *Local Registration Authority Office (LRA Office)* of the request to lift the suspension has been received, the FNMT-RCM shall withdraw the *Certificate* in question from the *List of Revoked Certificates*, not performing any technical action over the *Certificate*.

10. NORMALISED CERTIFICATES

10.1. CERTIFICATION POLICY FOR THE ISSUE OF NORMALISED CERTIFICATES

10.1.1. Identification

134. This *Certification Policy* of the FNMT-RCM for the issue of *Normalised Certificates* for their use within the scope of the *Organizations* and in the framework of the *EU Electronic Community*. .

Name: *Certification Policy* for the issue of *Normalized Certificates*

Reference / OID:

- 1.3.6.1.4.1.5734.3.4.2

Version: 1.0

Date of issue: 15th November 2010

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

Related DCP: General Certification Practice Statement of the FNMT-RCM

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

10.1.2. Typology of the Normalised Certificate

135. The *Normalised Certificate* is the electronic certificate issued by the FNMT-RCM which links its *Signatory* with certain *Signature Verification Data* and confirms, as a whole:

- The identity of the Signatory and safekeeping of the *Keys* and their condition as personnel in the service of the *Organization* who makes electronic signatures using the *Certificate* on behalf of the acting entity and,
- The *Subscriber of the Certificate*, which is the *Organization or Competent Body*.

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

137. The process necessary in order to manage this *Certificate* (issue, revocation, renewal, etc.) are developed by the FNMT-RCM through a specific PKI infrastructure, based on identification and registration actions performed by the network of *Local Registration Authority Office (LRA Office)* designated by the *Organizations Subscribing the Certificates.*

138. [ETSI042] identifies a series of requirements for the *Certification Polices* which amongst others issue *Certificates* which are called “Normalized Lightweight Certificate”. This name is equivalent to the term *Normalised Certificate* which is used in this document.

139. Due to the above, the requirements identified in [ETSI042] for the *Certification Policies* which issue “*Normalised Certificates*” are satisfied in this *Policy*. Additionally, it is indicated that the *Certificates* issued under this policy are issued with the technical profile

corresponding to the *Normalised Certificates* based on the criteria established for such *Certificates* in regulation [ETSI042], both as regards the *Certification Services Provider*, and the generation of the *Signature Creation and Verification Data* and the content of the *Certificate itself*.

140. On the other hand, [ETIS042] defines the *Normalized Certificates* as those which are issued by a *Certification Policy* (NCP) which offers a service quality **equivalent** to the *Certification Policy* for the issue of *Qualified Certificates* (QCP) defined in [ETSI456]. Furthermore, [ETSI042] expressly recognises the validity of the NCP *Certification Policy* for cryptographic issues in order to perform authentication or data encrypting operations.

141. The *Normalised Certificates* are created to increase of limits of use and scope of application in relation to the *Qualified Certificates*, thereby facilitating the adaption of the former with other institutions, specification and standards similar to [ETSI456].

142. In this effort to harmonise and give systems shared operability, the quality level set out in Directive [D99/93EC] may be consecrated by being recognised and accepted in a much broader working framework but without being subject to its specifications.

10.1.3. Community and scope of application

143. This *Certification Policy* is applicable to the issue of electronic *Certificates* which have the following characteristics:

a) They are issued by the FNMT-RCM as *Certification Services Provider* complying with the criteria established in the Spanish Electronic Signature Act 59/2003, of 19th December and in the European Electronic Signature Directive [D99/93EC]

b) They are issued as *Normalised Certificates* based on the criteria established for them in the EESSI technical regulations, specifically in the Certification Policy for the issue of *Normalised Certificates* identified in regulation [ETSI042] – NCP (Normalised Certificate Policy)

c) The *Certificates* issued under this *Certification Policy* are issued for the *Organizations* which form part of the *EU Electronic Community* as defined in the Definitions section of this document. Within the framework of this *Certification Policy*, the *Users* and safe keepers of the *Signature Creation Data* correspond to the personnel of the *Organizations* in the exercise of their competences and public functions of the position, of the employee relationship, of the functions of public employee, or of the condition of person authorised by the *Organization*, in relation to the entity to which they belong or with which these *Users* are related.

10.1.4. Responsibility and obligations of the parties

144. For the purposes of this section the following shall be parties:

- The *Organizations or Competent Bodies* represented through the different competent bodies and who are the *Subscribers* responsible for the *Certificates*.

- *Local Registration Authority Office (LRA Office)*, which, through the personnel designated by the *Organization*, are responsible for checking the requirements and conditions held by the *Users* of the *Certificate*.
- The *Users* of the *Certificate* and its *Keys*, who will be the personnel in the service of the *Organizations*.
- FNMT-RCM, as Certification Services Provider.
- The rest of the EU Electronic Community.

145. The rights and obligations regime of the *Organization* and the FNMT-RCM is governed by the corresponding agreements regulating the certification services.

146. As well as the obligations and responsibilities of the parties listed in this document and in the G-CPS, the *Organization* as *Local Registration Authority*, the *Local Registration Authority Referent (LRA Referent)* and the *Local Registration Authority Officer (LRA Officer)* are bound to:

- Comply with the registration procedures provided by the FNMT-RCM.
- Not to make registries or process applications from personnel who provide their services in an *Organisation* other than that which represents as *Local Registration Authority*, without prejudice to the creation, in the European Commission, of centralised *Local Registration Authorities* that have been established.
- To reliably check the data of the personnel in the service of the *Organization* regarding their identity and that they belong to said *Organization* to which it provides its services and, if applicable, any other data that reflects or characterises this belonging.
- To request the revocation or suspension of the *Normalised Certificate* for the personnel in the service of the *Organization* which represents the *Local Registration Authority Office (LRA Office)*, when any of the data in the *Certificate* is It must also request the revocation or suspension under the circumstances set out in the applicable legislation.
- To request the FNMT-RCM to revoke the *Certificate* when the circumstances which affect the condition of the office, job or any other detail which reflects or characterises the relationship between the *User* of the *Certificate* with the Organization where they provide their services, are inaccurate, incorrect, have varied or must be revoked on grounds of security.
- To request from the FNMT-RCM, through the *Local Registration Authority Office (LRA Office)*, the revocation or suspension of the *Certificate* when, directly or through communication from the personnel in the service of the *Organization*, there is a loss of the support of the *Certificate* or of its confidentiality or presumption thereof.
- To safe keep the documentation provided by any of those taking part in the management processes of the *Certificates* (requests for issue, suspension, cancellation of the suspension, revocation and any others of a similar nature) as well as the documents generated in said processes (receipts, contracts of issue, revocation, etc.)

147. The relationship between the FNMT-RCM and the *Organization* and the *Users* of the *Certificates* shall be determined, for the purposes for the *Certificates'* use regime, by the following documents: conditions of use or contract of issue of the *Certificate*, and of a subsidiary nature by these *Particular Certificate Policies and Practice Statement* and by the

G-CPS, according to the relationship agreements or documents between the FNMT-RCM and the *Organizations*.

148. The relations between the *Organization or Competent Body Subscribing the Certificate* and its personnel with the FNMT-RCM shall always be performed through the *Local Registration Authority Office (LRA Office)* and its *Referent.*

149. As well as the obligations and responsibilities of the parties listed in the G-CPS, the *User of the Certificate* is bound to:

- Not use the *Certificate* when any of the details referring to the position, job or any other which led to the issue of the *Certificate* is inaccurate, incorrect or does not reflect their relationship with the *Subscribing Organization or Competent Body*.
- To perform a proper use of the *Certificate* based on the competences and powers attributed by the position, job or employment as personnel in the service of the *Organization*.
- To maintain at all times exclusive control over the *Signature Creation Data* and to take reasonable precautions in order to prevent its unauthorised loss, revelation, modification or use.
- Communicate to the corresponding *Local Registration Authority Referent (LRA Referent)* the loss, or suspicion thereof, of the support of the *Certificate* or of its confidentiality, of which it is *User* in order to start, if appropriate, the *Certificate* revocation process.

150. The rest of the *EU Electronic Community* and the third parties shall regulate their relations with the FNMT-RCM through the G-CPS and these *Particular Certificate Policies and Practice Statement*, all without prejudice to that set out in the electronic signature regulations and other applicable regulations.

10.1.5. Limits on the use of the *Normalised Certificates*

151. Limits on the use of this type of *Certificates* are the authentication operations which may be performed within the systems of the *Subscribing Organizations or Competent Bodies.* Furthermore, the *Organization* can authorise the *User* to use this type of *Certificate* as an identification and authentication tool of systems not owned by it. These *Certificates* cannot be used outside of the functionality set out above.

152. The FNMT-RCM and the *Organizations* can fix additional limits in the corresponding agreements.

153. The FNMT-RCM will not have control of the acts and uses of the *Certificates* performed by the *Subscriber, User or the Local Registration Authority Office (LRA Office)*, and as such the FNMT-RCM shall be exempt from liability for such uses and the exceeding in the aforementioned use, as well as for the consequences and effects which may derive due to claims or possible asset liability performed by any member of the *EU Electronic Community* or by third parties.

154. In order that the *User* can diligently use the *Normalised Certificates* and associated *Keys*, the *Organization* which represents the user must previous form part of the *EU Electronic Community* and having been constituted as *Subscriber of the Certificate.*

155. In any event, if a third party wishes to trust the *Electronic signature* performed with one of these *Normalised Certificates* without accessing the *Information and consultation services on the state of validity of the certificates* issued under this *Certification Policy*, no cover shall be obtained from these *Particular Certificate Policies and Practices* and shall lack any legitimacy to claim or start legal actions against the FNMT-RCM for damages or conflicts due to using or trusting a *Certificate*.

156. Furthermore, even within the scope of the *EU Electronic Community,* this type of *Certificate* cannot be used by a person or entity other than the FNMT-RCM, to:

- Sign another *Certificate*, unless expressly authorised in advance.
- Particular or private uses
- To sign software or components
- To generate time stamps for *Time-stamping* procedures
- To render services free of charge or for a consideration, unless expressly authorised in advance, such as for example:
    - Providing OCSP services
    - Generate Revocation Lists
    - Provide notification services
- To use the *Certificate* for uses other than those initially set out for the *Normalised Certificates*

10.2. PARTICULAR CERTIFICATION PRACTICES FOR THE NORMALISED CERTIFICATES

157. The FNMT-RCM in its work as *Certification Services Provider* and in order to demonstrate the necessary reliability for the provision of said services, has developed a *Certification Practice Statement* with the aim of providing public information about the general conditions for the provision of certification services by the FNMT-RCM as *Certification Services Provider*.

158. The “Definitions” sector of the G-CPS and of this document must be taken into special account in order to interpret this appendix.

159. This document forms an integral part of the *Certification Practice Statement* of the FNMT-RCM and defines the set of particular practices adopted by the FNMT-RCM as *Certification Services Provider* for the management of the lifecycle of the *Normalised Certificates* issued by the *Certification Policy* identified with the OIDs 1.3.6.1.4.1.5734.3.4.2

10.2.1. *Key* Management Services

160. Under no circumstances does the FNMT-RCM generate or store the *Private Keys* of the *Signatories*, which are generated under their exclusive control and, if applicable, with the

intervention of the corresponding *Local Registration Authority Office (LRA Office)* and whose safekeeping is under the responsibility of the *User* of the *Certificate*.

10.2.2. Management of the lifecycle of the *Certificates*

161. Here are defined those aspects which, although some have been indicated in the G-CPS, have certain special characteristics which require greater detail.

10.2.2.1. Application and issue procedure for the Normalised Certificate

162. Below is a description of the application procedure for which the *Local Registration Authority Officer (LRA Officer)* takes the details of the personnel in the service of the *Organization*, confirms their identity and formalises, between said personnel and the FNMT-RCM, the conditions of use document or the issue contract, as set out in the agreement between the FNMT-RCM with the *Organization* for the subsequent issue of a Normalised Certificate.

163. It is stated that the FNMT-RCM, according to the list of *Subscribers* and dependent *User* personnel sent by the *Local Registration Authority Office (LRA Office)*, shall consider, under the responsibility of the corresponding *Organizations*, that they shall act through the *Local Registration Authority Office (LRA Office)* as *Local Registry Authority*, that this personnel has their position in force, that their personal details are authentic and in force, and therefore authorised to obtain and use the *Certificate*.

164. The European Commission can establish, within the scope of action of its competences, central or common *Registration Authority Offices* with uniform effects for any of the different entities of the Member States.

165. FNMT-RCM, shall not have, in this type of *Certificate*, the responsibility to check the position or employment of the *User*, or that these requirements are maintain throughout the life of the *Certificate*. The FNMT-RCM does not have a functional, administrative or employment legal relationship with the *User* beyond the conditions of use document or, if applicable, the issue document.

166. The above checking activities shall be performed by the personnel of the *Local Registration Authority Office (LRA Office)* introduced by the *Organization*, which is the entity where the *User* provides their services. As such, and for these purposes, the *Local Registration Authority Office (LRA Office)* shall not be delegate or dependent authorities of the FNMT-RCM.

167. This *Certificate* shall be requested by the *Subscribing Organization or Competent Body* which shall act as applicant without prejudice to the fact that the operations necessary in order to request and obtain the *Certificate* are performed by the *Referent* or the *Local Registration Authority Officer (LRA Officer)* or, in an instrumental manner, by the *Users* themselves.

168. The three steps to be performed in order to obtain the *Certificate* are:

10.2.2.1.1. Pre-application (Step 1)

169. Beforehand, the *User* and the *Subscriber* must consult the G-CPS and these *Particular Certificate Policies and Practice Statement* at http://www.cert.fnmt.es/dpcs/ with the conditions of use and obligations as *Users* and *Subscriber*, respectively, of the *Certificate*, which are in the conditions of use document or, if applicable, the issue contract.

170. The *User* must access https://ec.fnmt.es which shows the instructions for generating *Keys.* At this webpage they must introduce their name, first surname and email address in the part for collecting data.

171. The *Public and Private Keys* shall then be generated and shall be linked to the *Certificate*, becoming at this time *Signature Verification and Creation Data* respectively.

172. On making this pre-application the *Public Key* generated is sent to the FNMT-RCM, together with the corresponding possession tests of the *private Key*, for the subsequent issue of the *Certificate.*

173. After the FNMT-RCM receives this information, it shall check via the *User's Public Key* the validity of the information from the signed pre-application, only checking the possession and correspondence of the pair of cryptographic *Keys by it.*

174. If everything is correct, the FNMT-RCM shall assign an application code for the request made by the *User* and shall indicate it in a response webpage.

175. This information shall not give rise to the generation of a *Certificate* by the FNMT-RCM, until the *Local Registration Authority Office (LRA Office)* receives the signed application for the *Certificate.*

10.2.2.1.2. Accreditation of the identity and application (Step 2)

176. Once the *User* has obtained the application code in the "Pre-application" sub-process it must make the corresponding *Certificate* issue request via the corresponding *Local Registration Authority Office (LRA Office)* (that which represents the *Organization* before the FNMT-RCM in the *Certificates* management operations and in which the *User* provides its services).

177. This application shall require the physical presence of the *User* at the *Local Registration Authority Office (LRA Office)* where the *Local Registration Authority Officer (LRA Officer)* shall authenticate the *User* by requesting that they provide

- Personal details (at least the name, surname, email and distinctive number of the official document) and data linked to the request in question (application code) and
- The official document which proves the identity of the *User* and which includes their identifying details. .

178. The *Local Registration Authority Officer (LRA Officer)* shall check the *User's* condition as employee of the *Organization or Competent Body Subscribing the Certificate* and in force, via the means available and in view of the fact that the *Local Registration Authority Office (LRA Office)* acts in representation of the *Organization* in question and therefore reliably knows this information.

179. The FNMT-RCM, shall not be responsible for checking the personal details or the condition of employee, or that these requirements or conditions are maintained during the life of the *Certificate*, as there is no functional, administrative or employment legal relationship with the *User*, beyond the conditions of use document or, if applicable, issue contract, whose effect is strictly instrumental for the performance of the functions corresponding to the position.

180. The presence of the *User* before the *Local Registration Authority Officer (LRA Officer)* and the presentation of the official document which proves their identity, as well as the procedures to be followed by the latter, shall guarantee the identity of the *User* and their relationship with the *Subscribing Organization or Competent Body*, with it being a necessary and sufficient condition in order to establish the link between the identity and the *Signature Creation Data* that it is created at the time of the issue of the *Certificate*.

181. The registration application will generate two forms with the application contract and the conditions of use, to be printed and signed by the *User and Local Registration Authority Officer (LRA Officer)*.

182. Once the *Local Registration Authority Officer (LRA Officer)* confirms the identity of the *User*, that their position or employment in the *Organization* is in force and having signed the contractual firms, the *Local Registration Authority Officer (LRA Officer)* shall validate the data and send it to the FNMT-RCM together with the application code obtained in the pre-application step.

183. The *Local Registration Authority Office (LRA Office)* shall safe keep the contractual forms signed by both parties as part of the application.

184. The personal data and its processing shall be subject to the specific legislation.

185. This transfer of information to the FNMT-RCM shall be made by secure communications established for such purposes between the *Local Registration Authority Office (LRA Office)* and the FNMT-RCM.

10.2.2.1.3. Issue of the Certificate (Step 3)

186. Once the FNMT-RCM has received the personal details of the *User*, the information describing their relationship with the *Organization or Competent Body Subscribing the Certificate*, as well as the application request obtained in the pre-application step, the *Certificate* shall be issued.

187. The issue of the *Certificate* involves the generation of electronic documents which confirm the identity of the *Signatory*, their relationship with the *Organization* and their correspondence with the associated *Public Key*.

188. The issue of the *Certificates* subject to these *Policies* can only be made by the FNMT-RCM as *Certification Services Provider*, and there is no other body or entity capable of issuing them.

189. Through its *Electronic signature* the FNMT-RCM authenticates the *Certificate* and confirms the identity of the *Subscriber*, and its relationship with the *User*, in accordance with the information received by the *Local Registration Authority Office (LRA Office)*. On the other hand, and in order to avoid the manipulation of the information contained in the *Certificate*,

the FNMT-RCM shall use the cryptographic mechanisms which provide authenticity and integrity to the *Certificate*.

190. In any event, the FNMT-RCM shall act effectively in order to:

- Check that the *User* of the *Certificate* uses the *Private Key* corresponding to the *Public Key* linked to the identity of its *Signatory*. For this purpose, the FNMT-RCM shall check the correspondence between the *Private* Key and the *Public Key*.
- Achieve that the information included in the *Certificate* is based on the information provided by the corresponding *Local Registration Authority Office (LRA Office)*.
- Not ignore notorious events which could affect the reliability of the *Certificate*.
- Achieve that the *DN* (distinctive name) assigned in the *Certificate* is unique throughout the *Public Keys Infrastructure* of the FNMT-RCM.

191. In order to issue the *Normalised Certificate* the following steps shall be followed:

1. Composition of the distinctive name (DN) of the *Normalised Certificate*

With the personal details of the *User* collected during the *Certificate* application process, the distinctive name (DN) is composed according to the *X 500* standard, ensuring that said name makes sense and does not lead to any ambiguities. Pseudonyms are not considered as a form of identification.

The *DN* for this type of *Certificates* is made up of the following elements:

DN≡CN, O, C

The attributes O, C represent the branch of the directory containing the entry corresponding to the *Normalised Certificates* issued to the *User* in the service of the *Organization* in question.

The *CN* attribute contains the identification details of the *User*.

The O attribute contains the name of the *Organization*.

The C attribute contains the code of the country of the *Organization*.

Once the distinctive name (*DN*) has been composed, the corresponding entry is created in the *Directory*, ensuring that the distinctive name is unique through the *Public Key Infrastructure* of the *Certification Services Provider*.

2. Composition of the *User's* alternative identity

The User's alternative identity, as considered in this type of *Certificates*, contains the email address that it provided during the pre-application and identity accreditation steps. The subjectAltName extension defined in X 509 version 3 is used to offer this information.

3. Generation of the *Certificate* according to the profile of the *Normalized Certificate*

The *Normalised Certificate* format shall be in accordance with the UIT-T X.509 version 3 format and in accordance with the applicable regulations.

The profile of this type of *Certificate* can be consulted in **Table 3 –*Normalised Certificate* Profile** attached to this document.

10.2.2.2. Publication of the Normalised Certificate

192. Once the *Certificate* is generated by the *Certification Services Provider*, it will be published in the *Directory*, specifically in the entry corresponding to the *Organization*.

193. A communication that the *Certificate* is available for downloading will be sent to the email provided by the *User*.

10.2.2.3. Downloading and installation of the Normalised Certificate

194. Once the *Certificate* has been generated, a downloading mechanism is made available to the *User* at

https://ec.fnmt.es

Accessing the option "Descarga de su Certificado/Download your Certificate".

195. In this guided process the interested party will be asked to enter their name, first surname and email used to process the pre-application, as well as the application code returned by the system at the end of the process.

196. If the *Certificate* has not for any reason been generated, this will be indicated when trying to download. Otherwise it will be provided to the interested party who will introduce it into the support in which the *Keys* were generated during the pre-application process.

10.2.2.4. Validity of the Normalised Certificate

10.2.2.4.1. Expiry

197. The *Normalised Certificates* issued under this *Certification Policy* by the FNMT-RCM shall be valid for a period of four (4) years counting from the time of issue of the *Certificate*, provided that their validity is not extinguished. After that period and if the *Certificate* continues active, it will expire, and it shall be necessary to issue a new one if the *Titleholder* wishes to continue using the services of the *Certification Services Provider*.

10.2.2.4.2. Extinction of the validity

198. The *Normalised Certificates* issued by the FNMT-RCM under this policy shall become without effect under the following circumstances:

a) Termination of the period of validity of the *Certificate*

b) The FNMT-RCM ceases its activity as a *Certification Services Provider*, unless, with the express prior consent of the *Titleholder*, 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 when these circumstances occur.

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

199. For the purposes listed above, it is stated that the application to issue a *Normalised Certificate* for personnel in the service of the entities of the European Union when there is another in force in favour of the same *Titleholder* and under the same *Certification Policy* shall lead to the revocation of the first one obtained.

200. The effects of the revocation or suspension of the *Certificate*, i.e. the extinction of its validity, shall take effect from the date on which the FNMT-RCM becomes reliably aware of any of the determining events and it is recorded in its *information and consultancy services about the state of validity of the certificates*.

10.2.2.5. Revocation of the Normalised Certificate

10.2.2.5.1. Grounds for revoking the Normalised Certificate

201. The following are grounds for revoking a *Normalised Certificate*:

a) Revocation request by the authorised persons. The following shall under all circumstances lead to this request:

- The loss of the support of the *Certificate* or suspicion that its confidentiality has been compromised.
- The use by a third party of the *Titleholder's Signature Creation Data,* corresponding to the *Signature Verification Data* contained in the *Certificate* and linked to the identity of the *Titleholder.*
- The violation or putting in danger the secrecy of the *Titleholder's Signature Creation Data.*
- The non-acceptance by the *Organization or Competent Body* of the new conditions which may involve the issue of new *Declarations of Certification Practices*, during the period of one month following their publication.

b) Judicial or administrative decision which orders it, as well as the cases set out in the applicable legislation.

c) Extinction or dissolution of the legal status of the *Titleholder.*

d) Termination of the relationship between the *User* and the *Titleholder Organization or Competent Body of the Certificate*

e) Clear total or partial incapacity, or death of the *User*

f) Inaccuracies or alterations in the data provided by the *User* in order to obtain the *Certificate* or modification of the verified circumstances for its issue, as well as those relating to the position or the powers of representation, so that they are not now in accordance with the reality.

g) Breach of a substantial obligation in this *Certification Practice Statement* by the *User, the Certificate Titleholder* or the personnel of the *Local Registration Authority Office (LRA Office)* if it may affect the *Certificate* issue procedure.

h) Cancellation of the contract signed between the *Organization* and the FNMT-RCM.

i) Violation or putting in danger the secrecy of the *Signature Creation Data* of the -RCM with which it signs the *Certificates* that it issues.

202. Under no circumstances shall it be considered that the FNMT-RCM accepts any obligation to check the points mentioned in letters c) to g) of this section.

203. The actions constituting an offence of which the FNMT-RCM becomes aware performed in relation to the data or *Certificates*, the inaccuracies in the data or lack of diligence in its communication, including the grounds mentioned above, to the FNMT-RCM, shall exempt the FNMT-RCM from liability.

10.2.2.5.2. Effects of the revocation

204. The effects of the revocation or suspension of the *Certificate*, i.e. the extinction of its validity, shall take effect from the date on which the FNMT-RCM becomes reliably aware of any of the determining events and this is thus recorded in its *Information and consultation service on the state of the validity of the certificates.*

205. The revocation of *Certificates* involves, apart from its extinction, the end of the relationship and regime of use of the *Certificate* with the FNMT-RCM.

10.2.2.5.3. Procedure for the revocation

206. The revocation application for the *Normalised Certificates* can be made during the validity period recorded in said *Certificate.*

207. The revocation of a *Normalised Certificate* can be requested by the *Titleholder* through the *Local Registration Authority Referent (LRA Referent)* or the *Local Registration Authority Officer (LRA Officer).* Furthermore, the *User* can request from the *Local Registration Authority Office (LRA Office)* to revoke or suspend it there are justifying grounds, under the terms contained in this *Particular Certification Policy and Practices.*

208. Without prejudice to the above, the FNMT-RCM can revoke the *Normalised Certificates* in the cases contained in the *Certification Practice Statement* and in the applicable legislation.

209. The *User* or the *Titleholder* through a representative with sufficient capacity can request the revocation operation either personally at the corresponding *Local Registration Authority Office (LRA Office)*, or remotely. The Local Registration Authority Officer (LRA Officer) must check the sufficient capacity of the applicant in order to carry out the revocation application.

210. The applicant must prove the identity of the *User* of the *Certificate* to be revoked by providing its personal data (at least the name, first surname and email). In any event, the applicant must prove their identity by providing the corresponding official document.

211. The Local Registration Authority Officer (LRA Officer) will formalise the revocation application via the registration application, which will generate two forms with the application contract to be printed and signed by the applicant and the *Local Registration Authority Officer (LRA Officer)*

212. After the *Local Registration Authority Officer (LRA Officer)* confirms the identity of the applicant and their sufficient capacity and having signed the contractual forms, the *Local*

Registration Authority Officer (LRA Officer) shall valid the data and send it to the FNMT-RCM.

213. The *Local Registration Authority Office (LRA Office)* must look after the contractual forms signed by both parties as part of the application.

214. The FNMT-RCM shall receive that relevant information for the purposes of the revocation of a *Certificate* through the revocation application model that is presented, on paper or electronically, by the *Local Registration Authority Office (LRA Office).*

215. The *Local Registration Authority Office (LRA Office)* shall transfer the requests to the FNMT-RCM so that it can revoke the *Certificate.* The personal data and its handling shall be subject to the specific legislation.

216. FNMT-RCM shall consider that the applicant to revoke a *Certificate* of this type has sufficient capacity if the request is made through the corresponding *Local Registration Authority Office (LRA Office).* FNMT-RCM shall not assess the appropriateness of the revocation request when it is made through the aforementioned *Local Registration Authority Office (LRA Office).*

217. Once the FNMT-RCM has revoked the *Certificate,* the corresponding *List of Revoked Certificates* shall be published in the secure *Directory*, containing the series number of the revoked *Certificate,* the date and time of revocation and the reason for the revocation. Similarly, this information shall also be available via the OCSP protocol in the corresponding *Information service on the state of validity of the Certificates.*

10.2.2.6. Suspension of the Normalised Certificate

218. The suspension of the *Certificates* shall be considered a temporary revocation of the validity of the *Certificate* and as such the authorised procedures and entities for the application and processing of the revocation of the *Certificate* are applicable in the case of suspension.

10.2.2.6.1. Grounds for the suspension of the Normalised Certificate

219. The FNMT-RCM can suspend the validity of the *Certificates* in the event of a request from the same authorised persons and under the same conditions as for the revocation request.

220. Furthermore, the suspension request may be due to the existence of a ongoing investigation or judicial or administrative proceedings, which could conclude that the *Certificate* is effectively affected by a ground for revocation. In these cases, the FNMT-RCM, on request from a legitimate interested party, shall suspend the validity of the *Certificate* for the requested period and, after said period has passed, shall revoke the *Certificate* unless the FNMT-RCM is reliably request by the legitimate interested party to reactivate it.

10.2.2.6.2. Effects of the suspension

221. The suspension of *Certificates* leaves the *Certificate* without effect (extinguishes its validity) during a certain period of time and under certain conditions.

10.2.2.6.3. Procedure for the suspension of Certificates

222. The procedures and authorised persons for the *Certificate* revocation application and process are applicable in the case of suspension.

223. The *Local Registration Authority Office (LRA Office)* shall transfer the applications to the FNMT-RCM so that it can proceed to the suspension of the *Certificate.* The personal data and its processing shall be subject to the specific legislation.

224. The FNMT-RCM shall suspend the *Certificate* provisionally for a period of fifteen (15) days, after which the *Certificate* shall be extinguished by its direct revocation by the *Certification Services Provider,* unless the suspension has been cancelled. Notwithstanding the above, the period established for the suspension of the *Certificate* may be altered according to the duration of the investigations or judicial or administrative proceedings which may affect it.

225. Once the FNMT-RCM has suspended the *Certificate*, the corresponding *List of Revoked Certificates* shall be published in the secure *Directory,* containing the series number of the revoked *Certificate,* the date and time of revocation and the reason for the revocation. Similarly, this information shall also be available via the OCSP protocol in the corresponding *Information service on the state of validity of the Certificates.*

226. If during the *Certificate's* suspension period it expires or its revocation is requested, the same consequences will occur as for the non-suspended *Certificates* which expire or are revoked.

10.2.2.6.4. Cancelation of the suspension of the Normalised Certificate

227. The same legitimate persons for the suspension request can request the cancellation of the suspension of the *Normalised Certificates,* and under the same conditions and following the same procedures.

228. The *Local Registration Authority Office (LRA Office)* shall transfer requests to the FNMT-RCM so that it can cancel the suspension of the *Certificates,* The personal data and its processing shall be subject to the specific legislation.

229. Once the data validated by the *Local Registration Authority Office (LRA Office)* of the request to lift the suspension has been received, the FNMT-RCM shall withdraw the *Certificate* in question from the *List of Revoked Certificates,* not performing any technical action over the *Certificate*.

11. QUALIFIED CERTIFICATES

11.1. CERTIFICATION POLICY FOR THE ISSUE OF QUALIFIED CERTIFICATES

11.1.1. Identification

230. This *Certification Policy* of the FNMT-RCM for the issue of *Qualified Certificates* for their use within the scope of the *Organizations* and in the framework of the *EU Electronic Community*.

Name: *Certification Policy* for the issue of *Qualified Certificates*

Reference / OID:

- 1.3.6.1.4.1.5734.3.4.1

Version: 1.0

Date of issue: 15th November 2010

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

Related DCP: General Certification Practice Statement of the FNMT-RCM

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

11.1.2. Typology of the Qualified Certificate

231. The *Qualified Certificate* is the electronic certificate issued by the FNMT-RCM which links its *Subscriber* (the *Organization*) with certain *Signature Verification Data* and confirms, as a whole:

- The identity of the signatory and safekeeping of the *Keys* and their condition as personnel in the service of the *Organization* who makes electronic signatures using the *Certificate* on behalf of the acting entity and,
- The *Subscriber of the Certificate*, which is the *Organization*.

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

233. The process necessary in order to manage this *Certificate* (issue, revocation, renewal, etc.) are developed by the FNMT-RCM through a specific PKI infrastructure, based on identification and registration actions performed by the network of *Local Registration Authority Office (LRA Office)* designated by the *Organizations* which are *Subscribers of the Certificates*.

234. [ETSI456] identifies a series of requirements for the *Certification Polices* which amongst others issue *Certificates* which are called “Qualified Certificate”. This name is equivalent to the term *Qualified Certificate* which is used in this document.

235. The requirements identified in [ETSI456] for the *Certification Policies* which issue "*Qualified Certificates*" are satisfied in this *Policy*. Additionally, it is indicated that the *Certificates* issued under this policy are issued with the technical profile corresponding to the *Qualified Certificates* based on the criteria established for such *Certificates* in regulations [ETSI456] and [ETSI862], both as regards the *Certification Services Provider*, and the generation of the *Signature Creation and Verification Data* and the content of the *Certificate itself*.

236. On the other hand, [ETIS456] defines the *Qualified Certificates* as those which comply with the requirements established in appendix I of Directive [D99/93EC] and issued by a *Certification Policy* (NCP) which complies with the requirements established in appendix II of said Directive and as regards the management of these *Certificates.*

237. Due to the above, we can conclude that the *Certificates* issued under this *Certification Policy* incorporate the requirements identified in appendix I and II of Directive [D99/93EC]

11.1.3. Community and scope of application

238. This *Certification Policy* is applicable to the issue of electronic *Certificates* which have the following characteristics:

a) They are issued by the FNMT-RCM as *Certification Services Provider* complying with the criteria established in the Spanish Electronic Signature Act 59/2003, of 19th December and in the European Electronic Signature Directive [D99/93EC]

b) They are issued as *Qualified Certificates* based on the criteria established for them in the EESSI technical regulations, specifically in the Certification Policy for the issue of *Qualified Certificates* identified in regulation [ETSI056] – QCP (Qualified Certificate Policy) and for the realisation of *Electronic signature* in *Secure signature creation devices.*

c) *Secure signature creation devices* are under stood as the *Smartcard* of the FNMT-RCM which technically complies with the criteria established in [D99/93EC].

d) The *Certificates* issued under this *Certification Policy* are issued for the *Organizations* which form part of the *EU Electronic Community* as defined in the Definitions section of this document. Within the framework of this *Certification Policy*, the *Users* and safe keepers of the *Signature Creation Data* correspond to the personnel of the *Organizations* in the exercise of their competences and public functions of the position, of the employee relationship, of the functions of public employee, or of the condition of person authorised by the *Organization*, in relation to the entity to which they belong or with which these *Users* are related.

11.1.4. Responsibility and obligations of the parties

239. For the purposes of this section the following shall be parties:

- The *Organizations* represented through the different competent bodies and who are the *Titleholders* responsible for the *Certificates*.

- *Local Registration Authority Office (LRA Office)*, which, through the personnel designated by the *Organization*, are responsible for checking the requirements and conditions held by the *Users* of the *Certificate*.
- The *Users* of the *Certificate* and its *Keys*, who will be the personnel in the service of the *Organizations*.
- FNMT-RCM, as Certification Services Provider.
- The rest of the EU Electronic Community.

240. The rights and obligations regime of the *Organization* and the FNMT-RCM is governed by the corresponding agreements regulating the certification services.

241. As well as the obligations and responsibilities of the parties listed in this document and in the G-CPS, the *Organization* as *Local Registration Authority*, the *Local Registration Authority Referent (LRA Referent)* and the *Local Registration Authority Officer (LRA Officer)* are bound to:

- Comply with the registration procedures provided by the FNMT-RCM.
- To refrain from registering or processing requests from personnel who provide their services in an *Organization* other than it represents as *Registration Office*, without prejudice to the creation, in the European Commission, of centralised *Registration Offices* that have been established.
- To reliably check the data of the personnel in the service of the *Organization* regarding their identity and that they belong to said *Organization* to which it provides its services and, if applicable, any other data that reflects or characterises this belonging.
- To request the revocation or suspension of the *Qualified Certificate* for the personnel in the service of the *Organization* which represents the *Local Registration Authority Office (LRA Office)*, when any of the data in the *Certificate* is incorrect, has varied or needs to be reviewed for security reasons. It must also request the revocation or suspension under the circumstances set out in the applicable legislation.
- To request the FNMT-RCM to revoke the *Certificate* when the circumstances which affect the condition of the office, job or any other detail which reflects or characterises the relationship between the *User* of the *Certificate* with the Organization where they provide their services, are inaccurate, incorrect, have varied or must be revoked on grounds of security.
- To request from the FNMT-RCM, through the *Local Registration Authority Office (LRA Office)*, the revocation or suspension of the *Certificate* when, directly or through communication from the personnel in the service of the *Organization*, there is a loss of the support of the *Certificate* or of its confidentiality or presumption thereof.
- To safe keep the documentation provided by any of those taking part in the management processes of the *Certificates* (requests for issue, suspension, cancellation of the suspension, revocation and any others of a similar nature) as well as the documents generated in said processes (receipts, contracts of issue, revocation, etc.)
- To diligently look after the *Smartcards* which the FNMT-RCM delivers to the *Organization* so that its distribution to the *Users* is controlled and no activation data is kept or used (for example, the PIN, unblocking code, etc.). Any incident related to the *Smartcards* must be reported to the FNMT-RCM

242. The relationship between the FNMT-RCM and the *Organization* and the *Users* of the *Certificates* shall be determined, for the purposes for the *Certificates'* use regime, by the following documents: conditions of use or contract of issue of the *Certificate*, and of a subsidiary nature by these *Particular Certificate Policies and Practice Statement* and by the G-CPS, according to the relationship agreements or documents between the FNMT-RCM and the *Organizations*.

243. The relations between the *Titleholder Organization* of *the Certificate* and its personnel with the FNMT-RCM shall always be performed through the *Local Registration Authority Office (LRA Office)* and its *Referent.*

244. As well as the obligations and responsibilities of the parties listed in the G-CPS, the *User of the Certificate* is bound to:

- Not use the *Certificate* when any of the details referring to the position, job or any other which led to the issue of the *Certificate* is inaccurate, incorrect or does not reflect their relationship with the *Titleholder Organization.*
- To perform a proper use of the *Certificate* based on the competences and powers attributed by the position, job or employment as personnel in the service of the *Organization*.
- To maintain at all times exclusive control over the *Signature Creation Data* and to take reasonable precautions in order to prevent its unauthorised loss, revelation, modification or use. Furthermore, the *User* must keep under its control the activation data or use of the *Smartcard.*
- To return the *Smartcard* to the *Local Registration Authority Referent (LRA Referent)* once the *Certificates* which are in them have lost their validity.
- Communicate to the corresponding *Local Registration Authority Referent (LRA Referent)* the loss, or suspicion thereof, of the support of the *Certificate* or of its confidentiality, of which it is *User* in order to start, if appropriate, the *Certificate* revocation process.

245. The rest of the *EU Electronic Community* and the third parties shall regulate their relations with the FNMT-RCM through the G-CPS and these *Particular Certificate Policies and Practice Statement,* all without prejudice to that set out in the electronic signature regulations and other applicable regulations.

11.1.5. Limits on the use of the *Qualified Certificates*

246. Limits on the use of this type of *Certificates* are the *Electronic signature* operations that the *Users* realise in the performance of their competences on behalf of the *Titleholder Organization* of *the Certificate,* always within the framework of the capacities of representation which allows the relationship that links them. These *Certificates* cannot be used outside of the functionality set out above.

247. The FNMT-RCM and the *Organizations* can fix additional limits in the corresponding agreements.

248. The FNMT-RCM will not have control of the acts and uses of the *Certificates* performed by the *Titleholder*, *User*, and as such the FNMT-RCM shall be exempt from liability for such uses and the exceeding in the aforementioned use, as well as for the consequences and effects which may derive due to claims or possible asset liability performed by any member of the *EU Electronic Community* or by third parties.

249. In relation to the activities performed by the personnel of the *Local Registration Authority Office (LRA Office)* will be subjected to obligations and responsibilities established in Act 59/2003, of 19th December, of Electronic Signature, without prejudice to that set out in the Article 11 of the Royal Decree 1317/2001, of 30th November, implementing Article 81 of Law 66/1997, of 30th December, of Fiscal, Administrative and Social Order Measures, in relation with the FNMT – RCM security services for the communications through electronic, computer and telematic means with Public Administrations.

250. In order that the *User* can diligently use the *Qualified Certificates* and associated *Keys*, the *Organization* which represents the user must previous form part of the *EU Electronic Community* and having been constituted as *Titleholder of the Certificate.*

251. In any event, if a third party wishes to trust the *Electronic signature* performed with one of these *Qualified Certificates* without accessing the *Information and consultation services on the state of validity of the certificates* issued under this *Certification Policy*, no cover shall be obtained from these *Particular Certificate Policies and Practices* and shall lack any legitimacy to claim or start legal actions against the FNMT-RCM for damages or conflicts due to using or trusting a *Certificate*.

252. Furthermore, even within the scope of the *EU Electronic Community*, this type of *Certificate* cannot be used by a person or entity other than the FNMT-RCM, to:

- Sign another *Certificate*, unless expressly authorised in advance.
- Particular or private uses
- To sign software or components
- To generate time stamps for *Time-stamping* procedures
- To prevent free or onerous services, unless expressly authorised in advance, like for example:
    - Providing OCSP services
    - Generate Revocation Lists
    - Provide notification services
- To use the *Certificate* for uses other than those initially set out for the *Qualified Certificates*

11.2. PARTICULAR CERTIFICATION PRACTICES FOR THE QUALIFIED CERTIFICATES

253. The FNMT-RCM in its work as *Certification Services Provider* and in order to demonstrate the necessary reliability for the provision of said services, has developed a *Certification Practice Statement* with the aim of providing public information about the general conditions for the provision of certification services by the FNMT-RCM as *Certification Services Provider*.

254. The "Definitions" sector of the G-CPS and of this document must be taken into special account in order to interpret this appendix.

255. This document forms an integral part of the *Certification Practice Statement* of the FNMT-RCM and defines the set of particular practices adopted by the FNMT-RCM as *Certification Services Provider* for the management of the lifecycle of the *Qualified Certificates* issued by the *Certification Policy* identified with the OIDs 1.3.6.1.4.1.5734.3.4.1.

11.2.1. Key Management Services

256. Under no circumstances does the FNMT-RCM generate or store the *Private Keys* of the *Signatories*, which are generated under their exclusive control and, if applicable, with the intervention of the corresponding *Local Registration Authority Office (LRA Office)* and whose safekeeping is under the responsibility of the *User* of the *Certificate*.

11.2.2. Preparation of the *Secure Signature Creation Devices*

257. This *Certification Policy* obliges the use of a *Secure signature creation device* for the generation of keys and the subsequent realisation of *Electronic signature.* In order to facilitate compliance with this requirement, the FNMT-RCM shall provide the *Organizations*, for delivery to the *Users*, with a *Smartcard* for the generation of their *Private Keys* and the storage of the *Certificates.*

258. The *Smartcard* is delivered without any type of content, with the software necessary in order to achieve integration with the most common browsers. Furthermore, at this time they are provided with the codes necessary in order to access said card so that later, from their position or from the position of the *Registry Office*, they generate their *Keys* and introduce the *Certificate* in the *Smartcard.*

259. The FNMT-RCM provides this type of card as it allows the *Signatories* to maintain "exclusive control" over the *Signature creation data.*

11.2.3. Management of the lifecycle of the *Certificates*

260. Here are defined those aspects which, although some have been indicated in the G-CPS, have certain special characteristics which require greater detail.

11.2.3.1. Application and issue procedure for the Qualified Certificate

261. Below is a description of the application procedure for which the *Local Registration Authority Officer (LRA Officer)* takes the details of the personnel in the service of the *Organization*, confirms their identity and formalises, between said personnel and the FNMT-RCM, the conditions of use document or the issue contract, as set out in the agreement between the FNMT-RCM with the *Organization* for the subsequent issue of a Qualified Certificate.

262. It is stated that the FNMT-RCM, according to the list of *Subscribers* and dependent *User* personnel sent by the *Local Registration Authority Office (LRA Office)*, shall consider, under

the responsibility of the corresponding *Organizations*, that they shall act through the *Local Registration Authority Office (LRA Office)* as *Local Registry Authority*, that this personnel has their position in force, that their personal details are authentic and in force, and therefore authorised to obtain and use the *Certificate*.

263. The European Commission can establish, within the scope of action of its competences, central or common *Local Registration Authority Offices(LRA Office)* with uniform effects for any of the different entities of the Member States.

264. FNMT-RCM, shall not have, in this type of *Certificate*, the responsibility to check the position or employment of the *User*, or that these requirements are maintain throughout the life of the *Certificate*. The FNMT-RCM does not have a functional, administrative or employment legal relationship with the *User* beyond the conditions of use document or, if applicable, the issue contract.

265. The above checking activities shall be performed by the personnel of the *Local Registration Authority Office (LRA Office)* introduced by the *Organization*, which is the entity where the *User* provides their services. As such, and for these purposes, the *Local Registration Authority Office (LRA Office)* shall not be delegate or dependent authorities of the FNMT-RCM.

266. This *Certificate* shall be requested by the *Subscribing Organization* acting as applicant without prejudice to the fact that the operations necessary in order to request and obtain the *Certificate* are performed by the *Referent* or the *Local Registration Authority Officer (LRA Officer)* or, in an instrumental manner, by the *Users* themselves.

267. The three steps to be performed in order to obtain the *Certificate* are:

11.2.3.1.1. Pre-application (Step 1)

268. Beforehand, the *User* and the *Subscriber* must consult the G-CPS and these *Particular Certificate Policies and Practice Statement* at http://www.cert.fnmt.es/dpcs/ with the conditions of use and obligations as *Users* and *Subscriber*, respectively, of the *Certificate*, which are in the conditions of use document or, if applicable, the issue contract.

269. With the Smartcard and the accessories necessary for its use duly installed, the *User* must access https://ec.fnmt.es which shows the instructions for generating *Keys*. At this webpage they must introduce their name, first surname and email address in the part for collecting data.

270. The *Public and Private Keys* shall then be generated and shall be linked to the *Certificate*, becoming at this time *Signature Verification and Creation Data* respectively.

271. On making this pre-application the *Public Key* generated is sent to the FNMT-RCM, together with the corresponding possession tests of the *private Key*, for the subsequent issue of the *Certificate.*

272. After the FNMT-RCM receives this information, it shall check via the *User's Public Key* the validity of the information from the signed pre-application, only checking the possession and correspondence of the pair of cryptographic *Keys by it.*

273. If everything is correct, the FNMT-RCM shall assign an application code for the request made by the *User* and shall indicate it in a response webpage.

274. This information shall not give rise to the generation of a *Certificate* by the FNMT-RCM, until the *Local Registration Authority Office (LRA Office)* receives the signed application for the *Certificate.*

11.2.3.1.2. Accreditation of the identity (Step 2)

275. Once the *User* has obtained the application code in the "Pre-application" sub-process it must make the corresponding *Certificate* issue request via the corresponding *Local Registration Authority Office (LRA Office)* (that which represents the *Organization* before the FNMT-RCM in the *Certificates* management operations and in which the *User* provides its services).

276. This application shall require the physical presence of the *User* at the *Local Registration Authority Office (LRA Office)* where the *Local Registration Authority Officer (LRA Officer)* shall authenticate the *User* by requesting that they provide

- Personal details (at least the name, surname, email and distinctive number of the official document) and data linked to the request in question (application code) and
- The official document which proves the identity of the *User* and which includes their identifying details.

277. The *Local Registration Authority Officer (LRA Officer)* shall check the *User's* condition as a current employee of the *Organization Subscribing the Certificate*, via the means available and in view of the fact that the *Local Registration Authority Office (LRA Office)* acts in representation of the *Organization* in question and therefore reliably knows this information.

278. The FNMT-RCM, shall not be responsible for checking the personal details or the condition of employee, or that these requirements or conditions are maintained during the life of the *Certificate*, as there is no functional, administrative or employment legal relationship with the *User*, beyond the conditions of use document or, if applicable, issue contract, whose effect is strictly instrumental for the performance of the functions corresponding to the position.

279. The presence of the *User* before the *Local Registration Authority Officer (LRA Officer)* and the presentation of the official document which proves their identity, as well as the procedures to be followed by the latter, shall guarantee the identity of the *User* and their relationship with the *Subscriber Organization*, with it being a necessary and sufficient condition in order to establish the link between the identity and the *Signature Creation Data* that it is created at the time of the issue of the *Certificate*.

280. The registration application will generate two forms with the application contract and the conditions of use, to be printed and signed by the *User and Local Registration Authority Officer (LRA Officer)*.

281. Once the *Local Registration Authority Officer (LRA Officer)* confirms the identity of the *User,* that their position or employment in the *Organization* is in force and having signed the contractual firms, the *Local Registration Authority Officer (LRA Officer)* shall validate

the data and send it to the FNMT-RCM together with the application code obtained in the pre-application step.

282. The *Local Registration Authority Office (LRA Office)* shall safe keep the contractual forms signed by both parties as part of the application.

283. The personal data and its processing shall be subject to the specific legislation.

284. This transfer of information to the FNMT-RCM shall be made by secure communications established for such purposes between the *Local Registration Authority Office (LRA Office)* and the FNMT-RCM.

11.2.3.1.3. Issue of the Certificate (Step 3)

285. Once the FNMT-RCM has received the personal details of the *User*, the information describing their relationship with the *Organization Subscribing the Certificate*, as well as the application request obtained in the pre-application step, the *Certificate* shall be issued.

286. The issue of the *Certificate* involves the generation of electronic documents which confirm the identity of the *Signatory*, their relationship with the *Organization* and their correspondence with the associated *Public Key*.

287. The issue of the *Certificates* subject to these *Policies* can only be made by the FNMT-RCM as *Certification Services Provider*, and there is no other body or entity capable of issuing them.

288. Through its *Electronic signature* the FNMT-RCM authenticates the *Certificate* and confirms the identity of the *Subscriber*, and its relationship with the *User*, in accordance with the information received by the *Local Registration Authority Office (LRA Office)*. On the other hand, and in order to avoid the manipulation of the information contained in the *Certificate*, the FNMT-RCM shall use the cryptographic mechanisms which provide authenticity and integrity to the *Certificate*.

289. In any event, the FNMT-RCM shall act effectively in order to:

- Check that the *User* of the *Certificate* uses the *Private Key* corresponding to the *Public Key* linked to the identity of its *Signatory*. For this purpose, the FNMT-RCM shall check the correspondence between the *Private Key* and the *Public Key*.
- Achieve that the information included in the *Certificate* is based on the information provided by the corresponding *Local Registration Authority Office (LRA Office)*.
- Not ignore notorious events which could affect the reliability of the *Certificate*.
- Achieve that the *DN* (distinctive name) assigned in the *Certificate* is unique throughout the *Public Keys Infrastructure* of the FNMT-RCM.

290. In order to issue the *Qualified Certificate* the following steps shall be followed:

1. Composition of the distinctive name (DN) of the *Qualified Certificate*

With the personal details of the *User* collected during the *Certificate* application process, the distinctive name (DN) is composed according to the *X 500* standard, ensuring that said name makes sense and does not lead to any ambiguities. Pseudonyms are not considered as a form of identification.

The *DN* for this type of *Certificates* is made up of the following elements:

DN≡CN, O, C

The attributes O, C represent the branch of the directory containing the entry corresponding to the *Qualified Certificates* issued to the *User* in the service of the *Organization* in question.

The *CN* attribute contains the identification details of the *User*.

The O attribute contains the name of the *Organization*.

The C attribute contains the code of the country of the *Organization*.

Once the distinctive name (*DN*) has been composed, the corresponding entry is created in the *Directory*, ensuring that the distinctive name is unique through the *Public Key Infrastructure* of the *Certification Services Provider*.

2. Composition of the *User's* alternative identity

The User's alternative identity, as considered in this type of *Certificates*, contains the name, surname and email address that it provided during the pre-application and identity accreditation steps. The subjectAltName extension defined in X 509 version 3 is used to offer this information.

3. Generation of the *Certificate* according to the profile of the *Qualified Certificate*

The *Qualified Certificate* format shall be in accordance with the UIT-T X.509 version 3 format and in accordance with the applicable regulations.

The profile of this type of *Certificate* can be consulted in **Table 4 – *Qualified Certificate* Profile** attached to this document.

11.2.3.2. Publication of the Qualified Certificate

291. Once the *Certificate* is generated by the *Certification Services Provider*, it will be published in the *Directory*, specifically in the entry corresponding to the *Organization*.

292. A communication that the *Certificate* is available for downloading will be sent to the email provided by the *User*.

11.2.3.3. Downloading and installation of the Qualified Certificate

293. Once the *Certificate* has been generated, a downloading mechanism is made available to the *User* at

https://ec.fnmt.es

Accessing the option "Descarga de su Certificado/Download your Certificate".

294. In this guided process the interested party will be asked to enter their name, first surname and email used to process the pre-application, as well as the application code returned by the system at the end of the process.

295. If the *Certificate* has not for any reason been generated, this will be indicated when trying to download. Otherwise it will be provided to the interested party who will introduce it into the support in which the *Keys* were generated during the pre-application process.

11.2.3.4. Validity of the Qualified Certificate

11.2.3.4.1. Expiry

296. The *Qualified Certificates* issued under this *Certification Policy* by the FNMT-RCM shall be valid for a period of four (4) years counting from the time of issue of the *Certificate*, provided that their validity is not extinguished. After that period and if the *Certificate* continues active, it will expire, and it shall be necessary to issue a new one if the *Subscriber* wishes to continue using the services of the *Certification Services Provider.*

11.2.3.4.2. Extinction of the validity

297. The *Qualified Certificates* issued by the FNMT-RCM under this policy shall become without effect under the following circumstances:

a) Termination of the period of validity of the *Certificate*

b) The FNMT-RCM ceases its activity as a *Certification Services Provider*, unless, with the express prior consent of 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 when these circumstances occur.

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

298. For the purposes listed above, it is stated that the application to issue a *Qualified Certificate* for personnel in the service of the entities of the European Union when there is another in force in favour of the same *Subscriber* and under the same *Certification Policy* shall lead to the revocation of the first one obtained.

299. The effects of the revocation or suspension of the *Certificate*, i.e. the extinction of its validity, shall take effect from the date on which the FNMT-RCM becomes reliably aware of any of the determining events and it is recorded in its *information and consultancy services about the state of validity of the certificates*.

11.2.3.5. Revocation of the Qualified Certificate

11.2.3.5.1. Grounds for revoking the Qualified Certificate

300. The following are grounds for revoking a *Qualified Certificate*:

a) Revocation request by the authorised persons. The following shall under all circumstances lead to this request:

- The loss of the support of the *Certificate* or suspicion that its confidentiality has been compromised.

- The use by a third party of the *Titleholder's Signature Creation Data,* corresponding to the *Signature Verification Data* contained in the *Certificate* and linked to the identity of the *Signatory.*
- The violation or putting in danger the secrecy of the *Signature Creation Data.*
- The non-acceptance by the *Organization* of the new conditions which may involve the issue of new *Declarations of Certification Practices,* during the period of one month following their publication.

b) Judicial or administrative decision which orders it, as well as the cases set out in the applicable legislation. .

c) Extinction or dissolution of the legal status of the *Subscriber*.

d) Termination of the relationship between the *User* and the *Organization Subscribing the Certificate*

e) Clear total or partial incapacity, or death of the *User*

f) Inaccuracies or alterations in the data provided by the *User* in order to obtain the *Certificate* or modification of the verified circumstances for its issue, as well as those relating to the position or the powers of representation, so that they are not now in accordance with the reality.

g) Breach of a substantial obligation in this *Certification Practice Statement* by the *User, the Certificate Subscriber* or the personnel of the *Local Registration Authority Office (LRA Office)* if it may affect the *Certificate* issue procedure.

h) Cancellation of the contract signed between the *Organization* and the FNMT-RCM.

i) Violation or putting in danger the secrecy of the *Signature Creation Data* of the FNMT-RCM with which it signs the *Certificates* that it issues.

301. Under no circumstances shall it be considered that the FNMT-RCM accepts any obligation to check the points mentioned in letters c) to g) of this section.

302. The actions constituting an offence of which the FNMT-RCM becomes aware performed in relation to the data or *Certificates*, the inaccuracies in the data or lack of diligence in its communication, including the grounds mentioned above, to the FNMT-RCM, shall exempt the FNMT-RCM from liability.

11.2.3.5.2. Effects of the revocation

303. The effects of the revocation or suspension of the *Certificate*, i.e. the extinction of its validity, shall take effect from the date on which the FNMT-RCM becomes reliably aware of any of the determining events and this is thus recorded in its *Information and consultation service on the state of the validity of the certificates.*

304. The revocation of *Certificates* involves, apart from its extinction, the end of the relationship and regime of use of the *Certificate* with the FNMT-RCM.

11.2.3.5.3. Procedure for the revocation

305. The revocation application for the *Qualified Certificates* can be made during the validity period recorded in said *Certificate.*

306. The revocation of a *Qualified Certificate* can be requested by the *Subscriber* through the *Local Registration Authority Referent (LRA Referent)* or the *Local Registration Authority Officer (LRA Officer).* Furthermore, the *User* can request from the *Local Registration Authority Office (LRA Office)* to revoke or suspend it there are justifying grounds, under the terms contained in this *Particular Certification Policy and Practices.*

307. Without prejudice to the above, the FNMT-RCM can revoke the *Qualified Certificates* in the cases contained in the *Certification Practice Statement* and in the applicable legislation.

308. The *User* or the *Subscriber* through a representative with sufficient capacity can request the revocation operation either personally at the corresponding *Local Registration Authority Office (LRA Office),* or remotely. The Local Registration Authority Officer (LRA Officer) must check the sufficient capacity of the applicant in order to carry out the revocation application.

309. In any of the cases, the applicant must prove the identity of the *User* of the *Certificate* to be revoked by providing its personal data (at least the name, first surname and email).

310. The Local Registration Authority Officer (LRA Officer) shall formalise the revocation request via the registration application, which will generate two forms with the application contract, to be printed and signed by the applicant and the *Local Registration Authority Officer (LRA Officer).*

311. After the *Local Registration Authority Officer (LRA Officer)* confirms the identity of the applicant and their sufficient capacity, and having signed the contractual forms, the *Local Registration Authority Officer (LRA Officer)* shall validate the data and sent it to the FNMT-RCM.

312. The *Local Registration Authority Office (LRA Office)* must look after the contractual forms signed by both parties as part of the application.

313. The FNMT-RCM shall receive that relevant information for the purposes of the revocation of a *Certificate* through the revocation application model that is presented, on paper or electronically, by the *Local Registration Authority Office (LRA Office).*

314. The *Local Registration Authority Office (LRA Office)* shall transfer the requests to the FNMT-RCM so that it can revoke the *Certificate.* The personal data and its handling shall be subject to the specific legislation.

315. FNMT-RCM shall consider that the applicant to revoke a *Certificate* of this type has sufficient capacity if the request is made through the corresponding *Local Registration Authority Office (LRA Office).* FNMT-RCM shall not assess the appropriateness of the revocation request when it is made through the aforementioned *Local Registration Authority Office (LRA Office).*

316. Once the FNMT-RCM has revoked the *Certificate,* the corresponding *List of Revoked Certificates* shall be published in the secure *Directory,* containing the series number of the revoked *Certificate,* the date and time of revocation and the reason for the revocation. Similarly, this information shall also be available via the OCSP protocol in the corresponding *Information service on the state of validity of the Certificates.*

11.2.3.6. Suspension of the Qualified Certificate

317. The suspension of the *Certificates* shall be considered a temporary revocation of the validity of the *Certificate* and as such the authorised procedures and entities for the application and processing of the revocation of the *Certificate* are applicable in the case of suspension.

11.2.3.6.1. Grounds for the suspension of the Qualified Certificate

318. The FNMT-RCM can suspend the validity of the *Certificates* in the event of a request from the same authorised persons and under the same conditions as for the revocation request.

319. Furthermore, the suspension request may be due to the existence of a ongoing investigation or judicial or administrative proceedings, which could conclude that the *Certificate* is effectively affected by a ground for revocation. In these cases, the FNMT-RCM, on request from a legitimate interested party, shall suspend the validity of the *Certificate* for the requested period and, after said period has passed, shall revoke the *Certificate* unless the FNMT-RCM is reliably request by the legitimate interested party to reactivate it.

11.2.3.6.2. Effects of the suspension

320. The suspension of *Certificates* leaves the *Certificate* without effect (extinguishes its validity) during a certain period of time and under certain conditions.

11.2.3.6.3. Procedure for the suspension of Certificates

321. The procedures and authorised persons for the *Certificate* revocation application and process are applicable in the case of suspension.

322. The *Local Registration Authority Office (LRA Office)* shall transfer the applications to the FNMT-RCM so that it can proceed to the suspension of the *Certificate.* The personal data and its processing shall be subject to the specific legislation.

323. The FNMT-RCM shall suspend the *Certificate* provisionally for a period of fifteen (15) days, after which the *Certificate* shall be extinguished by its direct revocation by the *Certification Services Provider,* unless the suspension has been cancelled. Notwithstanding the above, the period established for the suspension of the *Certificate* may be altered according to the duration of the investigations or judicial or administrative proceedings which may affect it.

324. Once the FNMT-RCM has suspended the *Certificate*, the corresponding *List of Revoked Certificates* shall be published in the secure *Directory*, containing the series number of the revoked *Certificate*, the date and time of revocation and the reason for the revocation. Similarly, this information shall also be available via the OCSP protocol in the corresponding *Information service on the state of validity of the Certificates.*

325. If during the *Certificate's* suspension period it expires or its revocation is requested, the same consequences will occur as for the non-suspended *Certificates* which expire or are revoked.

11.2.3.6.4. Cancelation of the suspension of the Qualified Certificate

326. The same legitimate persons for the suspension request can request the cancellation of the suspension of the *Qualified Certificates,* and under the same conditions and following the same procedures.

327. The *Local Registration Authority Office (LRA Office)* shall transfer requests to the FNMT-RCM so that it can cancel the suspension of the *Certificates,* The personal data and its processing shall be subject to the specific legislation.

328. Once the data validated by the *Local Registration Authority Office (LRA Office)* of the request to lift the suspension has been received, the FNMT-RCM shall withdraw the *Certificate* in question from the *List of Revoked Certificates,* not performing any technical action over the *Certificate*.

11.2.4. Exclusions and additional requirements to ETSI TS 101 456

329. In accordance with the regulation in section 8.2 c) the issued defined in section 7.3.5.f) are excluded. This issue will be regulated by that indicated in the section "*Publication of the Certificate"* of this appendix.

12. SERVER CERTIFICATES

12.1. CERTIFICATION POLICY FOR THE WEB SERVER CERTIFICATES

12.1.1. Identification

330. This *Certification Policy* of the FNMT-RCM for the issue of *Web server certificates,* also known as SSL/TSL *Certificates,* for their use within the scope of the *Organizations* and in the framework of the *EU Electronic Community.*

Name: *Certification Policy* for the issue of *Web server certificates*

Reference / OID:

- 1.3.6.1.4.1.5734.3.4.4 – For the Common Name Certificates
- 1.3.6.1.4.1.5734.3.4.5 – For the Wildcard Certificates

Version: 1.0

Date of issue: 15th November 2010

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

Related DCP: General Certification Practice Statement of the FNMT-RCM

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

12.1.2. Typology of the Web server certificate

331. The *Web server certificates* are those *Certificates* issued by the FNMT-RCM under this *Certification Policy* which link certain *Signature Verification Data* of a server or application in relation to which there is a certain individual or legal entity which acts as the responsible party, which has the control over said server or application.

332. This type of *Certificate* is used by the *Subscribing Organizations or Competent Bodies* in order to identify and authenticate the URL address (domain name) or IP of a web server, so that the users who access it have sufficient guarantees that said access is performed to the real web address (domain name or IP) of the server.

333. The *Private Key* associated to the *Public Key* shall be under the responsibility and custody of the *Party responsible for the certificate* who will act as representative of the individual or legal entity of the web server object of the *Certificate.*

334. For the purposes of article 6 of the Spanish Electronic Signature Act, of 19th December, the *Web server certificates* shall be considered electronic *Certificates* when there is an undeniable link between the *Web server certificate* and its *Subscribing Organization or Competent Body.* FNMT-RCM shall issue these *Certificates* whenever requested by the members of the *EU Electronic Community* for the various relationships that may arise and their use is not prohibited or limited by the applicable legislation.

335. The FNMT-RCM shall not be liable for the actions performed with this type of *Certificate* when there is an abuse of powers or they are insufficient and/or when there are decisions by the *Certificate Subscriber* which affects the validity of the powers of the responsible party, and as such any modification, revocation or restriction shall not be binding on the FNMT-RCM unless it is notified in a reliable manner.

336. These *Web server certificates* are issued and signed by the FNMT-RCM to be installed and used by servers with SSL/TSL support, so that it inherits the confidence represented by FNMT-RCM as *Certification Services Provider*.

337. Only those entities which have signed an agreement with the FNMT-RCM, by virtue of which they form part of the *EU Electronic Community*, as considered in the *Certification Practice Statement* of the FNMT-RCM, can obtain *Web server certificates.*

338. These *Web server certificates* do not have the legal effect equivalent to the electronic signature recognised with the actions performed through the traditional handwritten signature. However, they are valid and have legal effect according to their respective nature under the applicable legislation.

339. The FNMT-RCM, as *Certification Services Provider* reserves the right not to issue or to revoke this type of *Certificate* if its *Responsible Party* or the party responsible for the server or application which uses said *Certificate*, does not use it properly and infringes third party industrial or intellectual property rights over the applications, web sites or equipment that they wish to protect with said *Certificates*, or their use is provided to trick or confuse the ownership of said applications, websites or equipment. In particular, said reservation of rights can be performed by FNMT-RCM when the *Certificates* are used against the following principles:

- The safeguarding of public order, criminal investigation, public safety or national defence.
- The protection of public health, or the health of individuals or legal entities which are consumers or users, even when they act as investors.
- The respect for human dignity and the principle of non-discrimination on the grounds of race, gender, religion, opinion, nationality, disability or any other personal or social circumstance, and
- The protection of youth and children.

340. The FNMT–RCM is exempt and shall remain unscathed from any claim due to the improper use of the *Web server certificates* made by:

- its *Subscriber* or *Responsible party* or
- the owner or party responsible for the equipment or applications which use the *Certificate*

and, in both cases, which breach that set out in the *Certification Practice Statement.*

341. The FNMT-RCM issues under this *Certification Policy* the following types of *Web server certificates*:

- *Web server certificates* for their use in a domain name or IP (Common Name).
- *Web server certificates* for their use in various sub-domain names within a given domain (Wildcard).

342. In both cases, the *Web server certificates* allow for the identification of a web server accessible through a domain name or IP.

12.1.3. Community and scope of application

343. This *Certification Policy* is applicable to the issue of electronic *Certificates* which have the following characteristics:

a) They are issued by the FNMT-RCM as *Certification Services Provider* complying with the criteria established in the Spanish Electronic Signature Act 59/2003, of 19th December and in the European Electronic Signature Directive [D99/93EC]

b) The *Certificates* issued under this *Certification Policy* are issued for the *Organizations* which form part of the *EU Electronic Community* as defined in the Definitions section of this document. Within the framework of this *Certification Policy*, the *Users* and safe keepers of the *Signature Creation Data* correspond to the personnel of the *Organizations* in the exercise of their competences and public functions of the position, of the employee relationship, of the functions of public employee, or of the condition of person authorised by the *Organization*, in relation to the entity to which they belong or with which these *Users* are related.

12.1.4. Responsibility and obligations of the parties

344. For the purposes of this section, the following shall be parties:

- The *Organizations* or *Competent Bodies* represented through the different competent bodies and who are the *Subscribers* responsible for the *Certificates*.
- *Local Registration Authority Office (LRA Office)*, which, through the personnel designated by the *Organization*, are responsible for checking the requirements and conditions held by the *Users* of the *Certificate*.
- The *Users* of the *Certificate* and its *Keys*, who will be the personnel in the service of the *Organizations*.
- FNMT-RCM, as Certification Services Provider.
- The rest of the EU Electronic Community.

345. The rights and obligations regime of the *Organization* and the FNMT-RCM is governed by the corresponding agreements regulating the certification services.

346. As well as the obligations and responsibilities of the parties listed in this document and in the G-CPS, the *Organization* as *Local Registration Authority*, the *Local Registration Authority Referent (LRA Referent)* and the *Local Registration Authority Officer (LRA Officer)* are bound to:

- Comply with the registration procedures provided by the FNMT-RCM.

- To refrain from registering or processing requests from personnel who provide their services in an *Organization* other than that which represents as *Local Registration Authority Office (LRA Office),* without prejudice to the creation, in the European Commission, of centralised *Local Registration Authority Offices (LRA Office)* which have been established.
- To request the revocation or suspension of the *Web service certificate* when any of the data contained in the *Certificate* is inaccurate, incorrect, has varied or needs to be revoked on the grounds of security. The revocation or suspension must also be requested under the circumstances set out in the applicable legislation.
- To request the FNMT-RCM, through the *Local Registration Authority Office (LRA Office)*, to revoke when directly or through the communication from the personnel in the service of the *Organization,* there is a loss of the support of the *Certificate* or of its confidentiality, or presumption thereof.
- To safe keep the documentation provided by any of those taking part in the management processes of the *Certificates* (requests for issue, suspension, cancellation of the suspension, revocation and any others of a similar nature) as well as the documents generated in said processes (receipts, contracts of issue, revocation, etc.)
- To reliably check the data of the personnel in the service of the *Organization or Competent Body Subscribing the Certificate* regarding their identity and that they belong to said *Organization,* as well as the sufficient capacity in order to make requests on behalf of the *Certificate Subscriber.* Equally, their correspondence with the subscribers and contacts established in the corresponding databases must be verified in order to manage and administer the electronic address or domain name which will identify the *Certificate* object of the application and of the corresponding server.

347. The relationship between the FNMT-RCM and the *Organization* and the *Parties Responsible for the Certificates* shall be determined, for the purposes for the *Certificates'* use regime, by the following documents: conditions of use or contract of issue of the *Certificate,* and of a subsidiary nature by these *Particular Certificate Policies and Practice Statement* and by the G-CPS, according to the relationship agreements or documents between the FNMT-RCM and the *Organizations*.

348. The relations between the *Organization or Competent Body Subscribing the Certificate* or its personnel and the FNMT-RCM shall always be performed through the *Local Registration Authority Office (LRA Office)* and its *Referent.*

349. As well as the obligations and responsibilities of the parties listed in the G-CPS, the *Party Responsible for the Certificate* is bound:

    - Not to use the *Certificate* in web servers whose content:
        - May infringe third-party intellectual and industrial property rights, endanger public order, criminal investigation, public security or national defence.
        - Endanger the protection of public health or the health of individuals or legal entities which are consumers or users, even when they act as investors.

    - Reduce respect for people's dignity and the principle of non-discrimination on the grounds of race, gender, religion, opinion, nationality, disability or any other personal or social circumstance, and
    - Endanger the protection of youth and children.

- To perform a proper use of the *Certificate* based on the competences and powers attributed by the *Subscribing Organization or Competent Body*.
- To maintain at all times exclusive control over the *Signature Creation Data* and to take reasonable precautions in order to prevent its unauthorised loss, disclosure, modification or use.
- Communicate to the corresponding *Local Registration Authority Referent (LRA Referent)* the loss, or suspicion thereof, of the support of the *Certificate* or of its confidentiality, of which it is *Responsible Party* in order to start, if appropriate, the *Certificate* revocation process

350. The rest of the *EU Electronic Community* and the third parties shall regulate their relations with the FNMT-RCM through the G-CPS and this *Particular Certificate Policies and Practice Statement*, all without prejudice to that set out in the electronic signature regulations and other applicable regulations.

12.1.5. Limits on the use of the *Web server certificates*

351. The use of this type of *Certificates* is limited to the web servers of the *Subscribing Organizations or Competent Bodies* in order to identify and authenticate the URL address or IP of said servers. These *Certificates* cannot be used outside of the functionality set out above.

352. The FNMT-RCM and the *Organizations* can fix additional limits in the corresponding agreements.

353. The FNMT-RCM will not have control of the acts and uses of the *Certificates* performed by the *Subscriber*, *Responsible Party or the Local Registration Authority Office (LRA Office)*, and as such the FNMT-RCM shall be exempt from liability for such uses and the exceeding in the aforementioned use, as well as for the consequences and effects which may derive due to claims or possible asset liability performed by any member of the *EU Electronic Community* or by third parties.

354. In order that the *Responsible Party* can diligently use the *Web server certificates* and associated *Keys*, the *Organization or Competent Body* which represents the Responsible Party must previous form part of the *EU Electronic Community* and having been constituted as *Subscriber of the Certificate.*

355. In any event, if a third party wishes to trust the *Electronic signature* performed with one of these *Web server certificates* without accessing the *Information and consultation services on the state of validity of the certificates* issued under this *Certification Policy*, no cover shall be obtained from these *Particular Certificate Policies and Practices* and shall lack any

legitimacy to claim or start legal actions against the FNMT-RCM for damages or conflicts due to using or trusting a *Certificate*.

356. Furthermore, even within the scope of the *EU Electronic Community*, this type of *Certificate* cannot be used by a person or entity other than the FNMT-RCM, to:

- Sign another *Certificate*, unless expressly authorised in advance.
- Particular or private uses
- To sign software or components
- To generate time stamps for *Time-stamping* procedures
- To prevent free or onerous services, unless expressly authorised in advance, like for example:
    - Providing OCSP services
    - Generate Revocation Lists
    - Provide notification services
- To use the *Certificate* for uses other than those initially set out for the *Web server certificates*

12.2. PARTICULAR CERTIFICATION PRACTICES FOR SERVER CERTIFICATES

357. The FNMT-RCM in its work as *Certification Services Provider* and in order to demonstrate the necessary reliability for the provision of said services, has developed a *Certification Practice Statement* with the aim of providing public information about the general conditions for the provision of certification services by the FNMT-RCM as *Certification Services Provider*.

358. The "Definitions" section of the G-CPS and of this document must be taken into special account in order to interpret this appendix.

359. This document forms an integral part of the *Certification Practice Statement* of the FNMT-RCM and defines the set of particular practices adopted by the FNMT-RCM as *Certification Services Provider* for the management of the lifecycle of the *server certificates* issued under the *Certification Policy* identified with the OIDs

- 1.3.6.1.4.1.5734.3.4.4 – For Common Name *Web Server Certificates*
- 1.3.6.1.4.1.5734.3.4.5 – For Wildcard *Web Server Certificates*
- 1.3.6.1.4.1.5734.3.4.7 – For *Automated Action Certificates* of the type *Qualified certificate without a secure signature creation device for signing documents*
- 1.3.6.1.4.1.5734.3.4.8 – For *Automated Action Certificates* of the type *Normalised Certificate for signing or encrypting documents*

12.2.1. *Key* Management Services

360. Under no circumstances does the FNMT-RCM generate or store the *Private Keys* of the *Signatories*, which are generated under their exclusive control and, if applicable, with the

intervention of the corresponding *Local Registration Authority Office (LRA Office)* and whose safekeeping is under the responsibility of the *Responsible Party* of the *Certificate*.

12.2.2. Management of the lifecycle of the *Certificates*

361. Here are defined those aspects which, although some have been indicated in the G-CPS, have certain special characteristics which require greater detail.

12.2.2.1. Application and issue procedure for the server certificate

362. Below is a description of the application procedure by which the *Local Registration Authority Officer (LRA Officer)* takes the details of the personnel in the service of the *Organization,* confirms their identity and their capacity to request the *Certificate* for the domain name, IP, institution or system in question, as the case may be, and formalises, between said personnel and the FNMT-RCM, the conditions of use document or the issue contract, as set out in the agreement between the FNMT-RCM and the *Organization* for the subsequent issue of a *Server certificate*.

363. The FNMT-RCM considers under the responsibility of the *Organizations,* which will act through the *Local Registration Authority Office (LRA Office)* as *Local Registration Authority*, that this personnel have their positions in force, that their personal details are authentic and in force and, therefore, authorised to obtain and install the *Certificate.* The FNMT-RCM does not have a functional, administrative or employment legal relationship with this personnel beyond the conditions of use document or, if applicable, the issue document, and therefore has no obligation to check the aforementioned details.

364. The European Commission can establish, within the scope of action of its competences, central or common Registration Authority Office (LRA Office) with uniform effects for any of the different entities of the Member States.

365. The above checking activities shall be performed by the personnel of the *Local Registration Authority Office (LRA Office)* introduced by the *Organization*, which is the entity where the *Responsible Party of the Certificate* provides their services. As such, and for these purposes, the *Local Registration Authority Office (LRA Office)* shall not be delegate or dependent authorities of the FNMT-RCM.

366. This *Certificate* shall be requested by the *Subscribing Organization or Competent Body* which shall act as applicant without prejudice to the fact that the operations necessary in order to request and obtain the *Certificate* are performed by the *Referent* or the *Local Registration Authority Officer (LRA Officer)* or, in an instrumental manner, by the *Responsible Party* itself.

367. The three steps to be performed in order to obtain the *Certificate* are:

12.2.2.1.1. Generation of Keys (Step 1)

368. Beforehand, the *Responsible Party* and the *Subscriber* must consult the G-CPS and these *Particular Certificate Policies and Practice Statement* at http://www.cert.fnmt.es/dpcs/ with the conditions of use and obligations as *Responsible Party* and *Subscriber*, respectively, of

the *Certificate*, which are in the conditions of use document or, if applicable, the issue contract.

369. Afterwards, the *Responsible Party of the Certificate* must generate, in the server where it will be used, the *Public and Private Keys* which will be binding on it, becoming at that time *Signature Verification and Creation Data* or *Encrypting and Decrypting Data*, respectively. Furthermore, with these *Keys*, the *Party Responsible for the Certificate* shall generate a *PKCS#10* to make the *Certificate* application to the FNMT-RCM

12.2.2.1.2. Accreditation of the identity and application (Step 2)

370. The *Responsible Party of the Certificate* must then make the corresponding issue request via the corresponding *Local Registration Authority Office (LRA Office)* (that which represents the *Organization* before the FNMT-RCM in the *Certificates* management operations and in which the *Responsible Party* provides its services).

371. This application shall require the physical presence or remote presence. In any event the *Local Registration Authority Officer (LRA Officer)* shall authenticate the *Responsible Party of the Certificate* by requesting that they provide:

- Personal details (at least the name, surname, email and distinctive number of the official document) and data linked to the request in question (PKCS#10 and domain name, IP address, institution or system for which the *Certificate* is issued),
- Photocopy of the official documents which prove the identity of the *Responsible Party* and which includes their identifying details.
- Photocopy of the designation by the *Subscribing Organization or Competent Body* to the *Party Responsible for the Certificate* as party authorised to make the request for the *Server certificate*

372. The documentation provided by the *Party Responsible for the Certificate* shall be kept by the *Local Registration Authority Office (LRA Office)* as part of the application.

373. The *Local Registration Authority Officer (LRA Officer)* shall check the *Responsible Party and applicant's* condition as employee of the *Organization or Competent Body Subscribing the Certificate* and with position in force and sufficient powers via the corresponding authorisation of the *Organization*, as well as the accuracy of the email, all via the means available and in view of the fact that the *Local Registration Authority Office (LRA Office)* acts in representation of the *Organization* in question and therefore reliably knows this information.

374. The *Local Registration Authority Officer (LRA Officer)* shall check through the authorisation form or *Certificate* application, that the *Organization or Competent Body* has obtained the domain name, IP, institution or system to include in said *Certificate*, stating that it is the registered owner of the identification in question.

375. Providing the data and documents required in the application shall guarantee the identity of the *Party Responsible for the Certificate* and its conditions as employee and authorised by its *Subscribing Organization or Competent Body* and shall be a necessary and sufficient

condition in order to establish the link between identity and *Signature Creation Data* which is created at the time the *Certificate* is issued.

376. Once the data is revised, the *Local Registration Authority Officer (LRA Officer)* shall access the registration application in order to introduce said data, including the PKCS#10. If the application is complete, the *Local Registration Authority Officer (LRA Officer)* shall receive as a response an application code which will identify the transaction and which will be needed later in order to download the *Certificate.*

377. When the application is made the *Public Key* generated is sent to the FNMT-RCM together with the corresponding possession tests (including the PKCS#10 electronic request) of the *Private Key,* so that the *Certificate* can then be issued.

378. The personal data and its processing shall be subject to the specific legislation.

379. This transfer of information to the FNMT-RCM shall be made by secure communications established for such purposes between the *Local Registration Authority Office (LRA Office)* and the FNMT-RCM.

12.2.2.1.3. Issue of the Server certificate (Step 3)

380. The request made by the *Local Registration Authority Office (LRA Office)* shall be validated by the personnel of the FNMT-RCM which will check that the request has been issued by an authorised *Responsible Party* and that the authorisation document has been received from the *Party Responsible for the Certificate* in order to make the request to issue a *Server certificate* for the domain name or IP in question.

381. FNMT – RCM shall check, through the information systems that the Local Registration Authority Officer (LRA Officer) authorised for each case have available to them, that the domain name or IP address to include in the Web Server *Certificate* is owned by the applicant *Organization or Competent Body*. In the event that that such a check is not possible, the FNMT-RCM shall accept the *Organization or Competent Body*'s ownership over said names or addresses on the basis of the corresponding application.

382. The FNMT-RCM shall also validate the PKCS#10 received in the application checking only the possession and correspondence of the pair of cryptographic *Keys* by the *Party Responsible for the Certificate.*

383. As such, once the data corresponding to the application is received and the corresponding checks made, the *Certificate* shall be issued.

384. Issuing *Web Server Certificates* involves the generation of electronic documents linking certain *Signature Verification Data* to a domain name or IP address for secure access to a web server under the control of the *Organization*, and their correspondence with the associated *Public Key.*

385. The issue of the *Certificates* subject to these *Policies* can only be made by the FNMT-RCM as *Certification Services Provider*, and there is no other body or entity capable of issuing them.

386. Through its *Electronic signature* the FNMT-RCM authenticates the *Certificate* and confirms the identity of the *Subscriber*, and its relationship with the domain name, IP address,

institution or system for which the *Server Certificate* is issued, in accordance with the information received by the *Local Registration Authority Office (LRA Office)*. On the other hand, and in order to avoid the manipulation of the information contained in the *Certificate*, the FNMT-RCM shall use the cryptographic mechanisms which provide authenticity and integrity to the *Certificate*.

387. In any event, the FNMT-RCM shall act effectively in order to:

- Check that the *Responsible Party* of the *Certificate* uses the *Private Key* corresponding to the *Public Key* linked to the identity of its *Signatory*. For this purpose, the FNMT-RCM shall check the correspondence between the *Private* Key and the *Public Key*.
- Achieve that the information included in the *Certificate* is based on the information provided by the corresponding *Local Registration Authority Office (LRA Office)*.
- Not ignore notorious events which could affect the reliability of the *Certificate*.
- Achieve that the *DN* (distinctive name) assigned in the *Certificate* is unique throughout the *Public Keys Infrastructure* of the FNMT-RCM.

388. In order to issue the *Server certificate* the following steps shall be followed:

1. Composition of the distinctive name (DN) of the *Web server certificate*

With the personal details of the domain name, IP address, institution or system collected during the *Certificate* application process, the distinctive name (DN) is composed according to the *X 500* standard, ensuring that said name makes sense and does not lead to any ambiguities. Pseudonyms are not considered a suitable means to identify Subscribers.

The *DN* for this type of *Certificates* is made up of the following elements:

DN≡CN, O, C

The attributes O, C represent the branch of the directory containing the entry corresponding to the *Web server certificates* issued to the *Organization* in question.

The *CN* attribute contains the domain name, IP address, institution or system for which the *Certificate* is issued.

The O attribute contains the name of the *Organization*.

The C attribute contains the code of the country of the *Organization*.

e.g.:

CN=**www.eui.europa.eu**

CN=213.170.35.210

In the case of “Wildcard” type *Web server certificates* the CN of the *Certificate* shall be:

CN=*.secondleveldomainname.TLD

where,

[secondleveldomainname] is the domain name owned by the *Organization or Competent Body*

[TLD] is the top level domain name under which the second level domain name is registered.

Once the distinctive name (*DN*) has been composed, the corresponding entry is created in the *Directory*, ensuring that the distinctive name is unique through the *Public Key Infrastructure* of the *Certification Services Provider*.

2. Generation of the *Certificate* according to the profile of the *web server certificate*

The *Server certificate* format shall be in accordance with the UIT-T X.509 version 3 format and in accordance with the applicable regulations.

The tables attached to this document contain the profile of this type of *Certificate*.

The *Certificate* shall also include the corresponding Policy identifier.

12.2.2.2. Publication of the Server certificate

389. Once the *Certificate* is generated by the *Certification Services Provider*, it will be published in the *Directory*, specifically in the entry corresponding to the *Organization*.

390. A communication that the *Certificate* is available for downloading will be sent to the email provided by the *Responsible Party.*

12.2.2.3. Downloading and installing Server certificates

391. Once the *Certificate* has been generated, a downloading mechanism is made available to the *Local Registration Authority Officer (LRA Officer)* in the registration application.

392. In this guided process the interested party will be asked to enter the CN for which the *Certificate* was issued, as well as the application code returned by the system at the end of the process.

393. If the *Certificate* has not for any reason been generated, this will be indicated when trying to download. Otherwise it will be provided to the interested party.

394. Finally, the *Local Registration Authority Officer (LRA Officer)* shall send the generated *Certificate* to the *Party Responsible,* which will install it in the server where the corresponding keys were generated.

12.2.2.4. Validity of the Server certificate

12.2.2.4.1. Expiry

395. The *Server certificates* issued under this *Certification Policy* by the FNMT-RCM shall be valid for the period defined in APPENDIX I: Identification of certification profiles, counting from the time of issue of the *Certificate,* provided that their validity is not extinguished. After that period and if the *Certificate* continues active, it will expire, and it shall be necessary to issue a new one if the *Subscriber* wishes to continue using the services of the *Certification Services Provider.*

12.2.2.4.2. Extinction of the validity

396. The *Server certificates* issued by the FNMT-RCM under this policy shall become without effect under the following circumstances:

a) Termination of the period of validity of the *Certificate*

b) The FNMT-RCM ceases its activity as a *Certification Services Provider*, unless, with the express prior consent of 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 when these circumstances occur.

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

397. The effects of the revocation or suspension of the *Certificate,* i.e. the extinction of its validity, shall take effect from the date on which the FNMT-RCM becomes reliably aware of any of the determining events and it is recorded in its *information and consultancy services about the state of validity of the certificates*.

12.2.2.5. Revocation of the Server certificate

12.2.2.5.1. Grounds for revoking the Server certificate

398. The following are grounds for revoking a *Server certificate*:

a) The revocation request by the authorised persons. The following shall under all circumstances lead to this request:

- The loss of the support of the *Certificate* or suspicion that its confidentiality has been compromised.
- The use by a third party of *Signature Creation Data,* corresponding to the *Signature Verification Data* contained in the *Certificate* and linked to the identity of the *Signatory.*
- The violation or putting in danger the secrecy of the *Signature Creation Data.*
- The non-acceptance by the *Organization or Competent Body* of the new conditions which may involve the issue of new *Declarations of Certification Practices,* during the period of one month following their publication.

b) Judicial or administrative decision which orders it, as well as the cases set out in the applicable legislation. .

c) Extinction or dissolution of the legal status of the *Subscriber.*

d) Inaccuracies or alterations in the data provided by the *Responsible Party* in order to obtain the *Certificate* or modification of the verified circumstances for its issue, as well as those relating to the position or the powers of representation, so that they are not now in accordance with the reality.

e) Breach of a substantial obligation in this *Certification Practice Statement* by the *Responsible Party, the Certificate Subscriber* or the personnel of the *Local*

Registration Authority Office (LRA Office) if it may affect the *Certificate* issue procedure.

f) Cancellation of the contract signed between the *Organization* and the FNMT-RCM.

g) Violation or putting in danger the secrecy of the *Signature Creation Data* of the - RCM with which it signs the *Certificates* that it issues.

399. Under no circumstances shall it be considered that the FNMT-RCM accepts any obligation to check the points mentioned in letters c) to e) of this section.

400. The actions constituting an offence of which the FNMT-RCM becomes aware performed in relation to the data or *Certificates*, the inaccuracies in the data or lack of diligence in its communication, including the grounds mentioned above, to the FNMT-RCM, shall exempt the FNMT-RCM from liability.

12.2.2.5.2. Effects of the revocation

401. The effects of the revocation or suspension of the *Certificate*, i.e. the extinction of its validity, shall take effect from the date on which the FNMT-RCM becomes reliably aware of any of the determining events and this is thus recorded in its *Information and consultation service on the state of the validity of the certificates.*

402. The revocation of *Certificates* involves, apart from its extinction, the end of the relationship and regime of use of the *Certificate* with the FNMT-RCM.

12.2.2.5.3. Procedure for the revocation

403. The revocation application for the *Server certificates* can be made during the validity period recorded in said *Certificate*.

404. The revocation of a *Server certificate* can be requested by the *Subscriber* through the *Local Registration Authority Referent (LRA Referent)* or the *Local Registration Authority Officer (LRA Officer).* Furthermore, the *Responsible Party* can request from the *Local Registration Authority Office (LRA Office)* to revoke or suspend it there are justifying grounds, under the terms contained in this *Particular Certification Policy and Practices.*

405. Without prejudice to the above, the FNMT-RCM can revoke the *Web server certificates* in the cases contained in the *Certification Practice Statement* and in the applicable legislation.

406. The *Responsible Party* or the *Subscriber* through a representative with sufficient capacity can request the revocation operation either personally at the corresponding *Local Registration Authority Office (LRA Office),* or remotely. The Local Registration Authority Officer (LRA Officer) must check the sufficient capacity of the applicant in order to carry out the revocation application.

407. In the revocation application process, the applicant shall communicate to the *Local Registration Authority Officer (LRA Officer)* the series number and the CN of the *Certificate* to revoke. This data shall be introduced by the latter in the registration application in order for the revocation to be executed of the *Certificate.*

408. As such, the *Local Registration Authority Officer (LRA Officer)* shall formalise the revocation request via the registration application, which will generate two forms with the application contract to be printed.

409. After the *Local Registration Authority Officer (LRA Officer)* confirms the identity of the applicant and their sufficient capacity, the *Local Registration Authority Officer (LRA Officer)* shall valid the data and send it to the FNMT-RCM.

410. The *Local Registration Authority Office (LRA Office)* must look after the forms supporting the application as a part thereof.

411. The FNMT-RCM shall receive that relevant information for the purposes of the revocation of a *Certificate* through the revocation application model that is presented, on paper or electronically, by the *Local Registration Authority Office (LRA Office).*

412. The personal data and their processing shall be subject to the specific legislation.

413. FNMT-RCM shall consider that the applicant to revoke a *Server Certificate* has sufficient capacity if the request is made through the corresponding *Local Registration Authority Office (LRA Office).* FNMT-RCM shall not assess the appropriateness of the revocation request when it is made through the aforementioned *Local Registration Authority Office (LRA Office).*

414. Once the FNMT-RCM has revoked the *Certificate,* the corresponding *List of Revoked Certificates* shall be published in the secure *Directory,* containing the series number of the revoked *Certificate,* the date and time of revocation and the reason for the revocation. Similarly, this information shall also be available via the OCSP protocol in the corresponding *Information service on the state of validity of the Certificates.*

APPENDIX I: IDENTIFICATION OF CERTIFICATION PROFILES

Table 1 - FNMT-RCM Root Certificate for the issue of certificates for the European Commission (Subordinated hierarchy to the Root Certificate of the FNMT-RCM)

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}).
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Root CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. Organization Unit	ou=AC RAIZ FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
5. Validity		15 years		Yes	
6. Subject		Certificate issuer entity (Subordinate CA)		Yes	
	6.1. Country	C=ES		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3. Common Name	cn=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280)

Field		Content	Critical	Mandatory	Specifications
7. Authority Key Identifier		Root entity public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign the subordinate CA certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the Root CA.
8. Subject Public Key Info		Public key of the subordinate CA for the Public Administration, encoded accordingly the cryptographic algorithm. In this case RSA Encryption	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. The length is 4096.
9. Subject Key Identifier		Subordinate CA public key identifier. Medium to identify certificates that contain a particular public key, and eases the building of certification paths.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage		Permitted usage of the certified keys.	Yes	Yes	Normalized in X509
	10.1. Digital Signature	0		Yes	Allows electronic signature.
	10.2. Content Commitment	0		Yes	Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment	0		Yes	It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment	0		Yes	It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement	0		Yes	For use in the Key Agreement process.
	10.6. Key Certificate Signature	1		Yes	Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature	1		Yes	CRL signature allowed. It is used in CA Certificates.
11. Certificate Policies		Certificate policy	No	Yes	
	11.1. Policy Identifier	2.5.29.32.0 (anyPolicy)		Yes	According to rfc3280: *"To promote interoperability, this profile RECOMMENDS that policy information terms consist of only 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 }"*

Field			Content		Critical	Mandatory	Specifications
	11.2. Policy Qualifier Id						
		11.2.1	11.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		11.2.3	11.2.4 User Notice	Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
12. CRL Distribution Point					No	Yes	
	12.1. Distribution Point 1		CRL distribution point 1 (ARL) ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint			Yes	UTF8String Path where the CRL resides (distribution point 1)
	12.2. Distribution Point 2		CRL distribution point 2 (ARL) http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl			Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
13. Authority Info Access					No		
	Access Method 1		Access method identification for revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)			Yes	OCSP (1.3.6.1.5.5.7.48.1)
	Access Location 1		http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder			Yes	OCSP service URL
	Access Method 2		Access method identification for additional information for validation process: 1.3.6.1.5.5.7.48.2 (ca cert)			Yes	Root CA certificate 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.*"
	Access Location 2		http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt			Yes	Root CA Certificate download URL.
14. Basic Constraints			This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.		Yes		

Field		Content	Critical	Mandatory	Specifications
	14.1. Subject Type	CA			Type of subject: Certification Authority
	14.2. Path Length	0			A zero value pathLenConstraint points out that no more intermediate CA certificates are allowed in the certification path.

Table 2 - Lightweight Certificate Profile

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM.		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The offered certificates have to have an operational period of at least one (1) year.*
6. Subject		Identification/description of the owner of / person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification		Yes	UTF8 String, maximum size 128 (rfc5280)

Field		Content	Critical	Mandatory	Specifications
		service subject. o= EUI Description			
	6.3.				
	6.4. Common Name	Name and surname as appears on identification document, preceded by the string "(MAIL)"		Yes	UTF8String (rfc5280). For instance : cn=(MAIL) JUAN ESPAÑOL
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public Key Algorithm and Subject Public Key for the certificate subject. In this case RSA Encryption with 2048 key lenght.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The key length shall be at least 1024 bits*
9. Subject Key Identifier		Subject or Key Owner public key identifier. Medium to identify certificates that contain a particular public key and eases the building of certification paths.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage		Permitted usage of the certified keys.	Yes	Yes	Normalized in X509
	10.1. Digital Signature	1			Allows electronic signature.
	10.2. Content Commitment	0			Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment	1			It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment	0			It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement	0			For use in the Key Agreement process.
	10.6. Key Certificate Signature	0			Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature	0			CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage		Extended or improved usage of the keys.		Yes	This extension points out one or more purposes for which the

Field			Content		Critical	Mandatory	Specifications
							public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
	11.1. Email protection		1.3.6.1.5.5.7.3.4		No	Yes	Email protection
12. Certificate Policies			Certificate policy		No	Yes	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.3 0.4.0.2042.1.3			Yes	Policy identifiers of the lightweight certificate.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Light weight certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names			Identification/Description of the Administrative Identity		No	Yes	
	13.1. rfc822 Name		Subscriber's e-mail.			Yes	For instance : rfc822Name=jespanol@meh.es
	13.2. Subscriber's name		OID 1.3.6.1.4.1.5734.1.1 = Subscriber's name.			Yes	For instance OID 1.3.6.1.4.1.5734.1.1 = Juan
	13.3. Subscriber's surname		OID 1.3.6.1.4.1.5734.1.2 = Subscriber's surname.			Yes	For instance OID 1.3.6.1.4.1.5734.1.2 = Espanol
14. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	
	14.1. Distribution Point 1		CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2		CRL distribution point 2 ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European%20Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)

Field		Content	Critical	Mandatory	Specifications
15. Authority Info Access			No	Yes	
	15.1. Access Method 1	Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	
	15.2. Access Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	
	15.3. Access Method 2	Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Issuer of the certificates issuer entity (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."*
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates.
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			From rf5280: *" This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	Subject Type	Final entity (value FALSE)		Yes	Other certificates cannot be issued with this certificate.

Table 3 Normalised Certificate Profile

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The offered certificates have to have an operational period of at least one (1) year.*
6. Subject		Identification/description of the owner of/person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service subject. o= EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				

Field		Content	Critical	Mandatory	Specifications
	6.4. Common Name	Name and surname as appears on identification document, preceded by the string "(AUTH)"		Yes	UTF8String (rfc5280). For instance : cn=(AUTH) JUAN ESPAÑOL
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public Key Algorithm and Subject Public Key for the certificate subject. In this case RSA Encryption with 2048 key lenght.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The key length shall be at least 1024 bits*
9. Subject Key Identifier		Subject or Key Owner public key identifier. Medium to identify certificates that contain a particular public key and eases the building of certification paths.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage		Permitted usage of the certified keys.	Yes	Yes	Normalized in X509
	10.1. Digital Signature	1			Allows electronic signature.
	10.2. Content Commitment	0			Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment	0			It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment	0			It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement	0			For use in the Key Agreement process.
	10.6. Key Certificate Signature	0			Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature	0			CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage		Extended or improved usage of the keys.		Yes	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.

Field			Content		Critical	Mandatory	Specifications
	11.1. Client Authentication		1.3.6.1.5.5.7.3.2		No	Yes	Client Authentication
	11.2. Any Extended Key Usage		Other purposes (see comment in “Specifications”column”) 2.5.29.37.0		No	Yes	*[RFC5280]: Certificate using applications MAY require that a particular purpose be indicated in order for the certificate to be acceptable to that application. If a CA includes extended key usages to satisfy such applications, but does not wish to restrict usages of the key, the CA can include the special keyPurposeID* ***anyExtendedKeyUsage****. If the anyExtendedKeyUsage key purpose is present, the extension SHOULD NOT be critical.*
12. Certificate Policies			Certificate policy		No	Yes	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.2 0.4.0.2042.1.1			Yes	Policy identifiers of the normalized certificate.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Normalized certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names			Identification/Description of the Administrative Identity		No	Yes	
	13.1. rfc822 Name		Subscriber’s e-mail.			Yes	For instance : rfc822Name=jespanol@meh.es
	13.2. Subscriber’s name		OID 1.3.6.1.4.1.5734.1.1 = Subscriber’s name.			Yes	For instance OID 1.3.6.1.4.1.5734.1.1 = Juan
	13.3. Subscriber’s surname		OID 1.3.6.1.4.1.5734.1.2 = Subscriber’s surname.			Yes	For instance OID 1.3.6.1.4.1.5734.1.2 = Espanol
14. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	
	14.1. Distribution Point 1		CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String Path where the CRL resides (distribution point 1)

Field		Content	Critical	Mandatory	Specifications
	14.2. Distribution Point 2	CRL distribution point 2 ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European%20Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access			No	Yes	
	15.1. Access Method 1	Identifier of the access method to the revocation information: : 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	
	15.2. Access Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	
	15.3. Access Method 2	Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Issuer of the certificates issuer entity (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.”*
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			From rf5280: *“ This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	16.1. Subject Type	Final entity (value FALSE)		Yes	Other certificates cannot be issued with this certificate.

Table 4 - Qualified Certificate Profile

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o= FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The offered certificates have to have an operational period of at least one (1) year.*
6. Subject		Identification/description of the owner of / person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280))
	6.2. Organization	Title ("official" name of organization) of the certification service subscriber . o=EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				

Field		Content	Critical	Mandatory	Specifications
	6.4. Common Name	Name and surname as appears on identification document, preceded by the string "(SIGN)"		Yes	UTF8String (rfc5280). For instance : cn=(SIGN) JUAN ESPAÑOL
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public Key Algorithm and Subject Public Key for the certificate subscriber. In this case RSA Encryption with 2048 key lenght.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The key length shall be at least 1024 bits*
9. Subject Key Identifier		Subscriber or key owner public key identifier. Medium to identify certificates that contain a particular public key, and eases the building of certification paths.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage		Permitted usage of the certified keys.	Yes	Yes	Normalized in X509
	10.1. Digital Signature	0			Allows electronic signature.
	10.2. Content Commitment	1			Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment	0			It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment	0			It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement	0			For use in the Key Agreement process.
	10.6. Key Certificate Signature	0			Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature	0			CRL signature allowed. It is used in CA Certificates.
11. Qualified Certificate Statements		Qualified extensions.	No		ETSI TS 101 862 Defines the inclusion of certain declarations for qualified certificates.
	11.1. QcCompliance	Certificate issued as a Qualified Certificate		Yes	Indicates whether the certificate is acknowledged only if it is not explicit in the indicated policies

Field			Content		Critical	Mandatory	Specifications
							in the corresponding extension.
	11.2. QcRetentionPeriod		15 years			Yes	Number of years from certificate expiry date which registered details and other relevant information are available. In this case the law states "To conserve registered in a secure way all the information and documentation related to a qualified certificate and the CPD´s in force in each moment, for at least 15 years counted from the moment of its issue, so that the signatures done with it might be verified…"
	11.3. QcLimitValue		200 €			Yes	Limits of responsibility
	11.4. QcSSCD		Keys generated in a SSCD			Yes	Points out that the private key of the certificate is stored in a Secure Signature Creation Device in compliance with Annex III of the European Parliament directive 1999/91/EC regarding a communitary framework for electronic signatures. This value will only be filled when it can be assured irrefutably (technical mechanism or audited process) that the private key has been generated in a SSCD.
12. Certificate Policies			Certificate policy		No	Yes	
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.1 0.4.0.1456.1.1			Yes	Policy identifiers of the qualified certificate.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Qualified certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names					No	Yes	
	13.1. rfc822 Name		Subscriber's e-mail.			Yes	For instance : rfc822Name=jespanol@meh.es
	13.2. Subscriber's name		OID 1.3.6.1.4.1.5734.1.1 =			Yes	For instance OID

Field		Content	Critical	Mandatory	Specifications
		Subscriber’s name.			1.3.6.1.4.1.5734.1.1 = Juan
	13.3. Subscriber’s surname	OID 1.3.6.1.4.1.5734.1.2 = Subscriber’s surname.		Yes	For instance OID 1.3.6.1.4.1.5734.1.2 = Espanol
14. CRL Distribution Point		Informs how information about the CRL associated to the certificate is obtained.	No	Yes	
	14.1. Distribution Point 1	CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2	CRL distribution point 2. ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA %20CA,ou=European%20Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)		Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access			No	Yes	
	15.1. Access Method 1	Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)		Yes	
	15.2. Access Location 1	http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder		Yes	
	15.3. Access Method 2	Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		Yes	Issuer of the certificates issuer entity (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.*”
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			From rf5280: “ *This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	16.1. Subject Type	Final entity (value FALSE)		Yes	Other certificates cannot be issued with this certificate.

Table 5 - Web server Certificate Profile (Common Name type)

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Maximum validity limited by "Identification and Signature Scheme. Profiles of Certificates"
6. Subject		Identification/description of the owner of / person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o= EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				
	6.4. Common Name	Domain on which this certificate is valid Cn=www.domain.com		Yes	UTF8String (rfc5280).

Field		Content	Critical	Mandatory	Specifications
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public key of the site, encoded accordingly the cryptographic algorithm. In this case RSA Encryption.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. The length is 2048.
9. Subject Key Identifier		Subscriber or Key Owner public key identifier. Medium to identify certificates that contain a particular public key and eases the building of certification paths.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage		Permitted usage of the certified keys.	Yes	Yes	Normalized in X509
	10.1. Digital Signature	1			Allows electronic signature.
	10.2. Content Commitment	0			Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment	1			It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment	0			It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement	0			For use in the Key Agreement process.
	10.6. Key Certificate Signature	0			Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature	0			CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage		Extended or improved usage of the keys.		Yes	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
	11.1. Server Authentication	1.3.6.1.5.5.7.3.1	No	Yes	Server Authentication
	11.2. Email protection	1.3.6.1.5.5.7.3.4	No	Yes	Email protection
12. Certificate Policies		Certificate policy	No	Yes	

Field			Content		Critical	Mandatory	Specifications
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.4			Yes	Certificate policy identifier for SSL/TLS Server.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	TLS Server certificate. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names			Identification/Description of the Administrative Identity		No	Yes	
	13.1. dns Name		www.domain.com			Yes	
14. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	
	14.1. Distribution Point 1		CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2		CRL distribution point 2 ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access					No	Yes	
	15.1. Access Method 1		Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)			Yes	
	15.2. Access Location 1		http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder			Yes	
	15.3. Access Method 2		Identifier of the method of access to the information of the additional certificates needed for validation:			Yes	Issuer of the certificates issuer entity (Root CA) From rfc 5280: *"the id-ad-*

Field		Content	Critical	Mandatory	Specifications
		1.3.6.1.5.5.7.48.2 (ca cert)			*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.”*
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.			From rf5280: *“ This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	Subject Type	Final entity (value FALSE)		Yes	Other certificates cannot be issued with this certificate.

Table 6 - Web server Certificate Profile (Wildcard type)

Field		Content	Critical	Mandatory	Specifications
1. Version		2		Yes	Integer:=2 ([RFC5280] This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2)(X509v3).
2. Serial Number		Certificate unique identifier number.		Yes	Integer. SerialNumber = ex: 111222. Automatically set by the Certification Entity. [RFC5280]. It will be a positive integer, not bigger than 20 octets (1- 2^{159}). The Serial Number will be assigned randomly.
3. Signature Algorithm		Sha256withRsaEncryption		Yes	Identifies the type of algorithm used (OID 1.2.840.113549.1.1.11)
4. Issuer Distinguish Name		Certificate issuer entity (Subordinate CA)		Yes	
	4.1. Country	C=ES		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	4.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o=FNMT-RCM		Yes	UTF8 String, maximum size 128 (rfc5280)
	4.3. common Name	CN=ISA CA		Yes	UTF8 String, maximum size 128 (rfc5280).
5. Validity		4 years		Yes	Call for Tenders, DIGIT/R2/PO/2009/035, PKI SERVICES 1.2.1. Key generation/issuing certificates *The offered certificates have to have an operational period of at least one (1) year.*
6. Subject		Identification/description of the owner of / person responsible for the certified keys.		Yes	
	6.1. Country	C=XY Country which the EUI belongs to.		Yes	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	6.2. Organization	Title ("official" name of organization) of the certification service provider (certificate issuer). o= EUI Description		Yes	UTF8 String, maximum size 128 (rfc5280)
	6.3.				

Field		Content	Critical	Mandatory	Specifications
	6.4. Common Name	Domain on which this certificate is valid CN=*.domain.com		Yes	UTF8String (rfc5280). For instance : CN=*.domain.com
7. Authority Key Identifier		CSP public key identifier. Medium to identify the public key corresponding to the private key used by the CA to sign a certificate.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). Matches the field Subject Key Identifier of the issuer CA.
8. Subject Public Key Info		Public key of the site, encoded accordingly the cryptographic algorithm. In this case RSA Encryption.	No	Yes	Field to transport the Public Key and to identify the algorithm with which the key is used. The length is 2048.
9. Subject Key Identifier		Subscriber or Key Owner public key identifier. Medium to identify certificates that contain a particular public key and eases the building of certification paths.	No	Yes	RFC 5280: Is composed of the 20-bytes SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
10. Key Usage		Permitted usage of the certified keys.	Yes	Yes	Normalized in X509
	10.1. Digital Signature	1			Allows electronic signature.
	10.2. Content Commitment	0			Points out to the software that uses the certificate if it must allow the user to know the signed content.
	10.3. Key Encipherment	1			It is used for management and transport of keys to establish secure sessions.
	10.4. Data Encipherment	0			It is used to encipher details which are not cryptographic keys.
	10.5. Key Agreement	0			For use in the Key Agreement process.
	10.6. Key Certificate Signature	0			Certificate signature allowed. It is used in CA Certificates.
	10.7. CRL Signature	0			CRL signature allowed. It is used in CA Certificates.
11. Extended Key Usage		Extended or improved usage of the keys.		Yes	This extension points out one or more purposes for which the public key certificate may be used as well as or instead of the basic usages indicated in the Key Usage extension.
	1.1. Server Authentication	1.3.6.1.5.5.7.3.1	No	Yes	Server authentication.
	1.2. Email protection	1.3.6.1.5.5.7.3.4	No	Yes	Email protection
12. Certificate Policies		Certificate policy	No	Yes	

Field			Content		Critical	Mandatory	Specifications
	12.1. Policy Identifier		1.3.6.1.4.1.5734.3.4.4			Yes	Policy identifier of the SSL/TLS Server certificate.
	12.2. Policy Qualifier Id					Yes	
		12.2.1	12.2.2 CPS Pointer	http://www.cert.fnmt.es/dpcs/		Yes	IA5String String. URL for the usage conditions.
		12.2.3	12.2.4 User Notice	Certificate issued under wildcard policy. Under the usage conditions asserted in the FNMT-RCM CPS (106, Jorge Juan street,28009, Madrid, Spain).		Yes	UTF8 String. maximum size 200 characters.
13. Subject Alternative Names			Identification/Description of the Administrative Identity		No	Yes	
	13.1. dns Name		*.domain.com			Yes	
14. CRL Distribution Point			Informs how information about the CRL associated to the certificate is obtained.		No	Yes	
	14.1. Distribution Point 1		CRL distribution point 1 http://www.cert.fnmt.es/crls_ISAca/CRL<xxx*>.crl *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String Path where the CRL resides (distribution point 1)
	14.2. Distribution Point 2		CRL distribution point 2 ldap://ldapISAca.cert.fnmt.es/CN=CRL<xxx*>,cn=ISA%20CA,ou=European Commission,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: integer number identifier of the CRL(Partitioning CRL)			Yes	UTF8String. Path of LDAP service where the CRL resides. (distribution point 2)
15. Authority Info Access					No	Yes	
	15.1. Access Method 1		Identifier of the access method to the revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)			Yes	
	15.2. Access Location 1		http://ocspISAca.cert.fnmt.es/ocspISAca/OcspResponder			Yes	
	15.3. Access Method 2		Identifier of the method of access to the information of the additional certificates needed for validation: 1.3.6.1.5.5.7.48.2 (ca cert)			Yes	Issuer of the certificates issuer entity (Root CA) From rfc 5280: *"the id-ad-caIssuers OID is used when the additional information lists certificates that were issued to*

Field		Content	Critical	Mandatory	Specifications
					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."
	15.4. Access Location 2	http://www.cert.fnmt.es/certs/ISACA.crt		Yes	URL for the download of additional certificates to validate the certification path. In this case the certificate path is the certificate of FNMT-RCM used for the issuance of this type of certificates
16. Basic Constraints		This extension is used to identify whether the certification subject is a CA and the maximum depth level allowed for the certification path.	Yes		From rf5280: *" This extension MAY appear as a critical or non-critical extension in end entity certificates.*
	Subject Type	Final entity (valuer FALSE)		Yes	Other certificates cannot be issued with this certificate.