



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

**SPECIFIC CERTIFICATION POLICY AND PRACTICES APPLICABLE TO  
COMPONENT CERTIFICATES**

**“AC COMPONENTES INFORMÁTICOS”**

	<b>NOMBRE</b>	<b>FECHA</b>
Prepared by:	FNMT-RCM / v1.6	17/06/2017
Revised by:	FNMT-RCM / v1.6	02/10/2017
Approved by:	FNMT-RCM / v1.6	09/10/2017

<b>BACKGROUND OF THE DOCUMENT – TRACK CHANGES</b>			
<b>Version</b>	<b>Date</b>	<b>Description</b>	<b>Author</b>
(1.0)	21/11/2013	First version	FNMT-RCM
(1.1)	07/03/2014	Elimination of suspension	FNMT-RCM
(1.2)	22/10/2014	Review under WebTrust	FNMT-RCM
(1.3)	23/03/2015	Inclusion of certificate OID for use of Time Stamping Units	FNMT-RCM
(1.4)	24/06/2016	Profile update: inclusion of Locality field... and elimination of components for natural persons.	FNMT-RCM
(1.5)	03/01/2017	Adaptation to eIDAS Regulation.	FNMT-RCM
(1.6)	09/10/2017	Inclusion of CAB/Forum requirements	FNMT-RCM

**Reference:** DPC/PC-DPC-ACCOMP-0106/SGPSC/2017

**Document classified as:** *Public*



## Table of contents

<b>List of Tables .....</b>	<b>4</b>
<b>1. Preamble .....</b>	<b>5</b>
<b>2. Document organization .....</b>	<b>6</b>
<b>3. Definitions .....</b>	<b>7</b>
<b>4. Order of prevalence.....</b>	<b>8</b>
<b>5. Component Certification Policy .....</b>	<b>8</b>
5.1. Identification.....	8
5.2. Pseudonyms .....	10
5.3. Acknowledgment and authentication of registered marks .....	10
5.4. Community and scope of application .....	10
5.4.1. Participants .....	10
5.5. liability and duties of the parties .....	11
5.5.1. Liability of the parties .....	11
5.5.1.1. Trusted Services Provider’s Responsibility .....	11
5.5.1.2. Applicant’s responsibility .....	12
5.5.1.3. Subscriber’s responsibility .....	13
5.5.1.4. Responsibility of User Entity and relying parties .....	13
5.5.2. Duties and guarantees of the parties .....	14
5.5.2.1. Trust Services Provider’s duties and guarantees. ....	14
5.5.2.2. Duties of the Registry Office.....	16
5.5.2.3. Duties of Applicant and Subscriber.....	16
5.5.2.4. Duties of the User Entity and of relying parties .....	17
5.6. Limits of use and acceptance of certificates .....	18
<b>6. Specific certification practices for “AC Componentes Informáticos” component certificates.....</b>	<b>18</b>
6.1. Component certificate lifecycle management .....	18
6.1.1. Application procedure.....	19
6.1.2. Subscription and sending of contract by Subscriber .....	19
6.1.3. Validation of domain authorization or control.....	20
6.1.4. Issue .....	20
6.1.5. Publication and distribution .....	21
6.1.6. Notification to applicant .....	21
6.1.7. Validity .....	21
6.1.7.1. Expiry.....	21
6.1.7.2. Termination of Certificate validity .....	21
6.1.8. Renewal .....	22
6.1.9. Revocation .....	22

6.1.9.1.	Causes of revocation.....	22
6.1.9.2.	Procedure for Certificate revocation.....	24
6.1.9.3.	Effects and time of revocation .....	25
6.1.10.	Suspension .....	25
6.1.11.	Notification of the change of status of the certificate .....	25
6.1.12.	Verification of Certificate status .....	25
6.2.	<i>Certificate for use in the Time Stamping Unit of the FNMT-RCM</i> .....	26
<b>7.</b>	<b>Fees</b> .....	<b>26</b>
<b>8.</b>	<b>Audits</b> .....	<b>27</b>
<b>9.</b>	<b>Certificate profiles</b> .....	<b>27</b>
9.1.	<i>Name restrictions</i> .....	27
9.2.	<i>Use of the policy constraints extension</i> .....	27
9.3.	<i>Syntax and semantic of Policy Qualifiers</i> .....	27
9.4.	<i>Semantic treatment of the “Certificate Policy”</i> .....	27
<b>Anexo I: Identification of the Certification Authority Certificate</b> .....		<b>28</b>

**LIST OF TABLES**

<b>Table 1 – Certification Policy Identification</b> .....	<b>8</b>
--	----------



## **1. PREAMBLE**

1. These *Specific Certification Policies and Practices* describe the issue of *Component Certificates* by FNMT-RCM. These *Certificates* links *Signature Verification Data* to a *Subscriber* that controls the running of the *Component* that uses the *Certificate*.
2. *Component Certificates* are those certificates issued by FNMT-RCM under this *Certification Policy* and that link *Signature Verification Data* to a software *Component* or application over which a *Subscriber* acts as responsible party and has control. The *Private Key* associated with the *Public Key* will be under the *Applicant’s* responsibility until the *Component Certificate* is installed and, after installation, under the *Subscriber’s* responsibility.
3. For the purposes of article 6 of Law 59/2003, of 19 December, on electronic signature, *Component Certificates* will be considered electronic *Certificates* where there is no doubt about the link between the *Component Certificate* and the natural or legal person or administration *Subscriber* of the *Certificate*. FNMT-RCM will issue these *Certificates* where it is so requested by an authorized *Applicant* and their use is not banned or limited by the applicable legislation.
4. FNMT-RCM will not be liable for the actions carried out with this type of *Certificates* where there is improper use of authorities or insufficiency thereof and/or where there are decisions by the *Certificate Subscriber* that affect the validity of its *Representative’s* authorities; therefore, any modification, revocation or constraint shall not be opposable to FNMT-RCM unless reliably notified.
5. *Component Certificates* are issued and signed by FNMT-RCM to be installed and used by software *Components* so that the trust represented by FNMT-RCM as *Trusted Services Provider* passes on. *Component Certificates* can be obtained only by *Subscribers* that have subscribed a contract or agreement with FNMT-RCM, whereby they are part of the *Electronic Community* as contemplated in the FNMT-RCM *Certification Practices Statement*.
6. FNMT-RCM will issue these *Certificates* only for activities compatible with the scope and use of the *Certificate* in question, to which the *Component* is undoubtedly linked.
7. As *Trusted Services Provider*, FNMT-RCM reserves the right of not issuing or of revoking this type of *Certificates*, if the *Subscriber* that uses this type of *Certificate* does not use it in an appropriate manner, violating third-party industrial or intellectual property rights in respect of the applications, websites or equipment to be protected with such *Certificates*, or if their use is misleading or leads to confusion about the title ownership of such *Components*. In particular, the right that FNMT-RCM reserves may be exercised where the use of such certificates attempts against the following principles:
  - Safeguarding of the public order, criminal investigation, public safety and national defence.



- Public health protection or that of natural or legal persons that enjoy the condition of consumer or user, even when acting as investors.
  - Respect for human dignity and the non-discrimination principle for reasons of race, gender, faith, opinion, nationality, disability or any other personal or social situation.  
And
  - Protection of youth and children.
8. FNMT-RCM shall be released and held harmless in respect of any complaint or claim for the wrong use of *Component Certificates* where what is contained in the *Certification Practices Statement* is not complied with.

## 2. DOCUMENT ORGANIZATION

9. The FNMT-RCM *Certification Practices Statement* is comprised of several documents:
- The “*FNMT-RCM Trust Services Practices and Electronic Certification Statement*” [abbreviated in Spanish: TSPS]. The purpose of this Statement is to provide public information about the general conditions and characteristics of the certification services provided by FNMT-RCM as a *Trusted Services Provider*.
  - Any annexes as are considered relevant for public information about conditions of use, limitations, liability, property and any other information considered specific to each type of *Certificate*. These annexes will be considered the *Specific Certification Policy and Practices* for the type of *Certificate* in question, as is reflected in this document in relation to *Component Certificates*.
10. Therefore, the set of documents comprised of the TSPS and any annexes describing, developing or specifying the questions related to a type of specific *Certificate*, i.e., the specific *Certification Policy and Practices* for said type of *Certificate*, is considered the *Certification Practices Statement* for a specific type of *Certificate* issued by FNMT-RCM.
11. The section “Definitions” in the TSPS and in this document must be taken into account for the purpose of interpreting this annex.
12. This document deals with public information about the set of practices, conditions and characteristics of the certification services provided by FNMT-RCM as a *Trusted Services Provider*, in relation to the lifecycle of electronic *Component Certificates*.
13. So, this annex stems from and is an integral part of the FNMT-RCM *Certification Practices Statement* as regards *Component Certificates*. It contains the Certification Policy for this type of *Certificates* and the *Certification Practices* used in their lifecycle.
14. In short, these *Certification Policies and Specific Certification Practices* sum up what is articulated in the TSPS main body and, therefore, are an integral part thereof, both documents making up the FNMT-RCM *Certification Practices Statement* for *Component Certificates*. So, what is described in this document is only applicable to the set of *Certificates* characterized and identified in this *Specific Certification Policy and Practices*,





- and they can present special features reflected through the Certificate Issuance Law or corresponding group of *Certificates*, if there are specific characteristics or functionalities.
15. The FNMT-RCM manages its certification services and issues certificates in accordance with the "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates" established by the CA / Browser forum and which can be consulted at the following web site: [//cabforum.org/baseline-requirements-documents/](http://cabforum.org/baseline-requirements-documents/)
  16. The FNMT-RCM will review its certification policies and practices. It will annually update the corresponding Certificate Policy Statement to keep it in line with the latest version of those requirements, increasing the version number and adding a change log entry with date, even if no other changes were made to the document.

### 3. DEFINITIONS

17. For the interpretation of this document, the following definitions are added to those contained in the TSPS:
  - *CAA Record*: The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misissue.
  - *Certificate for website authentication*: *Component Certificate* that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.
  - *Component*: Set of software elements interrelated for data transmission or processing and capable of signing or encoding data autonomously.
  - *Component Certificate*: *Certificate* used by a software *Component* on a public key infrastructure.
  - *Representative*: *Subscriber's* Administrator, person in public office or general representative, where *Subscriber* is a legal person, public body or agency, and that acts for and in the name of *Subscriber*. It is also the natural person who is recognized the capacity to authorize the *Applicant*.
  - *Applicant*: Natural person, of legal age, that applies for issue of a *Certificate* and delivers the public key to FNMT-RCM and receives the *Certificate* from FNMT-RCM.
  - *Certificate Subject*: The “Subject” field on the *Certificate*. It identifies the *Subscriber* and the *Component*.
  - *Subscriber*: Legal person, public body or agency recipient of the activities of FNMT-RCM as *Trusted Services Provider* and that subscribes the service terms and conditions and is identified in the *Subject* field on the *Certificate*. It is the *Certificate* holder and the party responsible for its use and it has the sole control and decision-making capacity over the *Component*.



*(The words or expressions in italics are defined in this document or in the Trust Services Practices and Electronic Certification Statement)*

#### **4. ORDER OF PREVALENCE**

18. The order of prevalence is the following:

- These *Certification Policies* and *Specific Certification Practices* for *Component Certificates* are part of the *Certification Practices Statement* and shall prevail, in what is relevant and specific to this type of *Certificate*, over the provisions in the *TSPS*.

Therefore, should there be any contradiction between this document and the provisions of the *TSPS*, what is contained herein shall prevail.

- The *Issuance Law* for each *Certificate* or group of *Certificates* will be, if appropriate and because of its singularity, a special regulation over the provisions contained in these *Certification Policies* and *Specific Certification Practices*. The *Issuance Law*, if any, shall be included in the relationship document to be entered into between FNMT-RCM and the *User Entity*, and/or in the conditions of use or issue agreement and/or in the *Certificate* itself.

#### **5. COMPONENT CERTIFICATION POLICY**

##### **5.1. IDENTIFICATION**

19. This FNMT-RCM *Certification Policy* for issue of *Component Certificates* is broken down in the following policies:

**Table 1 – Certification Policy Identification**

General name	FNMT-RCM Component Certificate Certification Policy (AC Componentes Informáticos)
Reference/OID and specific name	<p>1.3.6.1.4.1.5734.3.9.19 – <i>Component Certificates</i> for entity seal</p> <p>1.3.6.1.4.1.5734.3.9.4 – <i>Component Certificates</i> for code signature</p> <p>1.3.6.1.4.1.5734.3.9.16 – <i>Standard Certificate for website authentication</i></p> <p>1.3.6.1.4.1.5734.3.9.17 – <i>Wildcard Certificate for website authentication</i></p> <p>1.3.6.1.4.1.5734.3.9.18 – <i>Multi-domain Certificate for website authentication</i></p> <p>1.3.6.1.4.1.5734.3.9.14 – <i>Component Certificates</i> for use in <i>Time Stamping Units</i></p> <p>1.3.6.1.4.1.5734.3.9.20 – <i>Component Certificate</i> for the <i>Time Stamping Unit</i></p>

	<i>of the FNMT – RCM Qualified Time Stamping Service</i>
Version	1.6
Related DPC	<i>FNMT-RCM Trust Services Practices and Electronic Certification Statement</i>
Location	<a href="http://www.ceres.fnmt.es/dpcs">http://www.ceres.fnmt.es/dpcs</a>

20. The table above identifies a policy OID for each *Certificate* profile, although all the policies are jointly described in this document. The reason for this is twofold: on the one hand, the structure of the fields to be interpreted on each type of *Certificate* can be automatically differentiated and, on the other hand, the rules for application of *Certificates* to the same community are unified and with the same security requirements. Each policy is related to a type of *Certificate*.
21. This DPC considers the following types of *Certificates*:
- *Standard Certificate for website authentication*: It allows the establishment of safe communications using the SSL/TSL protocol. This type of *Certificate* guarantees the identity of the web site domain.
  - *Wildcard Certificate for website authentication*: It guarantees security for an unlimited set of domains, starting from the third level, with a single *Certificate for website authentication*.
  - *Multi-domain Certificate for website authentication (SAN/ECC)*: It guarantees security for a set of domains which are independent from one another.
  - *Code Signature Component Certificate*: It makes it possible to sign software and guarantee the proprietor’s identity and the integrity of the code.
  - *Entity Seal Component Certificate*: It is used for signature process automation and software component authentication. In addition, it enables the user to choose the extended use of the *Certificate* keys (client authentication, e-mail protection).
  - *Component Certificate for use in Time Stamping Units*: It is used by third-party *Time Stamping Authorities*.
  - *Component Certificate for use in the Time Stamping Unit of the FNMT-RCM*: It is used by the *Time Stamping Authority* of the FNMT-RCM in order to provide the *Qualified Time Stamping Service* of this Entity, *Qualified Trust Service Provider*. In all matters relating to this service, it can be consulted the *Time Stamping Practices Statement* at the site <http://www.cert.fnmt.es/dpcs/>
22. The Entity Seal *Certificate* and the *Certificate* for use in the *Time Stamping Unit* of the FNMT-RCM, are *Qualified Certificates* in accordance with the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic

identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

## **5.2. PSEUDONYMS**

23. As regards identification of *Subscribers* using the *Certificates* issued under this *Certification Policy*, FNMT – RCM does not accept the use of pseudonyms.

## **5.3. ACKNOWLEDGMENT AND AUTHENTICATION OF REGISTERED MARKS**

24. FNMT – RCM assumes no commitment as regards the use of trademarks in the issue of the *Certificates* issued under this *Certification Policy*. The use of distinctive signs is not allowed where the *Holder* does not have the right to use them or it is not duly authorized, so FNMT – RCM is not under an obligation to verify first the ownership or registration of registered marks or any other distinctive signs before the issue of the certificates even though they appear registered on public registers.

## **5.4. COMMUNITY AND SCOPE OF APPLICATION**

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

- *Certificates* issued by FNMT-RCM that link *Signature Verification Data* to a *Component* and to a *Subscriber* that controls the *Component*.
- *Certificates* issued under this *Certification Policy* are issued for *User Entities* that are part of the *Electronic Community* as defined in the section “Definitions” in the TSPS of FNMTRCM.
- *Certificates* issued under this *Certification Policy* are considered adequate as an integral part of electronic signature systems that require specific security standards and, in particular, to establish secure communication between an electronic address and the user connecting to it, apart from their being a tool to check the authenticity of and identify the electronic address for which they have been issued.

### **5.4.1. Participants**

26. For the purposes of these *Specific Certification Policies and Practices*, the *Certification Authority* is FNMT – RCM, as *Trusted Services Provider*.

27. The *Registration Authority*, for the purposes of registration of operations, will be FNMT – RCM, which will act as the only authorized Registry Office, through its Registry Area.

28. The certificate *Subscriber* entities, which are the legal persons, public organizations or agencies that have under their control and operation the domain identified by the *Certificate for website authentication* o, in the case of *Entity Seal Component Certificate*, are their



creators. Therefore, these entities are the holders of and responsible for the use of the *Certificate*, with exclusive control and decision-making capacity over the *Component*.

29. Third parties that trust the *Certificates* issued under this *Certification Policy*: those that voluntarily trust said *Certificates* following the trust placed on FNMT – RCM as *Trusted Services Provider*.

#### 5.5. LIABILITY AND DUTIES OF THE PARTIES

30. This *Certification Policy* contains the responsibilities and obligations of the parties involved in the issue and use of *Component Certificates* issued under this *Policy*.

31. FNMT-RCM shall not be liable for the use of *Component Certificates* where the *Certificate Subscriber* and, as the case may be, its *Representative*, carries out activities without the authority to do so or exceeding its authority, or in contravention of the law or in fraud against third parties, if there is no reliable notice that allows to transfer the intended effects to the management of *Certificates*.

##### 5.5.1. Liability of the parties

32. Before being able to use *Component Certificates* issued by FNMT-RCM, one must be part of the *Electronic Community* and have the condition of *User Entity*. To trust a *Component Certificate*, it will be essential to verify the status of validity of the *Certificate* in question through the FNMT-RCM *Information and consultation service on the state of validity of the certificates*.

33. If a *Component Certificate* is trusted by a member of the *Electronic Community*, *User Entity* or a third party, and the status of the *Certificate* in question has not been verified, no cover shall be obtained from the *Certification Practices Statement* and said member, *User Entity* or third party shall not be entitled to claim or take legal action against FNMT-RCM. Therefore, given that situation, FNMT-RCM shall not be liable for any damages or conflict stemming from the use of or trust in a *Component Certificate*.

##### 5.5.1.1. Trusted Services Provider’s Responsibility

34. FNMT-RCM is responsible solely for the correct personal identification of the *Applicant*, *Subscriber* and, as the case may be, *Representative*. As regards this information, FNMT-RCM just expresses it on a *Certificate* for which evidence has been given as to the *Subscriber’s* identity.

35. FNMT-RCM is responsible for verifying, on the appropriate databases, that the *Subscriber* is the holder of the domain names specified on the *Certificate* application.

36. FNMT-RCM shall only be liable for deficiencies in the procedures pertaining to its activity as *Trusted Services Provider*, and in conformity with what is contained in these *Certification Policies* or in the legislation. Under no circumstance shall FNMT-RCM be liable for action or loss incurred by *Applicants*, *Subscribers*, *Representatives*, *User Entities* or, as the case may be, by any third party involved, as are not due to serious error,



- attributable to FNMT-RCM, in the above-mentioned procedures for *Certificate* issue and/or management.
37. FNMT-RCM shall not be liable for act of nature, force majeure, terrorist attempt, wildcat strike situations or for situations involving actions that amount to offences or misdemeanours that affect its service providing infrastructures, unless the entity has incurred serious negligence. In any event, FNMT-RCM may establish, in the relevant contracts and/or agreements, additional liability limitation stipulations to those contained in this document.
  38. FNMT-RCM shall not be liable to individuals who have been negligent in the use of *Certificates*, and for these purposes and in any event failure to comply with the provisions in the *Certification Practices Statement*, and particularly what is contained in the sections about obligations and liability of the parties, is considered negligence.
  39. FNMT-RCM shall bear no responsibility for any software that FNMT-RCM has not provided directly.
  40. FNMT-RCM does not guarantee the cryptographic algorithms; nor shall FNMT-RCM be liable for any damage caused by external successful attacks to the cryptographic algorithms used, if FNMT-RCM kept due diligence in accordance with the current state of technology and if it acted in conformity with this *Certification Practices Statement* and with the law.
  41. For the specific case of *Component Certificates* for their use in *Time Stamping Units* belonging to third-party Time Stamping Authorities, it is hereby stated for the record that FNMT-RCM shall bear no responsibility nor shall it guarantee any aspect of the Time Stamping Service offered by entities holding such Time Stamping Units and Authorities. In particular, the absence of responsibility shall extend to the management of any aspect related to the information systems used by said Units or Authorities and to the validity of the time sources, or their synchronism, used in the service.
  42. In any event and with the nature of a penal clause, the maximum amount that FNMT-RCM should pay, as damages, by court order, to a wronged third party or member of the *Electronic Community*, in the absence of specific regulation on contracts or agreements, is limited to no more than EUR SIX THOUSAND (€6,000).

#### 5.5.1.2. *Applicant's responsibility*

43. The *Applicant* shall be responsible for the truth and accuracy of the information submitted during the *Certificate* application process, in the sense that the *Applicant* has been authorized or empowered by the Subscriber to put in the application and that the *Applicant* will install the *Certificate* appropriately in the *Component* designated by the *Subscriber*.
44. The *Applicant* shall hold harmless and defend FNMT-RCM against and shall bear the cost of any action as might be undertaken against this *Entity* and in respect of any damages sustained by FNMT-RCM as a result of the wrong installation of the *Certificate*, of false or seriously wrong information supplied in the *Certificate* issue procedure, or arising from the *Applicant's* culpable or negligent act or omission.

5.5.1.3. *Subscriber’s responsibility*

45. In any event the *Subscriber* shall be responsible for using the *Certificate* adequately and safeguarding it diligently, according to the purpose and the function for which the *Certificate* has been issued, and for reporting to FNMT-RCM on any change of status or information concerning the *Certificate* content, for revocation and new issue thereof.
46. Additionally, the Subscriber shall be liable, in any event, to FNMT-RCM, the user *Entities* and, if applicable, to third parties, for the *Applicant’s* action, for the wrong use of the *Certificate*, or for the misrepresentations or errors in the statements gathered therein in the application process, or for acts or omissions that cause damages to FNMT-RCM or third parties.
47. The *Subscriber* shall be responsible for and, therefore, will have the obligation of not using the *Certificate* if the Trust Services Provider has ceased its activity as the *Certificate* issuing *Entity* that issued the *Certificate* in question and no other *Entity* has assumed the activity in the manner established by law. In any event, the Subscriber shall not use the *Certificate* in situations where the Provider’s *Signature Creation Data* may be threatened and/or at risk and it has been so reported by the Provider or, as the case may be, the Subscriber has heard about this circumstance.
48. In the case of *Certificates for Time Stamping Units* issued by the FNMT-RCM to third parties (*Entities* that will be established as *Time Stamping Authority* to provide a *Time Stamping Service*), it will be the responsibility of said *Entities* to guarantee, in its case, the validity of that service in accordance with the technical standards and current legislation. In these cases, the FNMT-RCM is exempt from all responsibility related to the provision of the aforementioned *Time Stamping Service*. FNMT-RCM is limited, in this case, to the issuance of an *electronic certificate*, with the technical capacity to issue *Electronic time stamps*, to the duly accredited *Entity*.
49. A specific case of *Certificate for Time Stamping Units* is the one used by FNMT-RCM to provide its *Time Stamping Service*, as a qualified *Trust Service Provider*, according to the Policy and Practices of the *Qualified Time Stamping Service*<sup>1</sup>, and in accordance with the European standard ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

5.5.1.4. *Responsibility of User Entity and relying parties*

50. The *User Entity*, the third parties that trust *Certificates* and, in general, the *Electronic Community* members, shall be responsible for verifying and checking the status of *Certificates*, and under no circumstance will the *Entity* assume that *Certificates* are valid without implementing any verification.

---

<sup>1</sup> Policy and Practices of the Qualified Time Stamping Service Statement can be consulted at <http://www.cert.fnmt.es/dpcs/>



51. The *User Entity* and third parties that trust *Certificates* shall not be considered to have acted with the minimum due diligence if it trusts in an *Electronic Signature* based on a *Certificate* issued by FNMT-RCM without having complied with the *Certification Practices Statement* and checked that said *Electronic Signature* can be verified by reference to a valid *Certification String*.
52. If the circumstances require additional guarantees, the *User Entity* must obtain additional guarantees so that such trust can be reasonable.
53. Similarly, the *User Entity* shall be responsible for complying with the *Certification Practices Statement* and possible amendments thereto in future, paying special attention to the limits of use established for *Certificates* under this *Certification Policy*.

#### 5.5.2. Duties and guarantees of the parties

##### 5.5.2.1. Trust Services Provider's duties and guarantees.

54. FNMT-RCM is not subject to any guarantees or obligations other than those established in the regulations applicable to the sector and in the *Certification Practices Statement*.
55. Subject to what is provided in the legislation on electronic signature and the regulations to develop it, as well as in its specific regulations, the *Trust Services Provider* is under the following obligations:
56. Before a *Certificate* is issued:

- Checking the identity and particulars of the *Certificate Applicant* and the *Subscriber* and/or its *Representative*, and obtaining the representation that the *Applicant* is authorized by the *Subscriber* to file the application. No *Certificates* shall be issued to those under age unless they qualify as emancipated.

Identification will be implemented through acceptable electronic signature certificates and the functionalities established in respect of the DNle [electronic ID document] for the above-mentioned purposes.

- In the registration process, verifying the data concerning the *Subscriber's* legal personality and the *Representative's* capacity. These verification measures must be implemented according to the *Specific Certification Practices* contained in this document and following the FNMT-RCM registration procedures.

In the processes for verification of the above-mentioned data, FNMT-RCM may verify said data through third parties that have the authority to attest or through public or private record and register offices.

- Verifying that all the information contained in the *Certificate* application matches that supplied by the *Applicant*.
- Checking that the *Applicant* has the *Private Key* that, upon issue of the *Certificate*, will be the *Seal Creation Data* corresponding to the *Seal Verification Data* that will appear in the *Certificate*; and checking that they match.



- Guaranteeing that the procedures followed ensure that the *Private Keys* that will be the *Seal Creation Data* are generated without any copies of the Data being made or without the Data being stored by FNMT-RCM.
- Delivering information to the Subscriber, Representative and *Applicant* in such a manner that the *Confidentiality* of the information is safeguarded.
- Making the *Certification Practices Statement* available to the *Applicant, Subscriber, Representative* and any other interested parties (<http://www.ceres.fnmt.es>), as well as any other information relevant to the development of the procedures related to the lifecycle of the Certificates purpose of this *Certification Policy* and *Specific Certification Practices* in conformity with the applicable regulations.

57. Information keeping by FNMT-RCM

- Keeping all information and documentation related to each *Certificate*, in the right conditions of safety, for fifteen (15) years as from the time of issue.
- Keeping a safe updated *Certificate Directory* where the *Certificates* issued are identified, as well as their validity, including identification of *Certificates* that have been revoked, in the form of *Revocation Lists*. The integrity of this *Directory* must be safeguarded through the use of systems that conform to the specific regulatory provisions issued in Spain and, as the case may be, in the EU in this respect.
- Keeping a *Certificate* status information and inquiry service.
- Setting a dating mechanism that makes it possible to determine accurately the date and the time when a *Certificate* was issued or its validity expired or was suspended.
- Keeping the *Certification Practices Statement* in the right conditions of safety for 15 years, after it has been repealed because a new version has been published.

58. Personal Data Protection:

- FNMT-RCM undertakes to comply with the legislation in force in matters of *Personal Data Protection*, fundamentally, Organic Law 15/1999, of 13 December, on Personal Data Protection, Royal Decree 1720/2007, of 21 December, which approves the Regulations for development of Organic Law 15/1999, of 13 December, on personal data protection and any other applicable regulations.
- The TSPS includes information about the data protection policy followed by FNMT-RCM, and about the use of data.

59. *Certificate* revocation :

- The procedure for *Certificate* revocation as contained in this document provides information about revocation of *Certificates* and the obligations that FNMT-RCM undertakes in this respect.

60. Termination of the activity of the FNMT-RCM as *Trust Service Provider*:

- In this regard you can see the corresponding section of the TSPS.

#### 5.5.2.2. *Duties of the Registry Office*

61. As regards management of the lifecycle of *Component Certificates*, FNMT-RCM is the only authorized *Registry Office*, through its *Registry Area*, and its duties will be the following:
- In general, to apply the procedures established by FNMT-RCM in the *Certification Policy and Practices* and applicable in the performance of its Certificate management, issue and revocation functions, and not to change this framework of action.
  - In particular, to check the identity and any other particulars of *Certificate Applicants, Subscribers* and *Representatives*, which are relevant to the actual purpose of Certificates, employing any means permitted by law and in conformity with the TSPS provisions in general and this *Specific Certification Policy and Practices* in particular.
  - To check that the domain title holder’s name matches the *Subscriber’s* identity or, if appropriate, to obtain the *Subscriber’s* authorization, which will be associated with the *Component Certificate*, using the means within its reach that, reasonably, make it possible to prove the title, according to the state of technology.
  - To obtain expressly the *Subscriber’s* representation as to the title over the *Component*, and this representation must state that the *Subscriber* has sole power to decide about the *Component*.
  - To keep all information and documentation related to *Certificates*, in respect of which it handles the application, renewal or revocation, for fifteen (15) years.
  - To receive and handle *Certificate* applications and issue contracts (pdf form) with the *Subscriber*.
  - To check diligently the grounds for revocation that might affect the validity of *Certificates*.

#### 5.5.2.3. *Duties of Applicant and Subscriber*

62. The *Applicant* and the *Subscriber* of *Certificates* issued under this *Certification Practices Statement* undertake:
- Not to use the Certificate outside the limits specified in this specific *Certification Policy and Practices*.
  - Not to use the *Certificate* if the *Trust Services Provider* has ceased its activity as the *Certificate Issuing Entity* that issued the *Certificate* in question, particularly in situations where the provider’s *Seal Creation Data* may be at risk and this has been reported.
  - To supply true information on the *Certificate* application and keep it updated, having the contracts subscribed by person with sufficient capacity.

- Not to apply, for the certificate *Subject*, for distinctive signs, names or other industrial or intellectual property rights if one is not their title holder or licensee or one cannot prove to have authorization for their use.
- To act diligently in respect of the custody and keeping of *Signature / Seal Creation Data* or any other sensitive information such as *Keys*, *Certificate* activation codes, access words, personal identification numbers, etc., as well as of *Certificate* physical formats. The foregoing means in any event that the data mentioned cannot be disclosed.
- To be aware of and comply with the *Certificate* conditions of use established in the conditions of use and in the *Certification Practices Statement* and in particular, the limits of use of *Certificates*.
- To be aware of and comply with any amendments to the *Certification Practices Statement*.
- To apply for revocation of the relevant *Certificate*, according to the procedure described in this document, notifying FNMT-RCM diligently of the circumstances for revocation or suspicion of the loss of *Confidentiality*, the disclosure, modification or unauthorized use of *Signature Creation Data*.
- To go over the information contained in the *Certificate* and report any error or inaccuracy to FNMT-RCM.
- To verify, before trusting in any *Certificate*, the recognized electronic *Signature* of the *Trust Services Provider* that issues the *Certificate*.
- To notify FNMT-RCM forthwith of any change in the data supplied on the *Certificate* application, applying, where appropriate accordingly, for revocation of the *Certificate*.
- To return or destroy the *Certificate* where it is so demanded by FNMT-RCM, and not to use it with the purpose of signing or identifying oneself electronically when the *Certificate* runs out or is revoked.

#### 5.5.2.4. *Duties of the User Entity and of relying parties*

63. The *User Entities*, the *Electronic Community* members and, in general, any third parties that trust *Certificates* issued under this *Certification Practices Statement* undertake:
- To verify, before trusting in any *Certificate*, the recognized Electronic Signature of the *Trust Services Provider* that issues the *Certificate*.
  - To verify that the *Subscriber’s Certificate* is still valid and active.
  - To verify the status of *Certificates* on the *Certification String*, through the FNMT-RCM *Information and consultation service on the state of validity of the certificates*.
  - To check the limits of use regarding the *Certificate* that is being verified.

- To be aware of the *Certificate* conditions of use according to the applicable *Certification Policies and Practices Statements*.
- To notify FNMT-RCM of any irregularity or information about the *Certificate* and which may be considered as grounds for revocation thereof, supplying all evidence available.

## **5.6. LIMITS OF USE AND ACCEPTANCE OF CERTIFICATES**

64. FNMT-RCM shall not be liable for *Certificates* that appear in a fraudulent manner to have been issued by FNMT-RCM, and FNMT-RCM shall take legal actions against these fraudulent actions if they come to its knowledge either directly or because they are reported by the interested parties.
65. If a member of the *Electronic Community* or a *User Entity* or a third party trust in a *Component Certificate* without verifying the status of the *Certificate* in question, no cover shall be obtained from this *Certification Practices Statement* and said member, *User Entity* or third party shall not be entitled to claim or take legal action against FNMT-RCM for damages or conflict stemming from the use of or trust in a *Component Certificate*.
66. In addition, even within the *Electronic Community*, this type of *Certificates* may not be used, by person other than FNMT-RCM, for:
- Signing another *Certificate*.
  - Generating *Time Stamps* for *Time Stamping* procedures, with the exception of *Certificates* issued by FNMT-RCM for *Time Stamping Units*.
  - Providing services, for a fee or free of charge, such as, for example, merely for enunciative purposes:
    - Providing OCPS services
    - Providing electronic billing services.
    - Generating *Revocation Lists*
    - Providing notice services.

## **6. SPECIFIC CERTIFICATION PRACTICES FOR “AC COMPONENTES INFORMÁTICOS” COMPONENT CERTIFICATES**

67. These *Specific Certification Practices for Component Certificates* define the set of practices adopted by FNMT-RCM, as *Trust Services Provider*, for management of the lifecycle of *Certificates* issued under the FNMT-RCM component *Certificate Certification Policy*.

### **6.1. COMPONENT CERTIFICATE LIFECYCLE MANAGEMENT**

68. This section defines aspects that because of their peculiarities need to be detailed further, even though these aspects are already indicated in the TSPS, of which this document is part.

### **6.1.1. Application procedure**

69. The application procedure includes collecting personal data on the *Component Certificate Applicant*, on the *Subscriber* and, if appropriate, on the *Representative*. Additionally, the specific information that the *Certificate* will contain is verified and the contract with FNMT-RCM is entered into, for subsequent issue thereof. Part of the development of this system is a detailed registration procedure, with the necessary aspects concerning application for the *Certificate* being made available to *Applicants*. These activities are performed only by the authorized *Registry Office*.
70. The FNMT-RCM checks for a CAA record for each DNS Name which will be included in a *Certificate for website authentication* to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found. If a CAA record exists, FNMT-RCM will not issue this *Certificate* unless either the certificate request is consistent with the applicable CAA Resource Record set.
71. The *Subscriber* (through the *Applicant*) generates the *Public and Private Keys* and applies for the *Certificate* by completing a FNMT-RCM web form that will include:
- The *Component* identification data
  - Data concerning the title to the *Domain Names*, or representation of the *Title* to the *Component*, which will be linked to each type of *Certificate*.
  - Data on the *Subscriber* as person or entity, whether public or private, interested in the issue of a *Component Certificate*.
  - Data on the *Certificate Subscriber’s Representative* where the *Subscriber* is an entity.
  - Data on the *Certificate Applicant*.
  - The *Component Certificate* petition PKCS#10 or SPKAC
72. In any event, all the form fields indicated as compulsory must be completed and the whole form must be electronically signed by the *Applicant*, and the signature will be verified by FNMT-RCM.

### **6.1.2. Subscription and sending of contract by Subscriber**

73. After completing the application, the *Subscriber* must sign the contract electronically (pdf format, which includes acceptance of the conditions of use for the *Certificate* applied for and that it will be available on the relevant webpage) and then send it, through the electronic address provided, to the FNMT-RCM *Registry Office*, for processing.
74. The pdf contract will be signed preferably with the *Subscriber’s Legal Person Certificate* issued by FNMT-RCM, but other acceptable *Certificates* can be used.
75. The following will be grounds for bringing to a halt the *Certificate* issuing process: not sending the contract signed by the *Subscriber*, not making the payment, the lack of data or of the documentation required.



76. FNMT-RCM will keep a copy signed by the Subscriber and will file it together with all the documentation relating to the software *Component* in question.
77. During the registration process, the FNMT – RCM *Registry Office* verifies all the information related to the *Certificate* holder’s identity.

#### 6.1.3. Validation of domain authorization or control

78. In order to validate the domain of the *Certificate for website authentication*, the FNMT-RCM uses one of the permitted processes and procedures for validating the applicant's ownership or control of the domain, according to the CA/Browser Forum's Baseline Requirements (version 1.4.1), concretely in the section “3.2.2.4.5 Domain Authorization Document”.
79. The FNMT-RCM confirms that the applicant controls over the requested Fully Qualified Domain Name (FQDN) which are included in the *Certificate for website authentication*. For this purpose, the FNMT-RCM consults, through the application registering the applications for these *Certificates*, the identity of the Applicant and the name of the FQDN. It then verifies that the request comes from the person who has the control over said domain (according to the registries of WHOIS domains, RED.ES, etc.) or has authorization by the latter. Additionally, it is verified that the request for the *Certificate* has been made after the registration in said registers.

#### 6.1.4. Issue

80. FNMT-RCM will verify that the data on the application are true and, if appropriate, the *Representative’s* capacity, through the relevant verification measures and keeping the appropriate electronic evidence.
81. The electronic signature generated for the signing of the contract will be verified by FNMT-RCM.
82. Upon receipt of the web application and the contract at the *Registry Office*, FNMT-RCM will begin to process the petition through its internal software.
83. If the *Certificate* is associated with one or more Internet domains, the Registry Office will check with the existence and singularity of such domains with the Internet Corporation for Assigned Names and Numbers (ICANN) and that the Subscriber is entitled to use such domains or subdomains by consulting on the authorized domain registrars’ databases (whois.icann.org, www.nic.es, [www.eurid.eu...](http://www.eurid.eu...)) and will keep proof of the inquiry.
84. The *Registry Office* will verify the *Subscriber’s* personality and, if appropriate, the *Representative’s* personality and capacity, through verification of the *Electronic Signatures* and *Certificates* used in the process and/or inquiry on the databases of the Companies Register or of trustworthy third parties.
85. Should there be any errors or contradictions, FNMT-RCM will contact the *Applicant* and *Subscriber*, for clarification and, if appropriate, rectification.



86. FNMT-RCM, using its *Electronic Signature*, will subscribe the information contained in the *Certificates* FNMT-RCM issues, thus validating their authenticity and integrity.
87. FNMT-RCM will act:
- To check that the *Certificate Applicant* has the *Private Key* corresponding to the *Public Key* to certify.
  - To determine that the information included in the *Certificate* is based on the information provided by the *Applicant* and the *Subscriber* and, applying the usual diligence in the performance of the verification procedure, that said information is true.

#### **6.1.5. Publication and distribution**

88. Upon prior notice, the *Certificate* is delivered by making it available to the *Applicant* on the *Certificate* download application, once the other requirements for its issue have been met.
89. FNMT – RCM will make the *Certificate* available to the *Applicant* no later than 72 hours as from receipt at the Registry Office of the necessary documentation to perform the verification process prior to issue.

#### **6.1.6. Notification to applicant**

90. FNMT – RCM notifies the *Applicant* of a *Certificate* that the *Certificate* is available by sending an electronic mail addressed to the *Certificate Subscriber’s Representative* and to the *Applicant*.
91. FNMT – RCM does not notify other entities of the issue of *Certificates*.

#### **6.1.7. Validity**

##### *6.1.7.1. Expiry*

92. The maximum term of validity of the *Certificates for website authentication* (Standard, Wildcard and Multi-domain) is two years as from the time they are issued. The *Component Certificates* for entity seal and for code signature, the maximum term of validity is three years. And for *Component Certificates* for use in *Time Stamping Units* the maximum term of validity is five years. These maximum term of validity are maintained as long as they are not affected by the reasons and procedures laid out in the section “Termination of a certificate validity”.

##### *6.1.7.2. Termination of Certificate validity*

93. The *Component Certificates* issued by FNMT-RCM shall become null and void in the following cases:
- a) Expiry of the *Certificate* term of validity.
  - b) Cessation of the FNMT-RCM activity as a *Trust Services Provider*, unless, upon

express consent by the *Subscriber*, the *Certificates* issued by FNMT-RCM have been transferred to another *Trust Services Provider*.

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

c) Revocation of a *Certificate* on any of the grounds contained in this document.

94. For the effects listed above, it is to be noted that the application for issue of a *Component Certificate*, where there is another *Certificate* in force with the same identification data and belonging to the same *Issuance Law*, shall not cause revocation of the first *Certificate* obtained. Therefore, there may be several *Certificates* in force with the same *Subject* but a different serial number.
95. Termination of the validity of a *Certificate* due to revocation shall take effect as from the date that FNMT-RCM has evidence of any determining facts and it is so stated on the *Revocation List* of the FNMT-RCM *Information and consultation service on the state of validity of the certificates*.

#### **6.1.8. Renewal**

96. *Component Certificates* are always renewed by issuing new keys, so the process is actually the same as that followed to obtain a new *Certificate*.

#### **6.1.9. Revocation**

97. Revocation of *Component Certificates* may be applied for during the term of validity appearing on the *Certificate*. It consists in the cancellation of the guarantee of the user's identity and other properties and its correspondence with the associated *Public Key*
98. Revocation of a *Component Certificate*, subject to the causes of revocation indicated below, may be applied for only by the *Subscriber*.
99. The FNMT-RCM makes available to subscribers, third parties that trust, software providers and third parties a means of communication through the web site <https://www.sede.fnmt.gob.es/> with clear instructions, to allow them to report any matter related to this type of *Certificates*, as to a supposed commitment of *Private key*, improper use of *Certificates* or other types of fraud, compromise, misuse or misconduct.

##### *6.1.9.1. Causes of revocation*

100. FNMT-RCM shall only be liable for the consequences arising from not having revoked a *Certificate* in the following cases:
- Where the revocation was requested by the *Subscriber* following the procedure established for the purpose.
  - Where FNMT-RCM was notified of the request for revocation or the cause of it through court or administrative decision.

- Where causes c) to e) in the following section are supported with unequivocal evidence, prior identification of the applicant for the revocation (the *Subscriber*).
101. The above being taken into account, the following are causes for revocation of a *Component Certificate* :
- a) Request for revocation by the *Subscriber*, or a duly authorized third party, made by reliable means. In any event, this request shall be made by the *Subscriber* in the following cases:
    - Loss of the *Certificate* physical format.
    - Use by a third party of the *Signature Creation Data* associated with the *Signature Verification Data* included in the *Certificate* and linked to the *Subscriber's* identity.
    - Jeopardizing the *Signature Creation Data*.
    - Non-acceptance of new conditions after new versions of *Certification Practices Statements* or *Specific Policies and Practices* have been drawn up and published, during the period of one month after publication.
  - b) Court or administrative order that rules it so.
  - c) The *Subscriber's* death or termination or dissolution of its legal personality.
  - d) The *Subscriber's* total or partial unforeseen disability.
  - e) Inaccuracy in the data provided by the *Applicant* to obtain the *Certificate*, or alteration of the data provided to obtain the *Certificate*, especially whenever the domain name or the IP consignee to the *Certificate* is no longer controlled by the *Subscriber*.
  - f) Applying, for the *Certificate Subject*, for distinctive signs, names or other industrial or intellectual property rights where the *Subscriber* is not their title holder or licensee or is not authorized for their use.
  - g) Failure to pay for the services provided.
  - h) *Certificate Subscriber's* violation of a substantial obligation contained in this *Certification Policy* and which has come to the knowledge of FNMT-RCM or the Registry Office and may have affected the *Certificate* issue procedure.
  - i) Jeopardizing the FNMT-RCM confidentiality of the *Signature Creation Data* used by FNMT-RCM to sign the *Certificates* that it issues.
  - j) Using the *Certificate* with the purpose of making users doubt about the provenance of the products or services offered, leading users to believe that the provenance is different from that offered. For this, the criteria on activity that violates the consumers and users, trade, competition and advertising regulations shall apply.
  - k) Failure to comply with the requirements defined by the audits schemes that the *Certification Authority* "AC Computer Components" is submitted, with special

attention to those algorithms and key sizes which present an unacceptable risk by the relying parties on these certificates.

102. In no circumstance shall it be construed that FNMT-RCM undertakes any obligation to verify the points indicated in paragraphs c) to f) in this section. The other cases shall take effect as soon as they are known to FNMT-RCM.
103. Activities amounting to offences or misdemeanours and which are not known to FNMT-RCM and affect the data and/or Certificate, the inaccuracy in the data or lack of diligence in their communication to FNMT-RCM, shall release FNMT-RCM from responsibility.
104. If the data do not match reality, where the data are found in Public Record offices, this event shall not be attributable to FNMT-RCM in so far as there are no instruments for direct electronic transmission communication between FNMT-RCM and the different Public Record offices, unless the data are reported to FNMT-RCM by reliable means.

#### 6.1.9.2. *Procedure for Certificate revocation*

105. Revocation shall be processed only by the FNMT-RCM *Registry Office*.

1. *Subscriber’s request*

The *Subscriber* must send the application form for revocation, completed and electronically signed, to FNMT-RCM, with the same *Certificates* accepted for application and through the electronic channels enabled by this Entity.

Additionally, there is a 24/7 telephone helpline (902 200 616), where one can apply for revocation. The call will be recorded and registered, serving as support and guarantee of acceptance of the application made for revocation.

To apply for revocation of a *Certificate* by telephone, the *Applicant* must be the *Subscriber* or the *Subscriber’s Representative* in the case of legal persons or public organizations and it must appear as such on the certificate to revoke. In the case of the representative, it must be the same person that acted as such on the application for issue of the certificate for which revocation is applied for.

2. FNMT-RCM processing of request

The FNMT-RCM registrar will receive the revocation agreement and shall implement the same verification measures about the identity and capacity of the *Subscriber* and *Representative* as those implemented in the case of application for issue and, if appropriate, will process the revocation of the *Component Certificate*.

As soon as the revocation is approved, the *Subscriber* will be served notice of the *Certificate* revocation, on the electronic mail address indicated on the application.

After FNMT-RCM has proceeded to revoke the *Certificate*, the relevant *Revocation List* will be published in the safe Directory; the List will contain the revoked Certificate serial number, the date and time of revocation and the cause of revocation.



106. The FNMT - RCM, although it has not received the request for revocation by the *Subscriber* shall revoke those certificates for which has obtained evidences to be included in any of the grounds for revocation provided in this *Specific Certification Policies and Practices*.

#### 6.1.9.3. *Effects and time of revocation*

107. Revocation of a *Certificate*, i.e., termination of its validity, shall take effect as from the date that FNMT-RCM has evidence of any determining factors and it is so reflected on the *Revocation List* and on its *Information and consultation service on the state of validity of the certificates*.

108. Revocation of a *Certificate* is immediate as from receipt of the revocation agreement or as from the applicant’s accreditation by telephone.

#### 6.1.10. **Suspension**

109. Suspension it is not allowed for these types of *Certificates*.

#### 6.1.11. **Notification of the change of status of the certificate**

110. Once the revocation of the *Certificate* has become effective, FNMT-RCM sends a communication to the email address of the *Representative* of the *Subscriber*, informing of the change of status of the *Certificate*.

#### 6.1.12. **Verification of Certificate status**

111. The *Certificate Subscriber* and any third parties that trust the *Certificates* may verify the status of a *Certificate* in the manner and under the conditions contained in this section.

112. The status of a *Component Certificate* may be verified through the *Information and consultation service on the state of validity of the certificates* through the OCSP protocol.

113. These services will be available 24 hours every day of the year, except for circumstances outside FNMT–RCM or maintenance operations. FNMT-RCM will report the latter situation on <http://www.ceres.fnmt.es> if possible no less than forty-eight (48) hours in advance and will try to have the services back on again in no later than twenty-four (24) hours.

114. FNMT-RCM has an OCSP answering service (“OCPS answer”) to offer the *Information and consultation service on the state of validity of the certificates*.

115. The service operates in the following way: the OCSP server receives the OCSP request made by an *OCSP Client* registered with the system or by a commercial application (for example, a web browser) which gets from the certificate itself (field Authority Info Access) the link to this service. The OCSP server checks the status of the *Certificates* included in the request and, if the request is valid, an OCSP reply will be issued communicating the status at the time of the *Certificates* included in the request.



116. The User Entity has the responsibility of obtaining an *OCSP Client* to operate with the OCSP server made available by FNMT-RCM.
117. The User Entity applying for the OCSP service has the responsibility of securing, if appropriate, the consent of the *Subscriber* of the *Certificate* for which the OCSP service is applied for, and of giving the *Subscriber* information about the relevant conditions and limitations.
118. The foregoing is understood with the scope and limits established by the legislation on automated personal data processing and in accordance with the relevant contracts, agreements or *Issue Laws* which regulate the FNMT-RCM electronic certification service.
119. FNMT-RCM does not provide a service for verification of *Certificates* of other *Subscribers* except for those cases where it is so established through agreements and/or contracts with the due consent of the *Electronic Community* members or in the terms laid out in the Issue Law.
120. The FNMT-RCM operates and maintains its capabilities of maintaining its CRLs and OCSP service with sufficient resources to provide a maximum response time of ten seconds under normal operating conditions.

## **6.2. CERTIFICATE FOR USE IN THE TIME STAMPING UNIT OF THE FNMT-RCM**

121. A specific case of *Component Certificate* is the one used by FNMT-RCM to provide one of its Qualified Trust Service: the *Time Stamping Service*, as a qualified *Trust Service Provider*, according to the Policy and Practices of the *Qualified Time Stamping Service Statement*, that can be consulted at <http://www.cert.fnmt.es/dpcs/>.
122. The *Certificate* used by FNMT-RCM to provide its *Time Stamping Service* can be downloaded from <https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt>

## **7. FEES**

123. FNMT-RCM will apply to Public Administrations the fees approved by the Undersecretary’s Office to which it is attached, for the issue of Certificates or, by default, the fees arranged by management agreement or mandate entered into for the purpose.
124. Fees to apply to the private sector are governed by the contract subscribed for provision of *Certificates*. Additionally, for issue of *Certificates* to *Subscribers*, FNMT-RCM may set the fees and ways of payment it considers appropriate each time. Information on the price and terms of payment of *Certificates* may be obtained on the FNMT – RCM webpage or it will be provided by the appropriate commercial area upon request to the electronic mail address [commercial.ceres@fnmt.es](mailto:commercial.ceres@fnmt.es).

## **8. AUDITS**

125. The *Certification Authority* "AC Componentes Informáticos" is subject to periodic audits in accordance with the requirements established by the European standards ETSI EN 319 401 “General Policy Requirements for Trust Service Providers”.
126. The Entity Seal *Certificate* and the *Certificate* for use in the Time Stamping Unit of the FNMT-RCM, are *Qualified Certificates* in accordance with the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Therefore, periodic audits ensure compliance with the European standards ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”, ETSI EN 319 412-3 “Certificate profile for certificates issued to legal persons” y ETSI EN 319 412-4 “Certificate profile for web site certificates”. These audits are conducted annually by an accredited external company.
127. This document, certification policies and practices, is reviewed at least once a year to ensure alignment with technical updates and regulations.

## **9. CERTIFICATE PROFILES**

128. All *Certificates* issued under this policy conform to standard X.509 version 3. The profile of each type of Certificate can be consulted at <http://www.cert.fnmt.es/dpcs/>

### **9.1. NAME RESTRICTIONS**

129. The *Certificate* codes follow the standard RFC 3280 “Internet X.509 *Public Key Infrastructure Certificate* and Certificate Revocation List (CRL) Profile”. All the fields defined on the Certificate profiles in annex II to these *Certification Policies*, except for the fields where it is otherwise indicated, use the UTF8String codes.

### **9.2. USE OF THE POLICY CONSTRAINTS EXTENSION**

130. The Policy Constraints extension of the root certificate is not used.

### **9.3. SYNTAX AND SEMANTIC OF POLICY QUALIFIERS**

131. The Certificate Policies extension includes a Policy Qualifier field: CPS Pointer, which contains the URL where the *TSPS* and the *Certification Policies and Specific Certification Practices* as applicable to *Certificates* are published.

### **9.4. SEMANTIC TREATMENT OF THE “CERTIFICATE POLICY”**

132. The *Certificate Policy* extension includes the policy OID field, which identifies the policy associated with the *Certificate* by FNMT – RCM, as well as the two fields indicated in the paragraph above.

## **ANEXO I: IDENTIFICATION OF THE CERTIFICATION AUTHORITY CERTIFICATE**

The Certification Authority Certificate used for signature / seal the Certificates and the CRLs is identified as follows:

### **Certification Authority Certificate “AC Componentes Informáticos”**

Distinguished Name: OU = AC Componentes Informáticos, O = FNMT-RCM, C = ES

- Serial Number: 34:C6:AB:04:4E:36:99:12:51:C8:25:0B:6C:94:D6:C0
- Valid from: 24 June 2013
- Valid until: 24 June 2028
- Digital fingerprints:
  - Digital fingerprint (sha1):  
C7:72:B4:8D:23:85:E5:02:E8:47:37:DB:E7:87:B6:43:11:91:12:47
  - Digital fingerprint (sha256):  
F0:38:42:1F:07:F2:0D:63:A2:0D:36:91:E5:A1:78:AB:84:59:EB:E5:70:C1:64:7B  
:76:90:55:4E:F2:38:76:AB