Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SPECIFIC CERTIFICATION POLICY AND PRACTICES FOR
FNMT CLASS 2 CA COMPONENT CERTIFICATES

	NAME	DATE
Prepared by:	FNMT-RCM / v1.4	06/02/2013
Revised by:	FNMT-RCM / v1.4	06/02/2013
Approved by:	FNMT-RCM / v1.4	06/02/2013

Reference: DPC/PC-DPC-C2COMP-0104/SGPSC/2013

Document classified as: Public

BACKGROUND OF THE DOCUMENT			
Version	**Date**	**Description**	**Author**
1.0	01/08/2010	Creation of the document in accordance with that established in Appendix VI of the Certification Practices Statement version 2.7. The certificate renewal procedure is eliminated. The extension extKeyUsage is added to Code Signing Certificates. The extension extKeyUsage is added to Web Server Certificates.	FNMT-RCM
1.1	19/07/2011	New type of component certificate for time stamping units. New type of component certificate for web servers with several domain names (SAN).	FNMT-RCM
1.2	23/04/2012	The sections relating to information regarding the management of the policies in this document are eliminated because it is already included in the GCPS. The validity period of the certificates is changed (except for the TSU, which is kept as two years). The validity period is reduced from 4 to 2 years.	FNMT-RCM
1.3	29/08/2012	The profile of Code Signing Certificates is modified to mark the extension extKeyUsage as “critical”.	FNMT-RCM
1.4	06/02/2013	The extended Usage of “emailProtection” Key is added as an option to SSL Servers Certificates.	FNMT-RCM

INDEXES

INDEX OF CONTENTS

INDEX OF TABLES

1. INTRODUCTION AND CERTIFICATE TYPOLOGY

1. *Component Certificates* are the *Certificates* issued by the FNMT-RCM under this *Certification Policy,* which associate *Signature Verification Data* to a computer *Component* or application of which a specific natural or legal person acts as controller. That person is the *Controller* of the *Component* or application. The *Private Key* associated to the *Public Key* shall be under the responsibility of the *Component Controller,* who shall act as representative of the natural or legal person who owns the *Component* under the *Certificate.*

2. For purposes of article 16 of Law 59/2003, *Component Certificates* shall be considered to be electronic *Certificates* when there is an unequivocal association between the *Component Certificate* and the natural or legal person who is the *Holder* of the *Certificate*. The FNMT-RCM shall issue these *Certificates* when applied for by the members of the *Electronic Community* for the different relations that may be established and when their use is not prohibited or restricted under the applicable legislation.

3. The FNMT-RCM shall not be held liable for actions carried out using this type of *Certificates* with abuse or lack of authority and/or when decisions are made by the member of the *Electronic Community* who is the *Holder of the Certificate* which affect the validity of the *Controller's* authority. Therefore, any amendment, revocation or restriction affecting that authority shall be ineffective as against the FNMT-RCM unless reliably notified.

4. These *Component Certificates* are issued and signed by the FNMT-RCM and are to be installed in and used by servers with SSL support, software components signature applications, *Time Stamping Units* or applications which act as clients of the advanced services provided by the FNMT-RCM, for the purpose of inheriting the trust in the FNMT-RCM as *Certification Services Provider*. *Component Certificates* may only be obtained by entities which have signed a contract or an agreement with the FNMT-RCM, under which they are part of the *Electronic Community*, as described in the *Certification Practices Statement* of the FNMT-RCM.

5. These *Component Certificates* do not carry the legal effect of recognised equivalence of the electronic signature with actions carried out using the traditional handwritten signature. Nevertheless, they have the legal effect given to certificates of this nature under the applicable legislation. FNMT-RCM shall only issue these Certificates for use within the scope of the *Electronic Community* for actions which are not incompatible with the scope and use of the respective *Certificate* to which the component is unequivocally associated.

6. As *Certification Services Provider*, the FNMT-RCM reserves the right to refuse to issue or to revoke this type of *Certificates* if the user of the *Certificate* and/or the *Controller* of the *Component* or application who uses the *Certificate* makes improper use of the *Certificate* by infringing the industrial or intellectual property rights of third parties over the applications, websites or equipment sought to be protected with such *Certificates*, or uses the *Certificate* to deceive or mislead over the ownership of such websites, applications, *Time Stamping Units* or equipment. In particular, this reservation of rights may be enforced by the FNMT-RCM when in the use of such *Certificates* the following principles are violated:

- Safeguarding public order, criminal investigations, public security and national defence.

- Protecting public health or the health of natural or legal persons who hold the status of consumers or users, including when acting as investors.

- Respecting the dignity of persons and the principle of non-discrimination for reasons of race, sex, religion, opinion, nationality, disability or any other personal or social circumstance, and

- Protecting youths and children.

7. The FNMT-RCM shall be exempt and held harmless from any claim or demand arising from improper use of the *Component Certificates* by:

   - its *Holder* or *Subscriber* or

   - the owner or controller of the equipment or applications using the *Certificate*

   in both cases, who fail to comply with that established in the *Certification Practices Statement.*

8. The FNMT-RCM issues the following types of *Component Certificates* under this *Certification Policy*:

   - Server *Certificate*: Is the *Certificate* that enables a web server or URL to be identified.

     Within this category of server *Certificates* with the functionality to identify a web server or URL, the FNMT-RCM has two special types of **server *Certificates*: the so-called Wildcard certificates**, which enable their *Holders*, who are members of the *Electronic Community*, to secure all the sub-domains associated to a specific domain without having to acquire and manage many electronic *Certificates;* and the so-called **SAN certificates**, which enable their *Holders* to secure several domains with a single electronic Certificate by including the domains that the *Holder* wishes to secure in the Subject Alternative Name.

     The FNMT-RCM also issues **electronic *Certificates* for *RADIUS* servers** (Remote Authentication Dial-In User Service), which consist of a standard protocol included in Windows 2000used to facilitate connectivity in wireless local area networks.

   - Code signing *Certificate*: Is the *Certificate* used in applications, which enables to sign code executable like *Java applets.*

   - *Certificate* for *Time Stamping Units*: Is the *Certificate* used by a *Time Stamping Unit* (belonging to a *Time Stamping Authority*) to issue Time Stamps.

   - *Certificate* for clients of advanced services of the FNMT-RCM: Is the *Certificate* used in applications which act as clients of advanced services made available to the *Electronic Community* by the FNMT-RCM.

- *Certificate* for other computer *Components*: Is a different *Certificate* from the ones mentioned above used to distinguish applications from others and to establish secure sessions.

2. STRUCTURE OF THE DOCUMENT

9. The FNMT-RCM structures its *Certification Practices Statement* in several documents:

   - The so-called "*General Certification Practices Statement of the FNMT-RCM*" or GCPS, aimed at providing public information on the general conditions and characteristics of the certification services offered by the FNMT-RCM as *Certification Services Provider*.

   - The appendixes deemed necessary to provide public information on the conditions of use, restrictions, responsibilities, properties and any other information considered specific to each type of *Certificate*. These appendixes shall hold the status of *Specific Certification Policy and Practices* to the type of *Certificate* concerned.

10. Therefore, the *Certification Practices Statement* for a specific type of *Certificate* issued by the FNMT-RCM is considered to be the set of documents made up of the GCPS and all the appendixes which specify, develop or particularise questions related to the type of *Certificate* concerned, i.e., the specific *Certification Policy and Practices* for that type of *Certificate*.

11. For the purpose of interpreting this appendix, the "Definitions" section of the GCPS and of this document should be borne in mind.

12. The objective of this document is to provide public information on all the practices, conditions and characteristics of the certification services provided by the FNMT-RCM as *Certification Services Provider* in relation to the lifecycle of the *Component* electronic *Certificates*.

13. This document arises from and is an integral part of the *Certification Practices Statement* of the FNMT-RCM with regard to the *Component Certificates*. It contains the *Certification Policy* for this type of *Certificates* and the *Certification Practices* employed in their lifecycle.

14. In short, these *Specific Certification Policies* and *Practices* pinpoint that set out in the main body of the GCPS and are therefore an integral part of the GCPS. Consequently, both documents make up the *Certification Practices Statement* of the FNMT-RCM for the *Component Certificates*. Thus, that described in this document is only applicable to the group of *Certificates* characterised and identified in these *Specific Certification Policies and Practices,* which may also take on particularities established in the *Issuance Law* concerning the *Certificate* or respective group of *Certificates*, in the event of there being specific characteristics or functionalities.

3. DEFINITIONS

15. For the purposes of this document the following definitions are added to the ones contained in the GCPS:

- *(Computer) Component*: Set of interrelated elements to perform a computer function.
- *Component Certificate*: *Certificate* used by a computer *Component* to increase the functionality or guarantees for which it was designed.
- *Component Controller*: Natural or legal person responsible for the management and control of the computer *Component* for which a *Component Certificate* is requested. The *Component Controller* shall also be the *Holder* and *Subscriber* of this type of *Certificates* (See GCPS).
- *Representative of the Component Controller*: Natural person with sufficient authority to apply for the *Certificate* on behalf of the *Controller* of the *Component* for which the *Certificate* is issued.
- *Component Certificate Controller*: Natural or legal person responsible for the management and control of the *Component Certificate*.
- *Applicant*: See GCPS. In the context of this document, we consider the *Applicant* to be the person who requests an operation related to the *Certificate* and is responsible for the safekeeping of the *Electronic Signature Creation Data*. This person shall be the *Component Certificate Controller* and shall be authorised by the *Component Controller* or his or her *Representative*.

4. ORDER OF PREVALENCE

16. The order of prevalence is the following:

- These *Specific Certification Policies and Practices* for *Component Certificates* are part of the *Certification Practices Statement* and have prevalence, in that regarding and specific to this type of *Certificate*, over that established in the *General Certification Practices Statement.*

  Consequently, in the event of a contradiction between this document and that established in the GCPS, that set out in this document shall have preference.

- The *Issuance Law* concerning each *Certificate* or group of *Certificates* shall, where appropriate, due to its specific nature, be the special law with prevalence over that established in these *Specific Certification Policies and Practices*. The *Issuance Law*, if established, shall be set out in the related document to be signed by the FNMT-RCM and the *User Entity*, and/or in the conditions of use or issuance contract, and/or in the *Certificate* itself.

5. CERTIFICATION POLICY FOR FNMT CLASS 2 CA COMPONENT CERTIFICATES

5.1. IDENTIFICATION

17. This *Certification Policy* of the FNMT-RCM for the issuance of *Component Certificates* has the following identification:

Table 1 – Certification Policy Identification

Name	*Component Certificates Certification Policy* of the FNMT-RCM (FNMT Class 2 CA)
Reference/OID	1.3.6.1.4.1.5734.3.6
Version	1.0
Issue date	1 January 2004
Related GCPS	General Certification Practices Statement of the FNMT-RCM
Location	http://www.ceres.fnmt.es/dpcs

5.2. COMMUNITY AND SCOPE OF APPLICATION

18. This *Certification Policy* is applicable to the issuance of electronic *Certificates* with the following characteristics:

- They are the *Certificates* issued by the FNMT-RCM which associate specific *Signature Verification Data* to a computer *Component* or application of which a specific natural or legal person acts as controller. That person is the controller of the *Component* or application.

- They are not issued as *Recognised Certificates.*

- The *Certificates* under this *Certification Policy* are issued for *User Entities* which are part of the *Electronic Community* as defined in the "Definitions" section of the GCPS of the FNMT-RCM.

5.3. LIABILITY AND OBLIGATIONS OF THE PARTIES

19. This *Certification Policy* covers the obligations and liability of the parties involved in the issuance and use of the *Component Certificates* issued under this policy.

20. The FNMT-RCM shall not be held liable for the use of *the Component Certificates* should the *Controller* and/or *Holder* of the associated *Electronic Certificate* carry out actions without authority or exceeding his or her authority, and there has been no reliable notification enabling the desired effects to be transferred to the administration of the *Certificates*.

5.3.1. Liability of the parties

21. To be able to use the *Certificates* issued by the FNMT-RCM one must previously be part of the *Electronic Community* and acquire the status of *User Entity*. Outside the *Electronic Community* one should not trust a *Certificate* or an *Electronic Signature* based on a *Certificate*.

22. In any case, should a third party rely on that trust, no cover shall be given under the *Certification Practices Statement* and there shall be no entitlement to claim or take legal action against the FNMT-RCM for damage, loss or disputes arising from the use of or trust in a *Certificate.*

5.3.1.1. Liability of the Certification Services Provider

23. The FNMT-RCM is only liable for the correct personal identification of the *Applicant,* and not his or her characteristics or other information contained in the *Certificate*. With regard to this information, the FNMT-RCM merely expresses it in a *Certificate* for which it has been given proof of the identity of its *Holder* by means of a public document.

24. It is a "sine qua non" condition for the application of the guarantees, obligations and liability, that the damage or the event was produced in the scope of the *Electronic Community* as defined in the GCPS.

25. The FNMT-RCM shall only be held liable for deficiencies in the proper procedures of its activity as *Certification Services Provider*, and in accordance with that established in these *Certification Policies* or in the Law, and under no circumstances shall be held liable for the actions of or the losses incurred by the *Controllers*, *Holders, Subscribers* or *User Entities* of the *Component Certificate* or third parties involved, which are not due to errors attributable to FNMT-RCM in the aforementioned issuance and/or administration of the *Certificates* procedures.

26. The FNMT-RCM shall not be held liable in cases of acts of God, force majeure, terrorist attacks, wild strikes and actions which constitute a crime or an offense and affect the provider's infrastructure, unless there has been serious negligence on the part of the institution. In any case, in the respective contracts and/or agreement, the FNMT may establish additional liability limitation clauses to the ones contained in this document.

27. The FNMT-RCM shall not be held liable to persons who have made negligent use of the *Certificates*. For these purposes, negligence shall be understood as failure to observe that established in the *Certification Practices Declaration*, and in particular that established in the sections on the obligations and liability of the parties.

28. The FNMT-RCM shall not be held liable for any software not directly supplied by the FNMT-RCM.

29. The FNMT-RCM does not guarantee the cryptographic algorithms and shall not be held liable for damage caused by successful external attacks to the cryptographic algorithms used, provided that the FNMT-RCM exercised due diligence in accordance with the current state of the technique and acted in accordance with that established in this *Certification Practices Statement* and in the Law.

30. In the specific case of the *Component Certificates* used in the *Time Stamping Units* belonging to third-party *Time Stamping Authorities*, it is hereby stated that the FNMT-RCM shall not be held liable for, and does not guarantee, any aspect of the *Time Stamping* service offered by the entities which are the *Holders* of such *Units* and *Time Stamping Authorities*. In particular, the exemption from liability shall cover the administration of all the aspects related to the information systems employed by such *Units* or *Authorities* and the validity of the time sources, or their synchronism, employed in the service.

31. In any case, with the status of penalty clause, the amounts to be paid out by FNMT-RCM by legal requirement to injured third parties or members of the *Electronic Community* for damage and losses, in the absence of specific regulation in the contracts and agreements, is limited to a maximum of SIX THOUSAND EUROS (6,000€).

5.3.1.2. Liability of the Applicant

32. The *Applicant* shall be held liable for the truthfulness and accuracy of the information submitted during the *Certificate* application process.

33. The *Applicant* shall hold harmless and defend the FNMT-RCM at his or her expense against any action taken against this institution as a result of the falseness of the information supplied in the aforementioned *Certificate* issuing procedure, or against any damage or loss suffered by the FNMT-RCM as a result of any act or omission by the *Applicant.*

5.3.1.3. Liability of the Component Controller (Holder and Subscriber)

34. It shall be the *Component Controller's* obligation, and consequently his or her responsibility, to advise the FNMT-RCM of any change in the status or information contained in the *Certificate,* for the purpose of revoking and issuing a new one.

35. The *Subscriber* shall be liable to the *User Entities* or, as the case may be, to third parties, for inadequate use of the *Certificate*, falseness in the affirmations contained in the *Certificate,* or acts and omission which cause damage or losses to the FNMT- RCM or to third parties.

36. The *Component Controller* shall be liable for and consequently obliged to refrain from using the *Certificate* should the *Certification Services Provider* cease to carry out the issuing of *Certificates* activity which gave rise to the issue of the *Certificate* in question, provided that the subrogation established in the law has not taken place. In any case, *the Component Controller* shall not use the *Certificate* in cases where the *Provider's Signature Creation Data* may be threatened and/or compromised and this has been communicated by the Provider or, as the case may be, it is known by the *Component Controller*.

5.3.1.4. Liability of the User Entity

37. It is the *User Entity's* responsibility, unless this obligation is contracted out to the FNMT-RCM, to verify the *Electronic Signatures* of the documents and check the state of the *Certificates*, and under no circumstances shall the authenticity of the documents or *Certificates* be assumed without having made these verifications.

38. It shall be held that the *User Entity* has failed to act with due diligence if it trusts an Electronic Signature based on a *Certificate* issued by the FNMT-RCM without having observed that established in the *Certification Practices Statement* and ascertained that the *Electronic Signature* in question can be verified by reference to a valid *Certification Chain*.

39. If the circumstances point to the need for additional guarantees, the *User Entity* should obtain additional guarantees to ensure that that trust is reasonable.

40. Furthermore, it shall be the *User Entity's* responsibility to observe that established in the *Certification Practices Statement* and any possible amendments to it, paying particular attention to the use restrictions established in this *Certification Policy* for the *Certificates*.

5.3.2. Obligations and guarantees of the parties

5.3.2.1. Obligations and guarantees of the Certification Services Provider

41. The FNMT-RCM shall not be bound by other guarantees or obligations besides those established in the applicable sector regulations and in the *Certification Practices Statement*.

42. Notwithstanding that established in the legislation on the electronic signature and its implementation regulations, as well as in the specific regulations, the *Certification Services Provider* undertakes to:

43. Before issuing the *Certificate*:

- Identify and check the identity and personal circumstances of the *Applicant* of the *Certificate* in accordance with that established in the *Certification Practices Statement*. Under no circumstances shall *Certificates* be issued to minors unless they hold the status of emancipated minors.

  In any case, for the aforementioned purposes, the *Certification Services Provider* shall adhere to that established in the specific legislation on the functionalities provided for the electronic National Identity Document.

- During the application process, check the data relating to the formation and legal personality of the entity and the scope and validity of the *Applicant's* representation powers, and require substantiation of the reasons for the representation. All these verifications shall be carried out in accordance with that established in the *Specific Certification Practices* contained in this document.

  In the processes of verifying the aforementioned points, the FNMT-RCM may carry out such verifications through publicly authorised third parties, the cost of which, if carried out, shall be met by the *Applicant*.

- Check that all the information contained in the *Certificate* application is in keeping with the information supplied by the *Applicant*.

- Check that the *Component Certificate Controller* is in possession of the *Private Key* which, once the *Certificate* is issued, shall constitute the *Signature Creation Data* corresponding to the *Signature Verification Data* contained in the *Certificate,* and check their complementarity.

- Guarantee that the procedures followed ensure that the *Private Keys* which constitute the *Signature Creation Data* are generated without making copies or giving rise to their storage by the FNMT-RCM.

- Communicate the information to the interested party or *Applicant* in such a way that its *Confidentiality* is ensured.

- Make the *Certification Practices Statement* and all information relevant to the procedures associated to the life cycle of the *Certificates* under this *Policy* available to the *Applicant* and interested controllers (http://www.ceres.fnmt.es), in accordance with the applicable regulations.

44. Retention of information by the FNMT-RCM

- Retain all information and documentation related to each *Certificate* in appropriate security conditions for fifteen (15) years after the *Certificate* issue date, so that the signatures made with the *Certificate* may be verified.

- Keep a safe and updated *Certificates Directory,* in which issued *Certificates* and their validity are identified, including, in the form of *Revocation Lists,* the identification of *Certificates* which have been revoked. The integrity of this *Directory* shall be protected by utilising systems in keeping with the specific regulatory provisions adopted in Spain and, as the case may be, in the EU.

- Provide an information and consultation service on the state of the *Certificates*.

- Establish a dating mechanism that enables to determine with exactitude the date and time a *Certificate* was issued or its validity extinguished or suspended.

- Retain the *Certification Practices Statement* for 15 years after derogation due to the publication of a new version, in appropriate security conditions.

45. Personal Data Protection

- The FNMT-RCM undertakes to stay abreast of and comply with the legislation in force on Personal Data Protection, essentially Organic Law 15/1999 of 13 December, on Personal Data Protection. This includes a commitment by the FNMT-RCM to comply with the obligations established in the aforementioned law with regard to

information to the affected parties, declaration of files to the Spanish Data Protection Agency and retention of and access to information, as well as with the security measures established in the respective regulations. Furthermore, the FNMT-RCM guarantees that the utilisation of the personal data collected shall be confined to the purposes for which it was collected.

- To learn more about the data protection policy followed by the FNMT-RCM and how the data is used please consult the GCPS.

46. Revocation of Certificates

- On the revocation of *Certificates* and the obligations that the FNMT-RCM undertakes to assume in this regard, please read the *Certificates* revocation procedure described in this document.

47. Cessation of the activity of the FNMT-RCM as *Certification Services Provider*

- This subject is addressed in the relevant section of the GCPS.

5.3.2.2. Obligations of the Registry Office

48. The FNMT-RCM is the only authorised *Registry Office* to manage the lifecycle of the *Component Certificates*. Its obligations are:

- In general, to follow the procedures established by the FNMT-RCM in the applicable *Certification Policy and Practices* in performing its management, issuance, renewal and revocation of *Certificates* functions and not deviate from that policy framework.

- In particular, to verify the identity and any relevant personal circumstances of the *Applicants of Certificates* by any legal means and in accordance with that generally established in the GCPS and specifically in these *Specific Certification Policies and Practices.*

- To retain all information and documentation related to *Certificates* whose application, renewal, suspension or revocation is managed by the FNMT-RCM for a period of fifteen (15) years.

- Arrange the formalisation of the *Certificate* issuance contracts with the *Subscriber*.

- Verify with due diligence the revocation and suspension reasons which may affect the validity of the *Certificates*.

- The persons attached to the *Registry Office*, whether employees or public servants, are required to carry out public functions in accordance with the specific legislation applicable to the FNMT-RCM. The FNMT-RCM may use the registry function carried out by any of the corresponding posts, including telematic *Registry Offices,* to issue other *Certificates*, provided that the *Certificate Holders* have given their consent.

5.3.2.3. Obligations of the Component Controller (Holder and Subscriber)

- Refrain from using the *Certificate* outside the *Electronic Community* and beyond the limits specified in these *Specific Certification Policies and Practices*.
- Refrain from using the *Certificate* should the *Certification Services Provider* cease to carry out its activity as the issuing Entity responsible for issuing the *Certificate* in question, particularly in cases where the provider's *Signature Creation Data* may be compromised and this has been communicated.
- Provide truthful information in the *Certificate* application and keep the information up-to-date.
- Act with diligence with regard to the safekeeping and conservation of the *Signature Creation Data* or any other sensitive information such as *Keys*, *Certificate* activation codes, access words, personal identification numbers, etc. as well as the *Certificate* supports, which in every case entails non-disclosure of any of the aforementioned data.
- Know and comply with the *Certificates'* conditions of use set out in the *Certification Practices Statement*, particularly the *Certificates' use restrictions*.
- Know and comply with the amendments made to the *Certification Practices Statement.*
- Request the revocation of the respective *Certificate* in accordance with the procedure described in this document, promptly advising the FNMT-RCM of the circumstances or suspicions of loss of *Confidentiality*, disclosure, modification or unauthorised use of the *Signature Creation Data*.
- Check the information contained in the *Certificate* and advise the FNMT-RCM of any error or inaccuracy.
- Before trusting the *Certificates,* check the *recognised Electronic Signature* of the *Certification Services Provider* which issued the *Certificate.*
- Advise the FNMT-RCM promptly of any change in the data provided in the *Certificate* application, requesting the revocation of the Certificate whenever necessary.
- Return or destroy the *Certificate* when so required by the FNMT-RCM, and refrain from using it to sign or identify oneself electronically when the *Certificate* has expired or has been revoked.

5.3.2.4. Obligations of the User Entity

- Before trusting *Certificates*, check the recognised *Electronic Signature* of the *Certification Services Provider* which issued the *Certificate*.
- Check that the received *Holder's Certificate* continues to be in force.

- Check the state of the *Certificates* in the *Certification Chain* by consulting the *Certificates Revocation Lists* or (depending on whether it concerns a Public or Private Law Entity, respectively) through the *State of Certificates Information and Consultation Service* of the FNMT-RCM.

- Check the use restrictions of the *Certificate* being verified.

- Know the conditions of use of the *Certificate* in accordance with the applicable *Certification Policies and Practices Statement*.

- Advise the FNMT-RCM of any anomaly or information relating to the *Certificate* which may be considered to be a reason for revoking the *Certificate*, providing all the evidence at hand.

5.4. USE RESTRICTIONS AND ACCEPTANCE OF CERTIFICATES

49. To be able to use the *Certificates* effectively and, therefore, trust documents signed electronically based on them, one must previously be part of the *Electronic Community* and acquire the status of *User Entity,* so that the FNMT-RCM may provide the validity verification services for the different *Certificates*. Outside the *Electronic Community* one should not trust a *Certificate* or an *Electronic Signature* based on a *Certificate* issued by the FNMT-RCM.

50. The FNMT-RCM shall not be held responsible for the issuance of *Certificates* which have been fraudulently made to appear to have been issued by the FNMT-RCM. The FNMT-RCM shall take legal action against such fraudulent acts whenever it has direct knowledge of them or they are brought to its attention by the parties affected.

51. In any event, should a third party rely on that trust, no cover shall be given under this *Certification Practices Statement* and there shall be no entitlement to claim or take legal action against FNMT-RCM for damage, loss or disputes arising from the use of or trust in a *Certificate.*

52. Furthermore, even within the scope of the *Electronic Community*, this type of *Certificates* may not be used by anyone other than the FNMT-RCM to:

- Sign another *Certificate*.

- Generate *Time Stamps* for *Time Stamping* procedures – with the exception of the *Certificates* issued by the FNMT-RCM for *Time Stamping Units*.

- Offer services, against payment or free of charge, such as for example:

    - Provide *OCSP* services.

    - Provide electronic invoicing services.

    - Generate *Revocation Lists.*

    - Provide notification services

6. SPECIFIC CERTIFICATION PRACTICES FOR FNMT CLASS 2 CA COMPONENT CERTIFICATES

53. These *Specific Certification Practices* for *Component Certificates* describe the set of practices adopted by the FNMT-RCM as *Certification Services Provider* to manage the lifecycle of the *Certificates* issued under the *Component Certificates Certification Policy* of the FNMT-RCM, identified with the OID 1.3.6.1.4.1.5734.3.6.

54. *Component Certificates* are the *Certificates* issued by the FNMT-RCM under *the Component Certificates Certification Policy* of the FNMT-RCM identified with the OID 1.3.6.1.4.1.5734.3.6,to be installed in and used by computer *Components* or applications of which a specific natural or legal person acts as controller. That person is the *Controller* of the *Component* or application.

55. The *Signature Creation Data* associated to the *Signature Verification Data* shall be in the safe custody of the *Applicant* (natural person) of the *Component* for which the *Certificate* was issued.

56. These *Certificates* are issued and signed by the FNMT-RCM to be installed in and used by servers with SSL support, software components signature applications, *Time Stamping Units* or applications which act as clients of the advanced services provided by the FNMT-RCM, for the purpose of inheriting the trust in the FNMT-RCM as *Certification Services Provider*.

57. *Component Certificates* may only be obtained by entities which have signed a contract with the FNMT-RCM under which they are part of the *Electronic Community*, as described in the *Certification Practices Statement of the FNMT-RCM*.

58. **These *Certificates* do not produce the effects of acts carried out with a handwritten signature, unless they are unequivocally associated to a person and/or a *Recognised Certificate***, although they can operate with the same technical means and have the legal effects agreed by the members of the *Electronic Community* in their respective agreements/contracts, in accordance with that established in article 3.10 of the Law on the electronic signature and other applicable legislation.

59. It is hereby expressly stated that this type of *Certificates* are not issued with the quality of *Recognised Certificates,* with the exception of the aforementioned association provision.

60. An unequivocal association to a person and/or a *Recognised Certificate* is considered to exist when a specific type of *Certificate* issued by the FNMT-RCM includes the attribute of association to the *Component Certificate* in the field of the *Certificate*. An unequivocal association may also be considered to exist when the association is instrumented by means of a public instrument certifying the association. The FNMT-RCM reserves the right to include this type of attributes on the basis of the technical conditions and availability of the provider's infrastructure.

6.1. MANAGEMENT OF THE COMPONENT CERTIFICATES' LIFECYCLE

61. Defined here are the aspects which, although already mentioned in the GCPS of which this document is part, take on special characteristics which need to be explained in more detail.

6.1.1. Component Certificate Application Procedure

62. Described below is the application procedure by which the personal details of an *Applicant* of a *Component Certificate* are taken, his or her identity, the ownership of the domain, and where appropriate, the authority to make the application on behalf of the entity for which the *Component Certificate* is issued are confirmed, and the contract with the FNMT-RCM is signed for the subsequent issuance of the *Component Certificate,* once the pertinent validations have been made.

63. These activities are carried out directly by the Registry Area of the FNMT-RCM.

64. To apply for these products one should previously be part of the *Electronic Community*.

65. The computer functionality provided for the electronic National Identification Document shall be taken into account in accordance with the specific legislation.

6.1.1.1. Prior contact

66. The organisation and/or entity interested in applying for a *Component Certificate* should previously get in touch with the FNMT-RCM to obtain the necessary information on the issuance of the requested *Component Certificate* and the forms to be filled in.

67. The *Applicant* should prepare or compile the documents to be submitted and send them to the FNMT-RCM. Once received, the FNMT-RCM checks that the documents are in order. The documents are to include:

- The *Component Certificate* application form, duly completed and signed by the *Applicant*.
- Authorisation form from the *Component Controller* or his or her *Representative* for the Applicant to apply for the computer *Component Certificate*.
- Photocopy of the National Identification Document, Foreigners' National Identification Document or Passport of the *Applicant* of *the Component Certificate*, whose original must be valid and in force. The National Identification Document of the *Applicant* will not be required if the application form contains authorisation to the FNMT-RCM to check his or her personal data in the Identity Data Verification System.
- Document substantiating the ownership of the Domain Name or IP address, or internal document substantiating the Intranet.

- If applicable, formation deed and/or copy of agreement to set up the entity and, where appropriate, document substantiating the registration of the interested entity, whether private or public, in the respective registry.

- In the case of *Certificates* for *Time Stamping Units*, the *Time Stamping Practices Statement*, in accordance with Standard "ETSI 101 023 – Policy requirements for time-stamping authorities", of the entity which will provide the service as *Time Stamping Authority* and *Holder of the Certificate*.

  The *Certificate Holder* entity should be registered in the *Certification Services Providers* register of the Ministry of Industry, Tourism and Commerce as provider of *Time Stamping* services.

- File PKCS#10 of the *Component Certificate* request.

- In the case of a Code Signing *Component* for Advanced Services Clients and a generic computer *Component*, the PKCS#10 may be generated and inserted in the infrastructure of the FNMT-RCM following the same process as in the Pre-application for *Certificates* of natural persons. The Application Code generated during the Pre-application process should be attached to the documentation.

6.1.1.2. Processing the application and documentation by the FNMT-RCM

68. Once the application and pertinent documents have been received, the FNMT-RCM will process the application through its internal computer applications, will generate the contract to be presented to the *Applicant* for signing and will sign the specific component request for processing.

69. Depending on the type of *Component* specified in the request, the procedure will generate:

- In the case of a "Wildcard" or "SAN" type Web Server or *Time Stamping Units*: a PKCS#7 code shall be sent to the applicant by electronic mail.

- In the case of a Web Server, Code Signing or Computer Component *Certificate*, once the registration has been validated, a request confirmation message will appear. To download the *Component Certificate*, the application code provided by the *Applicant* should be used.

6.1.2. Subscription by the Component Controller

70. The *Component Controller* or his or her *Representative* should sign the two copies of the generated contract, keep one copy and send the other to the Registry Area of the FNMT-RCM for its filing system.

71. Should the *Component Controller* fail to send a copy of the signed contract to the Registry Area of the FNMT-RCM, the *Certificate* may be revoked or the issue process interrupted.

72. The FNMT-RCM shall file the copy of the contract signed by the *Component Controller* or his or her *Representative* with the rest of the documents relating to that computer *Component,* thus ending the *Component Certificate* application process.

6.1.3. Issuance of Component Certificate

73. The FNMT-RCM shall authenticate the *Certificates* using its *Electronic Signature*. On another front, in order to avoid manipulation of the information contained in the *Certificate*, the FNMT-RCM shall use cryptographic mechanisms to give authenticity and integrity to the *Certificates*.

74. The FNMT-RCM shall:

- Check that the *Applicant* of the *Certificate* uses the *Private Key* corresponding to the *Public Key*. To do this, the FNMT-RCM shall check the correspondence between the *Private Key* and the *Public Key*.
- Ensure that the information included in the *Certificate* is based on the information supplied by the *Applicant*.
- Not ignore known events which may affect the reliability of the *Certificate*.
- Ensure that the distinctive name on the *Certificate* is unique in the entire *Public Key Infrastructure* of the FNMT-RCM.

75. For the issuance of the *Certificate*, the following steps shall be followed:

1. Composition of the distinctive name of the *Component Certificate*.

   To compose the distinctive name of the *Certificate*, its typology shall be taken into account based on the classification set out below. For computer *Component Certificates* the FNMT-RCM shall not consider other distinctive names than those provided here.

   a) For SSL-support server *Certificates*

   Using the *Component* data gathered during the *Certificate Application* process, the distinctive name is composed in accordance with Standard X.500, ensuring that the name makes sense and does not give rise to ambiguities.

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

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

   The set of attributes OU, OU, OU, O, C represents the branch of the *Directory* where the entry corresponding to the *Component Certificate* in question is located.

   The attribute CN contains the name of the web server. The name may be **dns** or **ip** and should correspond with the service invocation method.

   E.g.:

   CN=**www.ceres.fnmt.es**

   CN=213.170.35.210

In the case of "wildcard" server *Certificates*, the CN of the *Certificate* shall be as follows:

CN=*.domainnamesecondlevel.TLD

Where,

[domainnamesecondlevel] the domain name whose owner is the applicant Entity

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

In the case of "SAN" server *Certificates*, the CN of the *Certificate* contains the name of the web server considered to be the main server.

Once the distinctive name which will identify the *Component* has been composed, the corresponding entry is created in the directory, making sure that the distinctive name is unique in the entire infrastructure of the certification authority.

b) For Code Signing Component, Advanced Services Clients, Time Stamping Units and Computer Component *Certificates.*

Using the *Component* data gathered during the *Certificate Application* process, the distinctive name is composed in accordance with Standard X.500, ensuring that the name makes sense and does not give rise to ambiguities.

The DN for a user is made up of the following elements:

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

The set of attributes OU, OU, OU, O, C represents the branch of the *Directory* where the entry corresponding to the user in question is located.

The attribute CN contains the identification data of the *Component* which will code sign and of the entity which owns the component. The syntax of that field depends on the type of user, which in the case of *Code Signing Components*, is:

CN=DESCRIPTION d – ENTITY e – CIF 12345678B

Where:

DESCRIPTION, ENTITY, CIF are labels, **[1]**

d is the description of the equipment or programme. It is advisable that this description makes sense. **[2]**

e is the entity which owns the equipment or programme.**[2]**

12345678B is the Fiscal Identification Number of the owner entity. **[3]**

[1] The labels always go in upper case and are separated from the value by a blank space. The pairs<label, value> are separated between them by a blank space, a dash and another blank space (" – ")

[2] With all the characters in upper case, except the letter eñe, which always goes in lower case. No symbols (commas, etc.) or characters with accents are included.

In cases relating to Time Stamping Units, it tends to take a "TSU n" type value, with n being an identifying number of the system.

[3] Fiscal Identification Number of the user = 8 digits + 1 upper case letter, with no separation between them. In the case of a user's National Identification Number with less than 8 digits, zeros are added at the beginning of the number to make up8 digits.

Once the distinctive name which will identify the *Component* is composed, the corresponding entry is created in the directory, making sure that the distinctive name is unique in the entire infrastructure of the certification authority.

2. Composition of the alternative identity

The alternative identity of the component under the *Certificate*, as described in this *Certification Policy*, contains information relating to the *Certificate Controller* entity and, optionally, the natural person who acts as custodian. The extension subjectAltName defined in X.509 version 3 is used to offer this information.

Within that extension, the subfield directoryName shall be used to include a set of attributes defined by the FNMT-RCM, which incorporate information on the entity which will be the *Certificate Subscriber*, in line with following criteria:

Table 2 – Extension SubjectAltName

Certificate Type	***Information***	***FNMT Attribute***	***OID (*)***
Computer Components **[1], [2]**	Description	fnmtDescripcion	fnmtoid.1.8
	Owner Entity	fnmtPropEntidad	fnmtoid.1.14
	Entity's Fiscal Id. No.	fnmtPropCif	fnmtoid.1.15
Optional	Controller's Name	fnmtRespNombre	fnmtoid.1.16
	Controller's 1st Surname	fnmtRespApellido1	fnmtoid.1.17
	Controller's 2nd Surname	fnmtRespApellido2	fnmtoid.1.18
	Controller's Fiscal Id. No.	fnmtRespNIF	fnmtoid.1.19

[1] On another front, apart from the *directoryName* subfield of the *subjectAltName* extension, if the entity provides a contact electronic mail address at the time of registration, the *rfc822Name*subfield will be included, which will contain that electronic mail address.

[2] The *subjectAltName* extension of the certificate may contain, apart from the *directoryName* subfield, the subfields *dNSName* and/or *iPAddress* to include, respectively, the domain name/s and/or IP address/es of the computer component.

(*) fnmtoid: 1.3.6.1.4.1.5734 : Number space assigned to the Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda by the IANA (Internet Assigned Number Authority).

3. Generation of the *Certificate* in accordance with the *Component Certificate* profile

   Here we must make a distinction between the format of the *Certificate* for SSL-support Web Servers, Code Signing components and Computer Components.

   The reason for this distinction is that there are two *Certificate* fields which will contain different values based on whether the component is one or another. This will be indicated in the specific field.

   The format of the issued certificate, in keeping with the Standard UIT-T X.509 version 3, contains the following fields:

Table 3 – Component Certificate Profile

Field	O.I.D.	Value
Basic Fields		
Version		2 (X.509 v3)
SerialNumber		Serial number of the *Certificate*. **[1]**
Issuer		C=ES,O=FNMT,OU=FNMT Class 2 CA
Validity		**[2]**
Subject		**Distinctive name of the Subscriber.[3]**
SubjectPublicKeyInfo		RsaEncryption, *Public Key*.**[4]**
SignatureAlgIdentifier	1.2.840.113549.1.1.5	Identifier of the Signature Algorithm used. **[5]**
Standard Extensions		
KeyUsage	2.5.29.15	**[6]**
extKeyUsage	2.5.29.37	**[7]**
PolicyIdentifier	2.5.29.32	1.3.6.1.4.1.5734.3.6
PrivateKeyUsageperiod	2.5.29.16	The same validity.
SubjectAltName	2.5.29.17	**[8]**

CRLDistributionPoints	2.5.29.31	Cn=CRLnnn, c=ES, o=FNMT, OU=FNMT Class 2 CA. **[9]**
AuthorityKeyIdentifier	2.5.29.35	*Key*identifier of the *PSC*
SubjectKeyIdentifier	2.5.29.14	*Key*identifier of the *Subscriber*
BasicConstraints	2.5.29.19	Basic constraints. End Entity.
Private Extensions		
NetscapeCertType	2.16.840.1.113730.1	**[10]**

Where:

[1] SerialNumber: Identifier number for the *Certificate*, unique within the infrastructure of the *Certification Services Provider*.

[2] Validity: Validity period of the *Certificate*, as described in the "Expiration" section of this document.

[3] Subject: Identifier of the *Subscriber* of the *Certificate*. Its composition is described above in this appendix.

[4] SubjectPublicKeyInfo: The *Public Key* that the *Subscriber* generated in the issuance of the Certificate pre-application stage. A possession of the corresponding *Private Key* test is carried out.

[5] SubjectAlgIdentifier: Identifier of the algorithm used to make the *Electronic Signature* of the *Certificate.* The algorithm used is SHA1WithRSAEncryption (*OID* 1.2.840.113549.1.1.5) and the length of the *Key* used is 1024 bits.

[6] KeyUsage: Accepted values for using the key. **It is not marked as critical, save in cases of Code Signing Certificates.** It takes the following values:

> **For SSL-support Web Servers: {digitalSignature, keyEncipherment}.**
>
> **For Code Signing Components and *Time Stamping Units*: {digitalSignature}.**
>
> **For Advanced Services Clients and Generic Computer Components: {digitalSignature, keyEncipherment}.**

[7] extKeyUsage: Extension that adds more information on using the key.

> **For Web Servers: {serverAuth (1.3.6.1.5.5.7.3.1)} – TLS Web server authentication.**
>
> **For Web Servers with email protection: {serverAuth (1.3.6.1.5.5.7.3.1), emailProtection (1.3.6.1.5.5.7.3.4)}.**

For Code Signing Components: {Code Signing (1.3.6.1.5.5.7.3.3)}.

For *Time Stamping Units*: {timeStamping (1.3.6.1.5.5.7.3.8)}.

[8] SubjectAltName: Alternative Identity of the Subject. **It is not marked as critical.**

Its correct composition has been described above in this appendix.

[9] CRLDistributionPoint: The specific distribution point of the *Revocation Lists* is generated by the *Certification Services Provider* at the time of generating the *Certificate*. **It is not marked as critical.**

[10] NetscapeCertType: Type of certificate according to Netscape. **It is not marked as critical.**

It takes the following values:

For SSL-support Web Servers: {sSLSERVER}.

For Code Signing Components: {objectSigning}.

For Advanced Services Clients and Generic Computer Components: {sSLCLIENT,sMIME}.

For *Time Stamping Units*: It is not included.

6.1.4. Publication and distribution of the Component Certificate

76. Once the *Certificate* has been issued by the *Certification Authority*, the *Certificate* is published in the secure directory, in the entry corresponding to the distinctive name assigned to the component, as described in the "Issuance of *Component Certificate*" section.

77. The FNMT-RCM will send the issued *Component Certificate* to the *Component Controller* via the indicated electronic mail address in the corresponding format. It may also make it available to the *Component Controller* via a secure application in the web page created for that purpose.

6.1.5. Validity period of Certificates

6.1.5.1. Expiration

78. The validity period of the *Certificates* issued by the FNMT-RCM under the *Certification Policy* that concerns us here shall be 24 months from the date the *Certificate* is issued, provided that the validity is not extinguished due to the reasons and through the procedures set out in the "Extinction of the validity of the *Certificate*" section below.

6.1.5.2. Extinction of the validity of the Certificate

79. The *Component Certificates* issued by the FNMT-RCM shall be rendered null and void in the following instances:

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

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

In both of (a) and (b) cases above, the *Certificates* shall lose their effectiveness the moment these circumstances are produced.

c) Revocation of the *Certificate* for any of the reasons set out in this document.

d) In *Certificates* unequivocally associated to a *Certificate* and/or person, the revocation and/or suspension of the *Certificate* to which the component *Certificate* will be associated, will entail the revocation/suspension of the latter.

80. For the purposes mentioned above, it is hereby stated that an application for the issuance of a *Component Certificate* when there already is another one in force in favour of the same *Holder* covered by the same *Issuance Law* will entail the revocation of the first certificate obtained.

81. The effects of the revocation or suspension of the *Certificate*, i.e., the extinction of its validity, shall take effect as of the date the FNMT-RCM has reliable knowledge of any of the determining factors and includes the revocation or suspension in the *Revocation List* of its *State of Certificates Consultation Service.*

6.1.6. Revocation

82. The application for the revocation of *Component Certificates* may be made during the validity period that appears in the *Certificate*. It involves the cancellation of the identity guarantee or other properties of the user and its correspondence with the associated *Public Key*.

83. The revocation of a *Component Certificate* may be applied for by:

- The *Holder* who owns the *Component* or a third party who represents the *Holder* with sufficient authority.
- The *Controller* of the *Component Certificate*.

6.1.6.1. Reasons for revocation

84. The FNMT-RCM shall only be held liable for consequences arising from failing to revoke a *Certificate* in the following instances:

- When the revocation should have been carried out due to extinction of the contract signed by the *Subscriber*.
- When the revocation was requested by the *Holder* or *Controller* in accordance with the procedure established for the purpose.
- When the application for the revocation or the reason for the revocation was notified via a court or administrative decision.

- When with reasons c) to e) of this section, the circumstances were duly substantiated and the *Applicant* of the revocation was duly identified.

85. Bearing in mind the above, a *Component Certificate* shall be revoked for the following reasons:

a) The *Holder*, *Component Controller* or duly authorised third party should always submit a revocation application in the following situations:

- Loss of the Certificate support.
- Use by a third party of the *Holder's Signature Creation Data* corresponding to the *Signature Verification Data* contained in the *Certificate* and associated to the *Holder's* identity.
- Violation or endangerment of the confidentiality of the *Signature Creation Data* of the *Holder* or those responsible for the safekeeping of the *Signature Creation Data.*
- Non-acceptance of new conditions introduced with the issue of future *Certification Practices Statements* within a period of one month after their publication.

b) Court or administrative decision requiring the revocation.

c) Death, extinction or dissolution of the legal status of the *Holder*.

d) Total or partial unforeseen incapacity of the *Subscriber* or his or her principal.

e) Inaccuracies in the data supplied by the *Applicant* to obtain the *Certificate*, alteration of the data supplied to obtain the *Certificate,* or change in the circumstances confirmed prior to issuing the *Certificate*, such as those relating to the job title or the representation powers, making those circumstances no longer true.

f) Breach of a substantial obligation in this *Certification Practices Statement* by the *Certificate Holder*, the *Certificate Controller* or by the *Registry Office* if, in the latter case, the breach may have affected the *Certificate* issuance procedure.

g) Termination of the contract signed by the *Certificate Subscriber* or his or her representative and the FNMT-RCM.

h) Violation or endangerment of the confidentiality of the *Signature Creation Data* of the FNMT-RCM with which it signs the *Certificates* that it issues.

86. Under no circumstances shall it be understood that the FNMT-RCM assumes any obligation to verify the circumstances mentioned in letters c) to e) of this section.

87. **The FNMT-RCM shall be exempt from liability for actions constituting a crime or an offense which are not known to the FNMT-RCM and involve the data and/or *Certificate,* inaccuracies in the data or lack of diligence in communicating the data to the FNMT-RCM.**

88. **Any data that fails to represent the true state of affairs, when that data is found in public registries, shall not be attributable to the FNMT-RCM whilst the FNMT-RCM does not have telematic instruments for direct communication with the different public registries, unless the data is communicated to the FNMT-RCM by reliable means.**

6.1.6.2. Effects of revocation

89. The revocation of the *Certificate*, i.e. the extinction of its validity, shall take effect as of the date the FNMT-RCM has reliable knowledge of the determining factors and includes the revocation in the *Revocation List* and in its *State of Certificates Consultation Service*.

6.1.6.3. Certificate revocation procedure

90. Described below is the procedure through which the personal data of the *Applicant* is obtained, his or her identity and the responsibility regarding the *Component Certificate* confirmed, and the *Component Certificate* revocation application by the legitimate interested party made.

91. These activities are only carried out by the Registry Area of the FNMT-RCM, and under no circumstances by *Registry Offices*.

1. Application of the *Holder* who owns the *Component*.

   The owner of the *Component* or his or her *Representative* shall send the duly completed and signed revocation application form to the FNMT-RCM by ordinary mail.

   The computer functionality provided for the electronic National Identification Document shall be taken into account, in accordance with the specific legislation.

2. Processing the application by the FNMT-RCM

   The registrar of the FNMT-RCM shall process the *Component Certificate* revocation, indicating in the certificate: the priority option that he or she considers appropriate for the revocation; the *Component* name, the Domain or IP, if any, the CN, the identity of the owner of the *Component* and his or her Fiscal Identification Number, the identity of the *Component Controller* and his or her Fiscal Identification Number, the corresponding application code, and the OU.

   As soon as the revocation has been determined, the registrar of the FNMT-RCM will notify the revocation to the *Component Controller* in accordance with the terms set out in the Availability of the Information and Communications section of the **GCPS**.

   Once the FNMT-RCM has revoked the *Certificate*, the corresponding *Revoked Certificates List* will be published in the secure directory, specifying the serial number of the revoked *Certificate*, the date and time of the revocation and the reason for the revocation.

6.1.7. Suspension of Component Certificate

92. The suspension (temporary revocation) of *Certificates* entails the cancellation of the identity guarantee and other properties of the user and its correspondence with the associated public key for a period of time and under certain conditions.

93. The suspension of a *Component Certificate* may be applied for by the same persons authorised to apply for the revocation.

94. The suspension of the *Component Certificate* means its temporary revocation. The suspension procedure is similar to the revocation procedure.

95. The FNMT-RCM shall suspend the *Certificate* on a provisional basis for a period of ninety (90) days, after which time the *Certificate* shall be extinguished through the revocation procedure (without requiring the express request of the interested party), unless the suspension has been lifted by the *Holder*. Notwithstanding the aforementioned, the period established for the suspension of the *Certificate* may change as a result of possible judicial or administrative proceedings affecting it.

96. Should the *Certificate* expire during the suspension period, the expiration shall have the same implications as for expired non-suspended *Certificates*.

6.1.8. Cancellation of suspension of *Component Certificate*

97. The cancellation of the suspension of the *Certificates* issued by the FNMT-RCM may be requested by the *Holders* and the *Controllers* provided that, prior to the suspension cancellation request, they hold the *Certificate* and the *Private Key* and the request is made within ninety (90) days of the suspension.

98. To do this, they must request the cancellation to the Registry Area of the FNMT-RCM, when the *Applicant* should supply the data requested and substantiate his or her personal identity as in the issuance process described above.

6.1.9. Verification of state of *Certificate*

99. The *Certificate Holder* or other user Entities belonging to the *Electronic Community* may check the state of a *Certificate* through the method and under the terms described in the "On the state of validity of certificates information and consultation service" section of the GCPS, except with this type of *Certificates* the verification of the state of *Certificates* can be made through the *Certificates* verification web service.

100. For the dissemination and trust in systems equipped with these *Certificates*, the FNMT-RCM can offer the possibility to verify, by the member of the *Electronic Community* or a third party, that the *Component Certificate* is a valid *Certificate* issued by the FMT-RCM, as well as other characteristics of the *Certificate*.

6.2. STANDARD FORMS

101. The standard forms to be filled in to carry out the described operations for managing the lifecycle of the *Component Certificates* shall be published in http://www.ceres.fnmt.es