TRANSLATION

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SPECIFIC CERTIFICATION POLICY AND PRACTICES

APPLICABLE TO "AC SOFTWARE COMPONENTS"

COMPONENT CERTIFICATES

	NAME	**DATE**
Prepared by:	FNMT-RCM / v1.1	07/03/2014
Revised by:	FNMT-RCM / v1.1	07/03/2014
Approved by:	FNMT-RCM / v1.1	07/03/2014

BACKGROUND OF THE DOCUMENT – TRACK CHANGES			
Version	**Date**	**Description**	**Author**
(1.0)	21/11/2013	First version	FNMT-RCM
(1.1)	07/03/2014	Elimination of suspension	FNMT-RCM

Reference: DPC/PC-DPC-ACCOMP-0100/SGPSC/2014

Document classified as: *Public*

Mª TERESA DE LA CUESTA LÓPEZ
TRADUCTORA E INTÉRPRETE DE INGLÉS
C/ BAHÍA DE MAHÓN, 14 - AT. DCHA.
28042 MADRID - TEL. 656 433 628

CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

[PF stands for natural person; and PL, for legal person.]

1. PREAMBLE

1. These *Specific Certification Policies and Practices* describe the issue of *Component Certificates* by FNMT-RCM for use by *Software Components*. These *Certificates* link *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 *Certification 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 *Certification 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 General Certification Practices Statement*" [abbreviated in Spanish: DGPC]. 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 *Certification Services Provider*.

- Any annexes as are considered relevant for public information about conditions of use, limitations, responsibilities, 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 DGPC 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 DGPC 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 *Certification 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 DGPC 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.

3. DEFINITIONS

15. For the interpretation of this document, the following definitions are added to those contained in the DGPC:

- *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*: Natural or legal person, public body or agency recipient of the activities of FNMT-RCM as *Certification 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 General Certification Practices Statement).

4. ORDER OF PREVALENCE

16. 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 *General Certification Practices Statements.*

Therefore, should there be any contradiction between this document and the provisions of the DGPC, 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

17. 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 Software Components)
Reference/OID and specific name	1.3.6.1.4.1.5734.3.9.1 – *Component Certificates* for entity stamp (*Subscriber's* profile: natural person) 1.3.6.1.4.1.5734.3.9.2 – *Component Certificates* for entity stamp (*Subscriber's* profile: legal person) 1.3.6.1.4.1.5734.3.9.3 – *Component Certificates* for code signature (*Subscriber's* profile: natural person) 1.3.6.1.4.1.5734.3.9.4 – *Component Certificates* for code signature (*Subscriber's* profile: legal person) 1.3.6.1.4.1.5734.3.9.5 – Standard SSL *Component Certificates* (*Subscriber's* profile: natural person) 1.3.6.1.4.1.5734.3.9.6 – Standard SSL *Component Certificates* (*Subscriber's* profile: legal person) 1.3.6.1.4.1.5734.3.9.7 – Wildcard SSL *Component Certificates* (*Subscriber's* profile: natural person) 1.3.6.1.4.1.5734.3.9.8 – Wildcard SSL *Component Certificates* (*Subscriber's* profile: legal person) 1.3.6.1.4.1.5734.3.9.9 – Plus SSL *Component Certificates* (*Subscriber's* profile: natural person) 1.3.6.1.4.1.5734.3.9.10 – Plus SSL *Component Certificates* (*Subscriber's* profile: legal person) 1.3.6.1.4.1.5734.3.9.11 – Multi-domain SSL *Component Certificates* (*Subscriber's* profile: natural person) 1.3.6.1.4.1.5734.3.9.7 – Multi-domain SSL *Component Certificates* (*Subscriber's* profile: legal person)

Version	1.0
Creation Date	21 November 2013
Related DPC	FNMT-RCM General Certification Practices Statement
Location	http://www.ceres.fnmt.es/dpcs

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* and a type of *Subscriber*. The *Subscriber* can be a natural person or a legal person.

This DPC contemplates the following types of *Certificates*:

- Standard SSL Certificate: It allows the establishment of safe communications using the SSL/TSL protocol. This type of *Certificate* guarantees the identity of the domain where a web is found.
- Plus SSL Certificate: Its purpose is the same as that of the standard SSL *Certificate* but it adds the possibility of choosing the extended use of the *Certificate* keys (client authentication and/or e-mail protection).
- Wildcard SSL Certificate: It guarantees security for an unlimited set of domains, starting from the third level, with a single SSL *Certificate*.
- Multi-domain SSL Certificate (SAN/ECC): It guarantees security for a set of domains which are independent from one another. In addition, it enables the user to choose the extended use of the *Certificate* keys (client authentication and/or e-mail protection).
- Code Signature Certificate: It makes it possible to sign software and guarantee the proprietor's identity and the integrity of the code.
- Entity Stamp 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, any extended use of the key).

5.2 COMMUNITY AND SCOPE OF APPLICATION

18. 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 DGPC of FNMT-RCM.

5.3 RESPONSIBILITIES AND DUTIES OF THE PARTIES

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

20. 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, if there is no reliable notice that allows to transfer the intended effects to the management of *Certificates.*

5.3.1 Responsibilities of the parties

21. 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 Inquiry Service on the Status of Certificates.*

22. 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 for damages or conflict stemming from the use of or trust in a *Component Certificate.*

5.3.1.1 Certification Services Provider's Responsibility

23. 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.

24. 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.

25. FNMT-RCM shall only be liable for deficiencies in the procedures pertaining to its activity as *Certification 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.

26. 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.

27. 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 responsibilities of the parties, is considered negligence.

28. FNMT-RCM shall bear no responsibility for any software that FNMT-RCM has not provided directly.

29. 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.

30. 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.

31. 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).

5.3.1.2 Applicant's responsibility

32. 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*.

33. 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.

5.3.1.3 Subscriber's responsibility

34. 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.

35. 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.

36. The *Subscriber* shall be responsible for and, therefore, will have the obligation of not using the *Certificate* if the *Certification 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.

5.3.1.4 User Entity's responsibility

37. The *User Entity* 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.

38. The *User Entity* 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*.

39. If the circumstances require additional guarantees, the User Entity must obtain additional guarantees so that such trust can be reasonable.

40. 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*.

5.3.2 Duties and guarantees of the parties

5.3.2.1 Certification Services Provider's duties and guarantees

41. 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.*

42. 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 *Certification Services Provider* is under the following obligations:

43. 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 DNIe [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 *Signature Creation Data* corresponding to the *Signature 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 *Signature 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.

44. 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.

45. 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 DGPC includes information about the data protection policy followed by FNMT-RCM, and about the use of data.

46. *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.

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

- The relevant section in the DGPC provides information in this respect.

5.3.2.2 Duties of the Registry Office

48. 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 DGPC 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, 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.*

5.3.2.3 Duties of Applicant and Subscriber

- Not to use the *Certificate* outside the limits specified in this specific *Certification Policy and Practices.*

- Not to use the *Certificate* if the *Certification Services Provider* has ceased its activity as the *Certificate Issuing Entity* that issued the *Certificate* in question, particularly in situations where the provider's *Signature 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 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 *Certification 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.

5.3.2.4 Duties of the User Entity and of trusting third parties

- To verify, before trusting in any Certificate, the recognized *Electronic Signature* of the *Certification 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 Inquiry Service on the Status of 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.

5.4 LIMITS OF USE AND ACCEPTANCE OF CERTIFICATES

49. 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.

50. 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.*

51. 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 SOFTWARE COMPONENTS" COMPONENT CERTIFICATES

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

6.1 COMPONENT CERTIFICATE LIFECYCLE MANAGEMENT

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

6.1.1 Application procedure

54. 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.*

55. The *Subscriber* (through the *Applicant*) 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.

56. 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.

57. For *Time Stamping Unit Certificates*, the *Time Stamping Practices Statement*, in conformity with standard "ETSI 101 023 – Requirements for the policies of time stamping authorities", of the entity[1] that will provide the service as *Time Stamping Authority* and *Certificate Subscriber.*

6.1.2 Subscription and sending of contract by *Subscriber*

58. 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.

59. 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.

60. 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.

61. 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.

6.1.3 Issue

62. 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.

[1] The *Certificate Subscriber* entity must be registered as *Time Stamping* services provider on the *Certification Services Providers* register of the Ministry of Industry Tourism and Trade.

63. The electronic signature generated for the signing of the contract will be verified by FNMT-RCM.

64. 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.

65. If the *Certificate* is associated with one or more Internet domains, the *Registry Office* will check, on the authorized domain registrars' databases, that the title holder of the domain and the *Certificate Subscriber* match, and will keep proof of the inquiry.

66. 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.

67. Should there be any errors or contradictions, FNMT-RCM will contact the *Applicant* and *Subscriber*, for clarification and, if appropriate, rectification.

68. FNMT-RCM, using its *Electronic Signature*, will subscribe the information contained in the *Certificates* FNMT-RCM issues, thus validating their authenticity and integrity.

69. 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.

6.1.4 Publication and distribution

70. 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.

6.1.5 Validity

6.1.5.1 Expiry

71. The maximum term of validity of *Component Certificates* is three years as from the time they are issued, provided that their validity does not terminate for the reasons and procedures laid out in the section "Termination of a certificate validity". For *Time Stamping Unit Certificates*, the term of validity will be no more than five years.

6.1.5.2 *Termination of Certificate validity*

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

73. 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.

74. 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 Inquiry Service on the Status of Certificates.*

6.1.6 Revocation

75. 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.*

76. Revocation of a *Component Certificate*, subject to the causes of revocation indicated below, may be applied for only by the *Subscriber.*

6.1.6.1 Causes of revocation

77. 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*).

78. The above being taken into account, the following are causes for revocation of a *Component Certificate*:

Mª TERESA DE LA CUESTA BERNÁLDEZ
TRADUCTORA E INTÉRPRETE DE INGLÉS
C/ BAHÍA DE MAHÓN, 14 - AT. DCHA.
28042 MADRID - TEL. 656 403 628

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.*

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.

79. 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.

80. 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.

81. 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.

[The paragraph above appears highlighted in yellow in the original document.]

6.1.6.2 Effects of revocation

82. 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 Inquiry Service on the Status of Certificates*.

6.1.6.3 Procedure for Certificate revocation

83. 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.

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.

6.1.7 Verification of Certificate status

84. The *OCSP* protocol is used to verify the status of *Certificates*, by accessing the *Information and Inquiry Service on the Status of Certificates* through the address indicated for the purpose in the *Certificate* itself.

7. CERTIFICATE PROFILES

7.1 CERTIFICATION AUTHORITY

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (CA Root)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC ROOT FNMT-RCM		
5. Validity		15 years	Yes	
6. Subject		Certificate issuing entity (Subordinate CA)	Yes	
	6.1 Country	C=ES		
	6.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	6.3 Organization Unit	OU=AC Software Components	Yes	
7. Authority Key Identifier		Identifier of public key of root entity. Means to identify the public key corresponding to the private key used by CA to sign the certificate of this Subordinate CA.	Yes	
8. Subject Public Key Info		Component CA public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of Component CA public key	Yes	
10. Key Usage		Use of certified keys allowed.	Yes	Yes
	10.1 Digital Signature	0	Yes	
	10.2 Content Commitment	0	Yes	
	10.3 Key Encipherment	0	Yes	

	10.4 data Encipherment		0	Yes	
	10.5 Key Agreement		0	Yes	
	10.6 Key Certificate Signature		1	Yes	
	10.7 CRL Signature		1	Yes	
11. Certificate Policies			Certification policy	Yes	No
	11.1 Policy Identifier		2.5.29.32.0 (any Policy)	Yes	
	11.2 Policy Qualifier Id				
		11.2.1 CPS Pointer	http://www.ceres.fnmt.es/dpcs/	Yes	
		11.2.2 User Notice	Subject to the conditions of use included in Certification Practices Statement of FNMT-RCM (C/ Jorge Juan 106-28009-Madrid-Spain)	Yes	
12. CRL Distribution Point				Yes	No
	12.1 Distribution Point 1		CRL (ARL) distribution point 1 ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint	Yes	
	12.2 Distribution Point 2		CRL (ARL) distribution point 2 http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl	Yes	
13. Basic Constraints					Yes
	13.1 Subject Type		CA		
	13.2 Path length		0		
14. Authority Info Access				Yes	
	14.1 Access Method 1		Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)		
	14.2 Access Location 1		http://ocpsfnmtrcma.cert.fnmt.es/ocpsfnmtrcma/OcspResponder		
	Access Method 2		Identifier of method to access information on		

		additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)		
	Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt		

7.2 CERTIFICATES ISSUED

7.2.1 PF Entity Stamp

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 Given Name	Name of subscriber for which the certificate is issued	Yes	
	6.3 Surname	Surname of subscriber for which the certificate is issued	Yes	
	6.4 Serial Number	Tax ID number of subscriber for which the certificate is issued	Yes	
	6.5 Common Name	Name of component	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key corresponding to the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard.	Yes	

			The length of the key will be 2048 bits.		
9. Subject Key Identifier			Identifier of Component public key	Yes	
10. Key Usage			Use of certified keys allowed.		Yes
	10.1 Digital Signature		1	Yes	
	10.2 Content Commitment		0	No	
	10.3 Key Encipherment		1	Yes	
	10.4 Data Encipherment		1	Yes	
	10.5 Key Agreement		0	Yes	
	10.6 Key Certificate Signature		0	Yes	
	10.7 CRL Signature		0	Yes	
11. Extended Key Usage			Improved or extended use of keys	No	No
	11.1 Email protection		1.3.6.1.5.5.7.3.4	No	
	11.2 Client Authentication		1.3.6.1.5.5.7.3.2	No	
	11.3 AnyExtendedKeyUsage		2.5.29.37.0	No	
12. Certificate Policies			Certification policy	Yes	No
	12.1 Policy Identifier		1.3.6.1.4.1.5734.3.9.1	Yes	
	12.2 Policy Qualifier Id			Yes	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names					
	14.1 Subscriber's name		Id Field / Value: 1.3.6.1.4.1.5734.1.1 = <Name>	Yes	
	14.2 Subscriber's first surname		Id Field / Value: 1.3.6.1.4.1.5734.1.2 = <First surname>	Yes	
	14.3 Subscriber's second surname		Id Field / Value:	No	

		1.3.6.1.4.1.5734.1.3 = <Second surname>		
	14.4 Subscriber's Tax ID number	Subscriber's identification unique number (Tax ID number) Id Field / Value: 1.3.6.1.4.1.5734.1.4 = <Tax ID Number>	Yes	
	14.5 Name of component	Id Field / Value: 1.3.6.1.4.1.5734.1.8 = <Name of component>	Yes	
14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1	CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU=AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level allowed for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

TERESA DE LA CUESTA BERNÁLDEZ
TRADUCTORA E INTÉRPRETE DE INGLÉS
C/ BAHÍA DE MAHÓN, 14 - AT. DCHA.
28042 MADRID - TEL. 656 433 628

7.2.2 PJ Entity Stamp

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 LocalityName	Name of subscriber's locality	Yes	
	6.3 Organization	Subscriber' name	Yes	
	6.4 Organizational Unit	Subscriber's department or section for which the certificate is issued	No	
	6.5 Serial Number	Subscriber's Tax ID number	Yes	
	6.6 Common Name	Name of component	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.		Yes
	10.1 Digital Signature	1	Yes	
	10.2 Content Commitment	0	No	

	10.3 Key Encipherment		1	Yes	
	10.4 Data Encipherment		1	Yes	
	10.5 Key Agreement		0	Yes	
	10.6 Key Certificate Signature		0	Yes	
	10.7 CRL Signature		0	Yes	
11. Extended Key Usage			Improved or extended use of keys	No	No
	11.1 Email protection		1.3.6.1.5.5.7.3.4	No	
	11.2 Client Authentication		1.3.6.1.5.5.7.3.2	No	
	11.3 AnyExtendedKeyUsage		2.5.29.37.0	No	
12. Certificate Policies			Certification policy	Yes	No
	12.1 Policy Identifier		1.3.6.1.4.1.5734.3.9.2	Yes	
	12.2 Policy Qualifier Id			Yes	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names					
	13.1 Name of component		Id Field / Value: 1.3.6.1.4.1.5734.1.8 = <Name of component>	Yes	
14. CRL Distribution Point			Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1		CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU=AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Yes	
	14.2 Distribution Point 2		CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority				Yes	No

Info Access				
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension identifies if the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.3 PF code signature component

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha56withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 Given Name	Name of subscriber for which the certificate is issued	Yes	
	6.3 Surname	Surname of subscriber for which the certificate is issued	Yes	
	6.4 Serial Number	Tax ID number of subscriber for which the certificate is issued	Yes	
	6.5 Common Name	Name of component	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of Component public key	Yes	
10. Key Usage		Use of certified keys allowed.	Yes	Yes
	10.1 Digital Signature	1		
	10.2 Content Commitment	0		
	10.3 Key Encipherment	0		

	10.4 Data Encipherment		0		
	10.5 Key Agreement		0		
	10.6 Key Certificate Signature		0		
	10.7 CRL Signature		0		
11. Extended Key Usage			Improved or extended use of keys	Yes	No
	11.1 Code signing		1.3.6.1.5.5.7.3.3	Yes	
12. Certificate Policies			Certification policy	Yes	No
	12.1 Policy Identifier		1.3.6.1.4.1.5734.3.9.3	Yes	
	12.2 Policy Qualifier Id			Yes	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names					No
	13.1 Subscriber's name		Id Field / Value: 1.3.6.1.4.1.5734.1.1 = <Name>	Yes	
	13.2 Subscriber's first surname		Id Field / Value: 1.3.6.1.4.1.5734.1.2 = <First surname>	Yes	
	13.3 Subscriber's second surname		Id Field / Value: 1.3.6.1.4.1.5734.1.3 = <Second surname>	No	
	13.4 Subscriber's Tax ID number		Subscriber's identification unique number (Tax ID number) Id Field / Value: 1.3.6.1.4.1.5734.1.4 = <Tax ID Number>	Yes	
	13.5 Name of component		Id Field / Value: 1.3.6.1.4.1.5734.1.8 = <Name of component>	Yes	
14. CRL Distribution Point			Information about how information is obtained from the CRL associated with the certificate	Yes	No

	14.1 Distribution Point 1	CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU= AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings”.	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.4 PJ code signature component

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 LocalityName	Name of subscriber's locality	Yes	
	6.3 Organization	Subscriber' name	Yes	
	6.4 Organizational Unit	Subscriber's department or section for which the certificate is issued	No	
	6.5 Serial Number	Subscriber's Tax ID number	Yes	
	6.6 Common Name	Name of component	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.	Yes	Yes
	10.1 Digital Signature	1		
	10.2 Content Commitment	0		

	10.3 Key Encipherment	0		
	10.4 Data Encipherment	0		
	10.5 Key Agreement	0		
	10.6 Key Certificate Signature	0		
	10.7 CRL Signature	0		
11. Extended Key Usage		Improved or extended use of keys	Yes	No
	11.1 Code signing	1.3.6.1.5.5.7.3.3	Yes	
12. Certificate Policies		Certification policy	Yes	No
	12.1 Policy Identifier	1.3.6.1.4.1.5734.3.9.4	Yes	
	12.2 Policy Qualifier Id		Yes	
	12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names				No
	13.1 Name of component	Id Field / Value: 1.3.6.1.4.1.5734.1.8 = <Name of component>	Yes	
14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1	CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU= AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information:	Yes	

		1.3.6.1.5.5.7.48.1 (ocsp)		
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.5 PF Standard SSL

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 Given Name	Name of subscriber for which the certificate is issued	Yes	
	6.3 Surname	Surname of subscriber for which the certificate is issued	Yes	
	6.4 Serial Number	Tax ID number of subscriber for which the certificate is issued	Yes	
	6.5 Common Name	Domain for which the certificate is issued	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.	Yes	Yes
	10.1 Digital Signature	1		
	10.2 Content Commitment	0		
	10.3 Key Encipherment	1		

	10.4 Data Encipherment	0		
	10.5 Key Agreement	0		
	10.6 Key Certificate Signature	0		
	10.7 CRL Signature	0		
11. Extended Key Usage		Improved or extended use of keys	Yes	No
	11.1 Server Authentication	1.3.6.1.5.5.7.3.1	Yes	
12. Certificate Policies		Certification policy	Yes	No
	12.1 Policy Identifier	1.3.6.1.4.1.5734.3.9.5	Yes	
	12.2 Policy Qualifier Id		Yes	
	12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names				No
	13.1 Subscriber's name	Id Field / Value: 1.3.6.1.4.1.5734.1.1 = <Name>	Yes	
	13.2 Subscriber's first surname	Id Field / Value: 1.3.6.1.4.1.5734.1.2 = <First surname>	Yes	
	13.3 Subscriber's second surname	Id Field / Value: 1.3.6.1.4.1.5734.1.3 = <Second surname>	No	
	13.4 Subscriber's Tax ID number	Subscriber's identification unique number (Tax ID number) Id Field / Value: 1.3.6.1.4.1.5734.1.4 = <Tax ID Number>	Yes	
	13.5 DNSName	Id Field / Value: DNSName = <Domain>	Yes	
14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No

M.ª TERESA DE LA CUESTA BERNÁLDEZ
TRADUCTORA E INTÉRPRETE DE INGLÉS
C/ BAHÍA DE MAHÓN, 14 - AT. DCHA.
28042 MADRID - TEL. 656 433 628

	14.1 Distribution Point 1	CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU=AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.6 PJ Standard SSL

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 LocalityName	Name of subscriber's locality	Yes	
	6.3 Organization	Subscriber' name	Yes	
	6.4 Organizational Unit	Subscriber's department or section for which the certificate is issued	No	
	6.5 Serial Number	Subscriber's Tax ID number	Yes	
	6.6 Common Name	Domain for which certificate is issued	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.	Yes	Yes
	10.1 Digital Signature	1		
	10.2 Content Commitment	0		

	10.3 Key Encipherment		1		
	10.4 Data Encipherment		0		
	10.5 Key Agreement		0		
	10.6 Key Certificate Signature		0		
	10.7 CRL Signature		0		
11. Extended Key Usage			Improved or extended use of keys	Yes	No
	11.1 Server Authentication		1.3.6.1.5.5.7.3.1	Yes	
12. Certificate Policies			Certification policy	Yes	No
	12.1 Policy Identifier		1.3.6.1.4.1.5734.3.9.6	Yes	
	12.2 Policy Qualifier Id			Yes	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names					No
	13.1 DNSName		Id Field / Value: DNSName = <Domain>	Yes	
14. CRL Distribution Point			Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1		CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU=AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)	Yes	
	14.2 Distribution Point 2		CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access				Yes	No
	15.1 Access Method 1		Identifier of method to access revocation information:	Yes	

		1.3.6.1.5.5.7.48.1 (ocsp)		
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.7 PF Wildcard SSL

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 Given Name	Name of subscriber for which the certificate is issued	Yes	
	6.3 Surname	Surname of subscriber for which the certificate is issued	Yes	
	6.4 Serial Number	Tax ID number of subscriber for which the certificate	Yes	

			is issued		
	6.5 Common Name		Wildcard domain for which the certificate is issued	Yes	
7. Authority Key Identifier			Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info			Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier			Identifier of component public key	Yes	
10. Key Usage			Use of certified keys allowed.	Yes	Yes
	10.1 Digital Signature		1		
	10.2 Content Commitment		0		
	10.3 Key Encipherment		1		
	10.4 Data Encipherment		0		
	10.5 Key Agreement		0		
	10.6 Key Certificate Signature		0		
	10.7 CRL Signature		0		
11. Extended Key Usage			Improved or extended use of keys	Yes	No
	11.1 Server Authentication		1.3.6.1.5.5.7.3.1	Yes	
12. Certificate Policies			Certification policy	Yes	No
	12.1 Policy Identifier		1.3.6.1.4.1.5734.3.9.7	Yes	
	12.2 Policy Qualifier Id			Yes	
		12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names					No
	13.1 Subscriber's name		Id Field / Value: 1.3.6.1.4.1.5734.1.1 = <Name>	Yes	
	13.2 Subscriber's first		Id Field / Value:	Yes	

	surname	1.3.6.1.4.1.5734.1.2 = <First surname>		
	13.3 Subscriber's second surname	Id Field / Value: 1.3.6.1.4.1.5734.1.3 = <Second surname>	No	
	13.4 Subscriber's Tax ID number	Subscriber's identification unique number (Tax ID number) Id Field / Value: 1.3.6.1.4.1.5734.1.4 = <Tax ID Number>	Yes	
	13.5 DNSName	Id Field / Value: DNSName = <Wildcard domain>	Yes	
14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1	CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU= AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.8 PJ Wildcard SSL

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 LocalityName	Name of subscriber's locality	Yes	
	6.3 Organization	Subscriber' name	Yes	
	6.4 Organizational Unit	Subscriber's department or section for which the certificate is issued	No	
	6.5 Serial Number	Subscriber's Tax ID number	Yes	
	6.6 Common Name	Wildcard domain for which certificate is issued	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.	Yes	Yes
	10.1 Digital Signature	1		
	10.2 Content Commitment	0		

	10.3 Key Encipherment	1		
	10.4 Data Encipherment	0		
	10.5 Key Agreement	0		
	10.6 Key Certificate Signature	0		
	10.7 CRL Signature	0		
11. Extended Key Usage		Improved or extended use of keys	Yes	No
	11.1 Server Authentication	1.3.6.1.5.5.7.3.1	Yes	
12. Certificate Policies		Certification policy	Yes	No
	12.1 Policy Identifier	1.3.6.1.4.1.5734.3.9.8	Yes	
	12.2 Policy Qualifier Id		Yes	
	12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names				No
	13.1 DNSName	Id Field / Value: DNSName = <Wildcard domain>	Yes	
14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1	CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU= AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information:	Yes	

		1.3.6.1.5.5.7.48.1 (ocsp)		
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

M.ª TERESA DE LA CUESTA BERMÚDEZ
TRADUCTORA E INTÉRPRETE DE INGLÉS
C/ BAHÍA DE MAHÓN, 14 - AT. DCHA.
28042 MADRID - TEL. 656 433 628

7.2.9 PF Plus SSL

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 Given Name	Name of subscriber for which the certificate is issued	Yes	
	6.3 Surname	Surname of subscriber for which the certificate is issued	Yes	
	6.4 Serial Number	Tax ID number of subscriber for which the certificate is issued	Yes	
	6.5 Common Name	Domain for which the certificate is issued	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.		Yes
	10.1 Digital Signature	1		
	10.2 Content Commitment	0	No	
	10.3 Key Encipherment	1	Yes	

	10.4 Data Encipherment	0	Yes	
	10.5 Key Agreement	0	Yes	
	10.6 Key Certificate Signature	0	Yes	
	10.7 CRL Signature	0	Yes	
11. Extended Key Usage		Improved or extended use of keys	Yes	No
	11.1 Server Authentication	1.3.6.1.5.5.7.3.1	Yes	
	11.2 Email protection	1.3.6.1.5.5.7.3.4	No	
	11.3 Client Authentication	1.3.6.1.5.5.7.3.2	No	
12. Certificate Policies		Certification policy	Yes	No
	12.1 Policy Identifier	1.3.6.1.4.1.5734.3.9.9	Yes	
	12.2 Policy Qualifier Id		Yes	
	12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names				No
	13.1 Subscriber's name	Id Field / Value: 1.3.6.1.4.1.5734.1.1 = <Name>	Yes	
	13.2 Subscriber's first surname	Id Field / Value: 1.3.6.1.4.1.5734.1.2 = <First surname>	Yes	
	13.3 Subscriber's second surname	Id Field / Value: 1.3.6.1.4.1.5734.1.3 = <Second surname>	No	
	13.4 Subscriber's Tax ID number	Subscriber's identification unique number (Tax ID number) Id Field / Value: 1.3.6.1.4.1.5734.1.4 = <Tax ID Number>	Yes	
	13.5 DNSName	Id Field / Value: DNSName = Domain	Yes	

14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1	CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU= AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.10 PJ Plus SSL

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 LocalityName	Name of subscriber's locality	Yes	
	6.3 Organization	Subscriber' name	Yes	
	6.4 Organizational Unit	Subscriber's department or section for which the certificate is issued	No	
	6.5 Serial Number	Subscriber's Tax ID number	Yes	
	6.6 Common Name	Domain for which the certificate is issued	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.		Yes
	10.1 Digital Signature	1	Yes	
	10.2 Content Commitment	0	No	

	10.3 Key Encipherment	1	Yes	
	10.4 Data Encipherment	0	Yes	
	10.5 Key Agreement	0	Yes	
	10.6 Key Certificate Signature	0	Yes	
	10.7 CRL Signature	0	Yes	
11. Extended Key Usage		Improved or extended use of keys	Yes	No
	11.1 Server Authentication	1.3.6.1.5.5.7.3.1	Yes	
	11.2 Email Protection	1.3.6.1.5.5.7.3.4	No	
	11.3 Client Authentication	1.3.6.1.5.5.7.3.2	No	
12. Certificate Policies		Certification policy	Yes	No
	12.1 Policy Identifier	1.3.6.1.4.1.5734.3.9.10	Yes	
	12.2 Policy Qualifier Id		Yes	
	12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names				No
	13.1 DNSName	Id Field / Value: DNSName = Domain	Yes	
14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1	CRL 1 publication point Idap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU=AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	

15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.11 PF multi-domain SSL (SAN / UCC)

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 Given Name	Name of subscriber for which the certificate is issued	Yes	
	6.3 Surname	Surname of subscriber for which the certificate is issued	Yes	
	6.4 Serial Number	Tax ID number of subscriber for which the certificate is issued	Yes	
	6.5 Common Name	Main domain for which the certificate is issued	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.	No	Yes
	10.1 Digital Signature	1	Yes	
	10.2 Content Commitment	0	No	
	10.3 Key Encipherment	1	Yes	

	10.4 Data Encipherment	0	Yes	
	10.5 Key Agreement	0	Yes	
	10.6 Key Certificate Signature	0	Yes	
	10.7 CRL Signature	0	Yes	
11. Extended Key Usage		Improved or extended use of keys	Yes	No
	11.1 Server Authentication	1.3.6.1.5.5.7.3.1	Yes	
	11.2 Email protection	1.3.6.1.5.5.7.3.4	No	
	11.3 Client Authentication	1.3.6.1.5.5.7.3.2	No	
12. Certificate Policies		Certification policy	Yes	No
	12.1 Policy Identifier	1.3.6.1.4.1.5734.3.9.11	Yes	
	12.2 Policy Qualifier Id		Yes	
	12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names				No
	13.1 Subscriber's name	Id Field / Value: 1.3.6.1.4.1.5734.1.1 = <Name>	Yes	
	13.2 Subscriber's first surname	Id Field / Value: 1.3.6.1.4.1.5734.1.2 = <First surname>	Yes	
	13.3 Subscriber's second surname	Id Field / Value: 1.3.6.1.4.1.5734.1.3 = <Second surname>	No	
	13.4 Subscriber's Tax ID number	Subscriber's identification unique number (Tax ID number) Id Field / Value: 1.3.6.1.4.1.5734.1.4 = <Tax ID Number>	Yes	
	13.5 DNSName	Id Field / Value: DNSName = Domain	Yes	

	13.6 DNSName	Id Field / Value: DNSName = Domain_2	Yes	
	13.7 DNSName	Id Field / Value: DNSName = Domain_*n*	No	
14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1	CRL 1 publication point ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>OU=AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)	Yes	
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum "depth" level permitted for certification strings".	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

7.2.12 PJ multi-domain SSL (SAN / UCC)

Field		Content	Compulsory	Criticality
1. Version		2	Yes	
2. Serial number		Unique identification number of certificate	Yes	
3. Signature Algorithm		Sha256withRsaEncryption	Yes	
4. Issuer Distinguish Name		Certificate issuing entity (Subordinate CA)	Yes	
	4.1 Country	C=ES	Yes	
	4.2 Organization	Name (organization's "official" name) of the certification services provider (certificate issuer) O=FNMT-RCM	Yes	
	4.3 Organization Unit	OU=AC Software components	Yes	
5. Validity		Variable	Yes	
6. Subject		Identification/description of subscriber's certificate and component	Yes	
	6.1 Country	C=ES	Yes	
	6.2 LocalityName	Name of subscriber's locality	Yes	
	6.3 Organization	Subscriber' name	Yes	
	6.4 Organizational Unit	Subscriber's department or section for which the certificate is issued	No	
	6.5 Serial Number	Subscriber's Tax ID number	Yes	
	6.6 Common Name	Main domain for which the certificate is issued	Yes	
7. Authority Key Identifier		Identifier of public key of the Component CA. Means to identify the public key matching the private key used by the CA to sign the component certificate.	Yes	
8. Subject Public Key Info		Component public key, encoded according to RSA PKCS#1 standard. The length of the key will be 2048 bits.	Yes	
9. Subject Key Identifier		Identifier of component public key	Yes	
10. Key Usage		Use of certified keys allowed.	No	Yes
	10.1 Digital Signature	1	Yes	
	10.2 Content Commitment	0	No	

	10.3 Key Encipherment	1	Yes	
	10.4 Data Encipherment	0	Yes	
	10.5 Key Agreement	0	Yes	
	10.6 Key Certificate Signature	0	Yes	
	10.7 CRL Signature	0	Yes	
11. Extended Key Usage		Improved or extended use of keys	Yes	No
	11.1 Server Authentication	1.3.6.1.5.5.7.3.1	Yes	
	11.2 Email Protection	1.3.6.1.5.5.7.3.4	No	
	11.3 Client Authentication	1.3.6.1.5.5.7.3.2	No	
12. Certificate Policies		Certification policy	Yes	No
	12.1 Policy Identifier	1.3.6.1.4.1.5734.3.9.12	Yes	
	12.2 Policy Qualifier Id		Yes	
	12.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Yes	
13. Subject Alternative Names				No
	13.1 DNSName	Id Field / Value: DNSName = Domain	Yes	
	13.2 DNSName	Id Field / Value: DNSName = Domain_2	Yes	
	13.3 DNSName	Id Field / Value: DNSName = Domain_*n*	No	
14. CRL Distribution Point		Information about how information is obtained from the CRL associated with the certificate	Yes	No
	14.1 Distribution Point 1	CRL 1 publication point Idap://Idapcomp.cert.fnmt.es/CN=CRL<xxx*>OU=AC%20Componentes%20informaticos, O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?	Yes	

		objectclass=cRLDistributionPoint *xxx: CRL identifier integer (partitioned CRL)		
	14.2 Distribution Point 2	CRL2 publication point http://www.cert.fnmt.es/crlscomp/CRLnnn.crl	Yes	
15. Authority Info Access			Yes	No
	15.1 Access Method 1	Identifier of method to access revocation information: 1.3.6.1.5.5.7.48.1 (ocsp)	Yes	
	15.2 Access Location 1	http://ocpscomp.cert.fnmt.es/ocps/OcspResponder	Yes	
	15.3 Access Method 2	Identifier of method to access information on additional certificates necessary for validation: 1.3.6.1.5.5.7.48.2 (ca cert)	Yes	
	15.4 Access Location 2	http://www.cert.fnmt.es/certs/ACCOMP.crt	Yes	
16. Basic Constraints		This extension helps identify whether the certification subject is a CA as well as the maximum “depth” level permitted for certification strings”.	Yes	No
	16.1 Subject Type	Value FALSE (end entity)		

Translator's note:
- This translated document is comprised of 59 sheets of paper, printed on one side only. All the front pages bear this translator's signature by way of endorsement.
- The original Spanish document this translator was asked to translate contains terms and expressions already written in English and they have been kept as such in the translated text above.
- In addition, this translator was sent a document in English for reference as to terms and expressions and, following the client's instructions, quite a number of the terms and expressions that appear in the translated text above are those appearing in the document sent for reference.

CERTIFICATION: Ms. M. Teresa de la Cuesta Bernaldez, Sworn English Interpreter, certifies that the foregoing is a truthful and complete translation into English of a document written in Spanish. Madrid, 19 March 2014.

CERTIFICACION: Dña. M. Teresa de la Cuesta Bernaldez, intérprete jurado de inglés, certifica que la que antecede es traducción fiel y completa al inglés de un documento redactado en español. En Madrid, a 19 de marzo, 2014.

Mª TERESA DE LA CUESTA BERNÁLDEZ
TRADUCTORA E INTÉRPRETE DE INGLÉS
C/ BAHÍA DE MAHÓN, 14 - AT. DCHA.
28042 MADRID - TEL. 656 433 628