Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

TIME-STAMPING SERVICE
POLICIES AND PRACTICES STATEMENT

	NAME	DATE
Prepared by:	FNMT-RCM / 2.2	04/03/2015
Revised by:	FNMT-RCM / 2.2	04/03/2015
Approved by:	FNMT-RCM / 2.2	04/03/2015

BACKGROUND OF THE DOCUMENT			
Version	**Date**	**Description**	**Author**
1.1	01/05/2003	Creation of the document.	FNMT-RCM
2.0	07/12/2009	Statement updated due to adaptation of the service to ETSI 102 023.	FNMT-RCM
2.1	19/12/2011	Increase in accepted algorithms for summary of the information received by the service. Change in the certificates employed in issuing time stamps under the time-stamp policy AC AP FNMT-RCM. Inclusion of information on a new TSU.	FNMT-RCM
2.2	04/03/2015	The number of Time Stamping Units (TSU) has been reduced to one. Algorithms RSA 3072 and accessing URLs have been updated	FNMT-RCM

Reference: DPST/DPST0202/SGPSC/2015

Document classified as: *Public*

TABLE OF CONTENTS

INDEX OF TABLES

1. REFERENCES

[GCPS] – General Certification Practices Statement (http://www.cert.fnmt.es/dpcs/)

[ETSI TS 102 042] – ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates.

[ETSI TS 101 456] – ETSI TS 101 456 Policy requirement for certification authorities issuing qualified certificates.

[ETSI TS 102 023] – ETSI TS 102 023 Policy requirement for time-stamping authorities, and

[ETSI TS 101 861] – ETSI TS 101 861 Time-stamping profile.

[ETSI TS 102 176] – ETSI TS 102 176 Algorithms and parameters for secure electronic signatures.

[RFC 3628] – RFC 3628 Policy requirements for time-stamping authorities (TSAs)

[RFC 3161] – RFC 3161 Internet X.509 public key infrastructure – Time stamp protocol (TSP)

2. ACRONYMS AND DEFINITIONS

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

- *Trust service provider:* A natural or a legal person who provides one or more trust services in compliance with 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

(the terms in italics are described either in the present document or in the General Certification Practices Statement)

3. INTRODUCTION AND OBJECTIVE

2. The Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (Royal Spanish Mint), (hereinafter referred to as "FNMT-RCM"), provides *Time-stamping* services aimed at establishing evidence of the existence of a set of data at a specific moment in the timeline. To do this, the FNMT-RCM uses the time reference provided by the Time Section of the Royal Institute and Observatory of the Spanish Navy in San Fernando, whose main mission is the maintenance of the basic unit of time, officially recognised as the National Standard of this unit, and the maintenance and official dissemination of the Coordinated Universal Time scale (UTC-ROA), which for all purposes is considered the basis of the official time in the entire Spanish territory (Royal Decree 1308/1992 of 23 October 1992).

3. The guarantees offered by the FNMT-RCM with this type of services are based on the certification, through electronic signature techniques, of a representation of the set of data of which it provides evidence. Thus, to provide the service the FNMT-RCM requires a prior

request from the time-stamp requestor (the representation of the set of data is sent), to which it replies with the corresponding electronic document (time stamp).

4. This document is considered to be an appendix to the GCPS and constitutes the *Time-stamp Policies and Time-stamping Practices Statement* (hereinafter referred to as "TSP" and "TSPS", respectively, of the FNMT-RCM, in its activity as Certification Service Provider (TSP), and covers the totality of operating policies and practices employed in the issuing of "electronic dating" or "time stamps" to guarantee that the service that generates them complies with the obligatory security, availability, and functionality requirements.

5. This is a declarative document which describes the most relevant aspects of the *Time-stamping Service* and the procedures employed and/or devised to manage and use the service. A self-declaration is also provided on the infrastructure safeguard measures and the technical and non-technical security controls applied to the systems involved in the provision of the service.

6. On another front, the TSP and the TSPS represent the totality of the conditions of use, the liability and obligations of the parties and the restrictions of the *Time-stamping Service,* which are applicable in the context of the *Electronic Community* upon signing the pertinent use agreements.

7. In short, the objective of this document is to provide public information on the conditions and characteristics of the *Time-stamping Service* of the FNMT-RCM as CSP, covering, in particular, the obligations that it undertakes to meet in managing the *Signature Creation and Verification Data*, the *Certificates* employed in offering the service, and the conditions applicable to the request, issuing, use and extinction of validity of the *Time Stamps*.

8. This document also covers the rights and obligations of all the parties relying on and accepting the service.

9. Considering that the provision of the *Time-stamping Service* is framed within the *Certification Services* of the FNMT-RCM, the sections of the GCPS concerning the system of liability applicable to the members of the *Electronic Community* and third parties relying on said services, the security controls applied in its procedures and installations, personal data protection and other aspects of an informative nature relating to the *Time Stamp* are applicable.

10. Thus, we consider the *Time-stamping Practices Statement* of any of the *Time-stamp Policies* described in this document to be the totality of the GCPS as a whole plus the relevant sections of this document.

4. ORDER OF PREVALENCE

11. The FNMT-RCM offers time-stamping services in the framework of its activity as *Certification Services Provider* and through the respective time-stamping units (TSU).

12. Consequently, the FNMT-RCM is established as a *Time-stamping Authority* (TSA) and, in order to guarantee the features of the service, reserves the right to establish as many time-stamping units (TSU) as it considers appropriate and manage them in accordance with the specific and differentiated policies and practices.

13. Within this scope of action, the following order of prevalence is established (in descending order) for the statements documentation of the *Time-stamping Service*:

    1) Should there be specific conditions or *Issuance Laws* applicable to specific time-stamping units, these would be unequivocally identified in this document with their specific policies and practices, and would prevail over the general terms of the *Time-Stamping Service*.

2) *This Time-stamp Policies and Practices Statement,* which is applicable to the provision of the *Time-stamping Service* and is set out over the entire length of this document, shall prevail over the general conditions on the provision of certification services by the FNMT-RCM established in the GCPS.

3) The GCPS, which generally affects any certification service provided by the FNMT-RCM, and shall be applied in addition to the documents referred to in points 1 and 2 above.

5. AVAILABILITY OF INFORMATION AND COMMUNICATIONS

14. See [GCPS].

6. SECURITY CONTROLS, REGISTRY OF EVENTS AND AUDITS

See [GCPS].

7. TIME SOURCE EMPLOYED IN THE PROVISION OF THE SERVICE AND VALIDITY PERIOD OF TIME STAMPS

16. The purpose of the Synchronism System with the Royal Observatory of the Spanish Navy (SS-ROA) installed in the Data Processing Centre (DPC) of the FNMT-RCM is to provide a source of time reference traceable to the UTC (ROA) time scale to the Time-Stamping Service of the FNMT-RCM.

17. The SS-ROA is mainly made up of a Rubidium frequency standard (Symmetricom Rubidium Frequency Standard 8040), a time and frequency comparison system via a satellite navigation system (GPS Symmetricom SyncServer S200 and Dicom Time&Frequency Transfer Receiver GTR50) and two External Synchronism Central Units mod. STF701.

18. This equipment as a whole generates a series of files containing the data on the monitoring carried out in one day, and the ROA uses this data to draw up the reports on the phase difference between the standard and the UTC (ROA) scale.

19. The date and time reference to the network is supplied by the STF701 External Synchronism Central Units through an NTP service. The time reference is supplied via a signal from the Symmetricom Rubidium Frequency Standard 8040.

20. The period during which the FNMT-RCM considers that the *Time Stamps* it issues are valid is determined by the algorithms employed or by technical or legal regulations which may apply. To determine the exact period of a specific Time Stamp issued under one of the policies identified in this document, please consult ETSI TS 102 176.

8. CESSATION OF THE ACTIVITY OF THE FNMT-RCM AS TIME-STAMPING AUTHORITY

21. See [GCPS].

9. INTELLECTUAL AND INDUSTRIAL PROPERTY

22. See [GCPS].

10. PROHIBITION ON RESERVICE WITH OR WITHOUT RESALE

23. The time-stamping services performed by the FNMT-RCM, may not be subject to re-service, with or without resale, with no added value to them. In case that the added value is provided to third parties based on validation services provided by the FNMT-RCM, this entity should be asked to sign a contract for the wholesale segment.

24. FNMT-RCM is exempted from liability for actions of persons, entities or organizations without entering into a contract for the wholesale segment, proceed to perform these services for other parties. This is without prejudice to any legal action that may be appropriate.

11. APPLICABLE LAW, INTERPRETATION AND COMPETENT JURISDICTION

25. See [GCPS].

12. MODIFICATION OF THE TSP AND TSPS

26. See [GCPS].

13. FNMT TIME-STAMP POLICY

13.1. IDENTIFICATION

27. This *Time-stamp Policy* of the FNMT-RCM for the issuing of *Time Stamps* has the following identification:

Table 1 – FNMT Time-stamp Policy Identification

Name	FNMT *Time-stamp Policy*
Reference/OID	1.3.6.1.4.1.5734.3.1.3.
Version	2.1
Location	http://www.cert.fnmt.es/dpcs/
Associated CPS	General Certification Practices Statement of the FNMT-RCM
Location	http://www.cert.fnmt.es/dpcs/

28. This policy is applicable to the different time-stamping units (TSU) that may be established by the FNMT-RCM to provide the service.

29. It is identified and referenced with the *OID* 1.3.6.1.4.1.5734.3.1.1 and the latest version in force can be found at the following address:

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

30. The procedures and contents referenced here are mainly based on the standards of the *European Telecommunications Standards Institute* (ETSI):

- ETSI TS 102 042 - Policy requirements for certification authorities issuing public key certificates,
- ETSI TS 101 456 - Policy requirements for certification authorities issuing qualified certificates,
- ETSI TS 102 023 - Policy requirements for time-stamping authorities, and
- ETSI TS 101 861- Time-stamping profile.

31. This policy is in keeping with standard ETSI TS 102 023 and with the equivalent specifications of the IETF - RFC 3628 Policy requirements for time-stamping authorities (TSAs).

13.2. COMMUNITY AND SCOPE OF APPLICATION

32. This policy is applicable to the issuing of *Time Stamps* with the following characteristics:

- They are issued by the FNMT-RCM as CSP in compliance with the criteria established in the EESSI technical standards, specifically ETSI TS 102 023.
- They are issued based on the criteria established for them in the EESSI technical standards ETSI TS 101 861 and RFC 3161.
- They are signed electronically with the *Certificates* and *Signature Creation Data* of the FNMT-RCM, specifically under the *Certification Chain* of the *Certification Authority* CN=FNMT-RCM ROOT CA.
- They expressly include data on adhesion to this policy through the "policy" field of the *Time Stamp* itself.
- They are issued on request of *User Entities* which are part of the *Electronic Community*, as defined in the ***Definitions*** section of the GCPS.

13.3. USE RESTRICTION OF THE TIME-STAMPING SERVICE AND TIME STAMPS

33. To be able to use the service adequately one must previously be part of the *Electronic Community,* acquire the status of *User Entity,* and have signed the respective service use agreement. Only within this framework will the *User Entity* be able to obtain the instructions and privileges needed to send data electronically to the FNMT-RCM for a time stamp to be created with that data.

34. On another front, to enable a third party to have confidence in the time stamps issued by the FNMT-RCM, there is an Information and consultation service on the state of validity of the certificates where consult the state of the Certificate used to construct the time stamp in question.

35. Therefore, before having made the pertinent verifications, one should not trust a *Time Stamp* issued under this *Time-stamp Policy* of the FNMT-RCM. In such a case, no cover shall be given under this policy and there shall be no entitlement to claim or take legal action against the FNMT-RCM for damage, loss or disputes arising from the use of or trust in a *Certificate.*

36. The FNMT-RCM does not guarantee the veracity of the contents represented by the electronic data being time-stamped or their authorship. Furthermore, the FNMT-RCM does not endorse them or participates in their creation in any way, and is not responsible for the use which may be made of them or for the effects that the latter may have on interested and/or third parties. The FNMT-RCM is not associated in any way with the origin or causality of this electronic data.

37. The FNMT-RCM, through its *Time-stamping Service*, only guarantees the existence of the data being time-stamped, which could well be a particular representation of other data, at the moment in time in which it receives the request, which is determined by the time reference employed. This guarantee is expressed through the joint electronic signature of that data and that time reference with a *Certificate* whose holder is the FNMT-RCM, the provider of the *Time-stamping Service,* whose role in the service is that of *Time-stamping Authority* and trusted third party. The FNMT-RCM rejects any interpretation of the guarantees offered by the time stamps that it issues beyond that expressed above. The *Time-stamping Authority*, which is the FNMT-RCM, is therefore a trusted third party without any particular interest in the documents being time-stamped, although its signature will be proof of their existence at a given moment in time.

13.4. LIABILITY AND OBLIGATIONS OF THE PARTIES

38. This *Time-stamp policy* covers the liability and obligations of the parties involved in the provision of the *Time-stamping Service* and in the issuing and use of the *Time Stamps*.

13.4.1. Liability of the parties

39. To be able to request the issuing of *Time Stamps*, one must previously be part of the *Electronic Community* and acquire the status of *User Entity*.

40.

13.4.1.1. Liability of the Certification Services Provider (FNMT-RCM)

41. The FNMT-RCM shall only be liable for variations in the time reference from to the reference provided by the Time Section of the Royal Institute and Observatory of the Spanish Navy in San Fernando, Cadiz, which is introduced into the time stamps at the time of the request, but not for the data attached to the time reference which appear in the issued time stamp itself or for the consequences derived from their use by a third party.

42. The FNMT-RCM shall not be liable for the veracity or the contents represented by the electronic data being time-stamped.

43. The FNMT-RCM shall not be liable for any damage or losses and/or defective functioning caused by the use of the *Time Stamps* that it issues, whether due to the fault of the interested parties or defects of origin in the elements.

44. The FNMT-RCM shall not be liable to persons whose conduct in the use of the Time-Stamping service and/or the Time Stamps themselves has been negligent. For this purpose, negligence shall be understood as failure to observe that established in this Time-stamping Policy and Practices Statement, in the GCPS and, in particular, in the sections on the obligations and liability of the parties.

45. The FNMT-RCM shall not be liable in cases of acts of God, force majeure, terrorist attacks, wild strikes and actions which constitute a crime or an offense and affect the provider's

infrastructure, unless there has been serious negligence on the part of the institution. In any case, in the respective contracts and/or agreement, the FNMT may establish additional liability limitation clauses to the ones contained in this document.

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

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

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

13.4.1.2. Liability of the User Entities of the service

49. Unless otherwise arranged with the FNMT-RCM, it is the *User Entity's* responsibility to verify the *Electronic Signatures* employed in issuing the *Time Stamps* and to check the state of the *Certificates* in the confidence chain, and under no circumstances shall the authenticity of the *Stamps* or *Certificates* be assumed without having made these verifications.

50. It is the responsibility of the *Requestor* and holder of the *Time Stamps* to re-sign or re-stamp the data object of the *Time Stamp* should the algorithm employed in issuing the *Time Stamp* become obsolete, thus invalidating its evidential and truthful nature.

51. The *Requestor* and receiver of the *Time Stamp* (*User Entities*) shall be liable to the relying parties for the data object of the time reference included in the *Time Stamp* and for the repercussions of its use by a third party.

52. Furthermore, the *User Entity* shall be responsible for observing that established in the applicable *Time-stamping Policies and Practices*, the GCPS and any possible future amendments to it, with particular attention to the use restrictions established for the *Time Stamps* in their respective policies.

13.4.1.3. Liability of the relying parties

53. Unless otherwise arranged with the FNMT-RCM, it is the *Relying Parties'* responsibility to verify the *Electronic Signatures* employed in issuing the *Time Stamps* and the *Certificates* in the confidence chain, and under no circumstances shall the authenticity of the *Stamps* or *Certificates* be assumed without having made these verifications.

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

55. If the circumstances point to the need for additional guarantees, the *Relying Party* should obtain additional guarantees to ensure that that trust is reasonable.

13.4.2. Obligations of the parties

13.4.2.1. Obligations of the Certification Services Provider (FNMT-RCM)

56. The FNMT-RCM, as *Time-stamping Service Provider* and established *Time-Stamping Authority* through this service, is required to:

- On a general basis, follow the procedures and guidelines set out in this policy and practices statement for the issuing of *Time Stamps* and in the GCPS.

- Maintain and calibrate the time reference employed in issuing *Time Stamps* with a maximum deviation of 50 ns from the time reference provided by the Time Section of the Royal Institute and Observatory of the Spanish Navy in San Fernando, Cadiz.

- Include in the *Time Stamps* that it issues the necessary elements to determine the date and time in which the stamp in question was issued, and the data being time-stamped received by the *User Entity*, without altering or changing them.

- Manage the *Private Keys* employed in issuing the *Time Stamps* and *Certificates* participating in the service in accordance with that established in the "Management of the lifecycle of the *Certification Services Provider's Keys*" section of the GCPS, in such a way that their confidentiality and integrity are ensured.

- Employ a secure signature creation device and a reliable time source as time reference in the *Time Stamp* issuing process.

- Retain all information and documentation relating to the *Time-stamp* requests and the respective replies resulting from the provision of the service for a period of at least fifteen (15) years.

- Make this policy public and freely accessible, and retain the *Time-stamping Policies and Practices* under appropriate security conditions for a period of 15 years after the end of their validity as a result of the publication of a new version.

- Keep a secure and updated *Certificates Directory,* in which the *Certificates* employed in the provision of the service and their validity are identified, including, in the form of *Revocation Lists,* the identification of the *Certificates* which have been revoked or suspended. The integrity of this *Directory* shall be protected by utilising systems in keeping with the specific regulatory provisions adopted in Spain and, as the case may be, in the EU, and access to the *Directory* shall be available as established in the *Specific Certification Policies and Practices* corresponding to the *Certificates* in question.

- Provide a consultation service on the validity of the *Certificates*. This service is provided as described in the GCPS and in the *Specific Certification Policies and Practices* corresponding to the *Certificates* to be validated.

- Should the calibration of the time reference be or be thought to be compromised, duly advise all the parties and provide a description of the situation.

- Refrain from issuing *Time Stamps* should the *Time-stamping service* operations be or be thought to be compromised (keys, loss of calibration of the clock, etc.). In this case, the FNMT-RCM shall make available to the parties and the competent authority the necessary information to identify the affected *Time Stamps*. The FNMT-RCM shall restore the service as soon as the necessary conditions for doing so are re-established.

13.4.2.2. Obligations of the User Entities of the service

57. The parties using the Time-Stamping Service (requests) are required to:

- On a general basis, follow the procedures and guidelines set out in this policy and practices statement for the issuing of *Time Stamps* and in the GCPS.
- Be a member of the *Electronic Community* and an established *User Entity*.
- Have signed the respective service use agreement.
- Identify oneself using an electronic *Certificate* with the pertinent characteristics and in force before requesting any Time Stamping.
- Before placing one's trust in the *Time Stamps*:
  1) Verify that the electronic Signature accompanying the *Time Stamps* is the signature of the FNMT-RCM and not another and that it is correct.
  2) Check the validity of the *Certificates* employed in issuing the *Time Stamp* in question through the procedures indicated in the *Specific Certification Policies and Practices* corresponding to the *Certificates* being validated.
- Use the *Time Stamps* within the limits and scope described in this policy.
- Don't rely on the *Time Stamps* as time reference should the *Certification Services Provider* have ceased its activity as *Time-stamping Authority* which issues stamps under this policy and the subrogation provided for in the law has not taken place. In any event, the *User Entity* shall refrain from using the *Time Stamps* in cases where the *Provider's Signature Creation Data* may be threatened and/or compromised and this has been communicated by the *Provider* or, as the case may be, the circumstance is made known to the *Requestor* or holder of the *Stamp*.
- Don't rely on the *Time Stamps* as time reference beyond the use restrictions established for them in their respective policy.

13.4.2.3. Obligations of the relying parties

58. The parties who rely on a *Time Stamp* issued by the FNMT-RCM are required to:

- On a general basis, follow the procedures and guidelines set out in this policy and practices statement for the issuing of *Time Stamps.*
- Before placing one's trust in the *Time Stamps*:
  1) Verify that the electronic Signature accompanying the *Time Stamps* is the signature of the FNMT-RCM and not another and that it is correct.

2) Check the validity of the *Certificates* employed in issuing the *Time Stamp* in question through the procedures indicated in the *Specific Certification Policies and Practices* corresponding to the *Certificates* being validated.

- Accept the Time Stamps within the limits and scope described in this time-stamping policy and practices statement.

13.5. MANAGEMENT OF THE LIFECYCLE OF THE TRUST SERVICE PROVIDER'S KEYS

59. For the purpose of providing the Time-Stamping Service, the FNMT-RCM carries out the management of the corresponding keys in accordance with that described in the "Management of the lifecycle of the Certification Services Provider's Keys" section of the [GCPS].

60. The *Time Stamps* issued under this policy are signed by specific *Certificates*, which in turn have been issued by the Certification chain of the CN=AC RAIZ FNMT-RCM *Root Certificate* of the *Certification Authority*.

61. For further information on said Root Certificate Authority Certification Chain. please consult the "Certification Chains" section of the [GCPS].

62. The *Signature Creation Data* of the *Time-stamping* unit are associated to the following *Certificate:*

Table 2 – Certificate profile of the first *Time-stamping* unit employed in issuing *Time Stamps* under the present policy

FIELD	**CONTENT**
1. Version	V3
2. Serial Number	26 3F 9B 10 3D FF 0A BB 54 F5 F5 1A A1 20 43 D4
3. Signature algorithm	Sha256withRSAEncryption

4. Issuer Distinguished Name	CN = AC Public Administration
	SERIALNUMBER = Q2826004J
	OU = CERES
	O = FNMT-RCM
	C = ES

5. Validity	From: Tuesday, 3 March 2015 To: Thursday, 3 March 2022

6. Subject	CN = TIME STAMPING AUTHORITY FNMT-RCM
	OU = CERES
	O = FNMT-RCM

	C = ES	
7. Subject Public Key Info	(RSA 3072 bits)	
8. subjectAltName	Directory address: OID.1.3.6.1.4.1.5734.1.8 (fnmtDescription) = TIME STAMPING AUTHORITY FNMT-RCM OID.1.3.6.1.4.1.5734.1.14 (fnmtPropEnt) = FNMT-RCM OID.1.3.6.1.4.1.5734.1.15 (fnmtPropCIF) = Q2826004J	
basicConstrains	Type of issue=End entity Route length restriction=None	
privateKeyUsagePeriod	From: 20090814141133 UTC To: 20120814141133 UTC	
keyUsage	Digital signature, without repudiation	
extKeyUsage	Digital dating	YES
subjectKeyIdentifier	b6 d1 71 c8 6a 21 61 9a 79 74 89 e5 6b 18 bd 59 e9 82 16 81	
authorityKeyIdentifier	14 11 e2 b5 2b b9 8c 98 ad 68 d3 31 54 40 e4 58 5f 03 1b 7d	
crlDistributionPoints	ldap://ldapape.cert.fnmt.es/CN=CRL180,CN=AC%20Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint http://www.cert.fnmt.es/crlsacap/CRL180.crl	

13.6. PROVISION AND AVAILABILITY OF THE TIME-STAMPING SERVICE

63. The issuing of *Time Stamps* is carried out on request of the *User Entity*. Whenever the *User Entity* wishes to obtain a *Time Stamp* for an electronic document, it should calculate a hash

value or set of values based on the document. This generates a small but compact amount of information that is sent to the FNMT-RCM for the corresponding *Time Stamp* to be issued.

64. This *Time Stamp* will bind the data received to the date and time of reception, through the electronic signature of the FNMT-RCM.

65. It is worth highlighting that the FNMT-RCM decides whether the hash algorithm used to represent the document is sufficiently secure in accordance with its service policies and, if it is, it will allow the request to be processed. Specifically, the following hash algorithms are accepted:

- SHA-1,
- SHA-256,
- SHA-384,
- SHA-512

66. The FNMT-RCM will not carry out any verification or processing of the representation of the data received for time-stamping, beyond their inclusion in the *Time Stamp* itself and in the events registration systems. The FNMT-RCM will not verify in any way the content or the veracity of the representation of the data to be time-stamped or their origin.

67. The *Time-stamping service* shall be available twenty-four (24) hours a day, every day of the year, unless due to circumstances outside the control of the FNMT-RCM or maintenance operations. The FNMT-RCM shall communicate the aforementioned circumstances through the address http://www.ceres.fnmt.es at least forty-eight (48) hours in advance, and it shall try to solve the problem within a period of twenty-four (24) hours.

68. Both the *Time-stamp* requests and the replies are managed in accordance with that described in recommendation [RFC 3161].

13.7. TIME-STAMP REQUEST

69. To be able to request a *Time Stamp* one must be part of the *Electronic Community,* hold the status of *User Entity* and have signed the respective service use agreement with the FNMT-RCM.

70. Before making a request, the *User Entity* must obtain a *Component Certificate,* which it will use as an identification and authentication mechanism with each *Time-stamp* request.

71. Using the HTTPS protocol and identifying oneself with the aforementioned *Component Certificate*, the *User Entity* will compose a *Time-stamp* request in accordance with recommendation RFC 3161.

72. The *Time-stamp* requests are sent to the following address: https://tsa.cert.fnmt.es/
encapsulated as Content-Type: application/timestamp-query, encoded in DER and described in ASN.1 (See RFC 3161).

73. The ASN.1 structure corresponding to the request is:

```
TimeStampRequest ::= SEQUENCE {
version Integer { v1 (1) },
messageImprint MessageImprint,
reqPolicy PolicyInformation OPTIONAL,
nonce Integer OPTIONAL,
certReq BOOLEAN DEFAULT FALSE,
extensions [0] IMPLICIT Extensions OPTIONAL
}
```

Version Whole. Describes the version of the request. It is currently version 1.

messageImprint Sequence. Structure containing the hash of the document to be time-stamped and the hash algorithm used.

reqPolicy Identifier of the policy requested to be applied in the provision of the service. It is optional and can be omitted, but if used, it should contain the OID of this policy (1.3.6.1.4.1.5734.3.1.1).

nonce Whole. Random number used to link request to reply.

certReq Boolean. If its value is “True” the TSA is required to include its certificate in the reply.

extensions Sequence. Extensions of the request.

13.8. TIME-STAMP REQUEST REPLY

74. The Digital-Dating requests are received from the following address: https://tsa.cert.fnmt.es/ encapsulated as Content-Type: application/timestamp-query, encoded in DER and described in ASN.1.

75. The content of the reply is an ASN.1 structure, which includes the result of the operation (status), i.e. whether or not the operation has been carried out satisfactorily, and a CMSSignedData (timeStampToken) structure, which includes the digital dating (TSTInfo) signed by the Digital Dating Authority.

76. The certificate of the Digital Dating Authority is a certificate issued by the CA with the extension id-kp-timestamping, which indicates that the certificate will be used for the sole purpose of dating digital documents.

```
TimeStampResp ::= SEQUENCE {

status PKIStatusInfo,
timeStampToken TimeStampToken OPTIONAL
}
```

status Sequence. Sequence in which, using three fields, the result of the operation is indicated as whole, one descriptive chain of the result and another descriptive chain used in the event of an error. If the result is not satisfactory, the field timeStampToken will not be present.
timeStampToken Sequence. Type CMSSignedData signed structure which includes the digital dating and its signature. It includes the certificates of the Digital Dating Authority and of the CA if requested in the petition.

```
TSTInfo ::= SEQUENCE {
version INTEGER { v1 (1) },
policy TSAPolicyId,
messageImprint MessageImprint,
serialNumber INTEGER
genTime GeneralizedTime,
accuracy Accuracy OPTIONAL,
ordering BOOLEAN DEFAULT FALSE,
nonce INTEGER OPTIONAL,
tsa [0] GeneralName OPTIONAL,
extensions [1] IMPLICIT Extensions OPTIONAL
}
```

version. Describes the version of the reply. It is currently version 1.

policy Identifier of the policy used to provide the service, i.e. this policy (OID 1.3.6.1.4.1.5734.3.1.3).

messageImprint. Structure that contains the hash of the time-stamped document and the hash algorithm used and sent by the client. Its value must be exactly the same as the one received in the request.

serialNumber. Whole unique number assigned by the TSA to the generated Digital Time Stamp.

genTime. Time mark assigned by the Time-Stamping Authority. A fractional second string to milliseconds will be displayed. In accordance with RFC 3161 trailing zeros are not to be included in fractional second strings.

accuracy. Represents the precision of the time provided.

ordering. False value. Ordering two digital Time Stamps is only possible when the difference between both genTime is higher than the sum of the precisions of both.

nonce Whole. Random number used to link request to reply. It should be present if it was present in the request.

tsa Sequence. Identifier of the tsa which coincides with the subject name included in the certificate of the TSA.

extensions. Extensions of the reply.

77. The *Time Stamps* issued under this policy are signed electronically by the *Signature Creation Data* of the FNMT-RCM using the following algorithms:

- SHA-256
- RSA 3072

The *Signature Creation Data* of the second *Time-stamping* unit are associated to the following *Certificate.*

Table 3 – Certificate profile of the second *Time-stamping* unit employed in issuing *Time Stamps* under the FNMT Class 2 CA policy

FIELD	**CONTENT**
1. Version	V3

2. Serial Number	3C AC 63 50	
3. Signature algorithm	Sha1withRSAEncryption	
4. Issuer Distinguished Name	OU = FNMT Class 2 CA, O = FNMT, C = ES	
5. Validity	From: Tuesday, 31 March 2009 15:39:51 To: Saturday, 31 March 2012 15:39:51	

6. Subject	DESCRIPTION TSA2 FNMT CLASS 2 CA – ENTITY FNMT RCM – CIF Q2826004J
	OU = 500070015
	OU = Public
	OU = FNMT Class 2 CA
	O = FNMT
	C = ES	

7. Subject Public Key Info	(RSA 2048 bits)	
8. subjectAltName	Directory address: OID.1.3.6.1.4.1.5734.1.8 (fnmtDescription) = TSA2 FNMT CLASS 2 CA OID.1.3.6.1.4.1.5734.1.14 (fnmtPropEnt) = Fabrica Nacional de Moneda y Timbre Real Casa de la Moneda OID.1.3.6.1.4.1.5734.1.15 (fnmtPropCIF) = Q2826004J	
basicConstrains	Type of issue=End entity Route length restriction=None	
privateKeyUsagePeriod	From: 20090331144033 UTC To: 20120331144033 UTC	
keyUsage	Digital signature	

extKeyUsage	Digital dating	YES
subjectKeyIdentifier	14 b5 8a 4c 20 50 20 8e be f3 46 cd 11 aa df 02 cc 7d 87 00	
authorityKeyIdentifier	40 9a 76 44 97 74 07 c4 ac 14 cb 1e 8d 4f 3a 45 7c 30 d7 61	
crlDistributionPoints	CN=CRL5683, OU=FNMT Class 2 CA, O=FNMT, C=ES	

AC AP FNMT-RCM TIME-STAMP POLICY

IDENTIFICATION

This *Time Stamp Policy* of the FNMT-RCM for issuing *Time Stamps* has the following identification:

Table 4 – AC AP FNMT-RCM Time Stamp Policy Identification

Name	AC AP FNMT-RCM *Time-stamp Policy*
Reference/OID	1.3.6.1.4.1.5734.3.1.2.
Version	1.1
Location	http://www.cert.fnmt.es/dpcs/
Associated CPS	General Certification Practices Statement of the FNMT-RCM
Location	http://www.cert.fnmt.es/dpcs/

This policy is applicable to the different time-stamping units (TSU) that the FNMT-RCM may establish to provide the service.

It is identified and referenced with the *OID* 1.3.6.1.4.1.5734.3.1.2 and can be found at the following address:

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

in its latest version in force.

The procedures and contents referenced here are mainly based on the standards of the *European Telecommunications Standards Institute* (ETSI):

- ETSI TS 102 042 - Policy requirements for certification authorities issuing public key certificates.

- ETSI TS 101 456 - Policy requirements for certification authorities issuing qualified certificates.

- ETSI TS 102 023 - Policy requirements for time-stamping authorities, and

- ETSI TS 101 861- Time-stamping profile.

This policy is in keeping with standard ETSI TS 102 023 and with the equivalent specifications of the IETF - RFC 3628 Policy requirements for Time-stamping Authorities (TSAs).

COMMUNITY AND SCOPE OF APPLICATION

This policy is applicable to the issuing of *Time Stamps* with the following characteristics:

- They are issued by the FNMT-RCM as CSP in compliance with the criteria established in Law 59/2003 of 19 December, on the Electronic Signature, Law 11/2007 of 22 June, on Citizen Electronic Access to Public Services and the EESSI technical standards, specifically [ETSI TS 102 023].

- They are issued based on the criteria established for them in the EESSI technical standards [ETSI TS 101 861] and [RFC 3161].

- They are signed electronically with the *Certificates* and *Signature Creation Data* of the FNMT-RCM, specifically under the certification chain of the root Certification Authority with CN=AC ROOT FNMT-RCM.

- They expressly include data on adhesion to this policy through the “policy” field of the *Time Stamp* itself.

- They are issued on request of *User Entities* which are part of the *Electronic Community*, as defined in the ***Definitions*** section of the [GCPS], which are specifically the administrations defined in the scope of application of the above-mentioned Law 11/2007 of 22 June.

USE RESTRICTION OF THE TIME-STAMPING SERVICE AND TIME STAMPS

To be able to use the service adequately one must previously be part of the *Electronic Community,* acquire the status of *User Entity,* be one of the administrations defined in the scope of application of the above-mentioned Law 11/2007 of 22 June, and have signed the respective service use agreement. Only within this framework shall the *User Entity* be able to obtain the instructions and privileges needed to send data electronically to the FNMT-RCM for a *Time Stamp* to be created with that data.

On another front, to enable a third party to have confidence in the *Time Stamps* issued by the FNMT-RCM, a *Certificates* verification service is made available to *User Entities* of the *Electronic Community*, where they can consult the state of the *Certificate* used to construct the time stamp in question.

Therefore, outside the *Electronic Community* and before having made the pertinent verifications, one should not trust a *Time Stamp* issued under this *Time-stamp Policy* of the FNMT-RCM. In any case, should a third party rely on that trust, no cover shall be given under this policy and there shall be no entitlement to claim or take legal action against the FNMT-RCM for damage, loss or disputes arising from the use of or trust in a *Certificate.*

The FNMT-RCM does not guarantee the veracity of the contents represented by the electronic data being time-stamped, such as electronic files, or their authorship. Furthermore, the FNMT-RCM does not endorse them or participates in their creation in any way, and is not responsible for the use that may be made of them or for the effects that the latter may have on interested and/or third parties, subject to the general rules of the procedure. The FNMT-RCM is not associated in any way with the origin or causality of this electronic data.

The FNMT-RCM, through its *Time-stamping Service*, only guarantees the existence of the data being time-stamped, which could well be a particular representation of other data, at the moment in time in which it receives the request, which is determined by the time reference employed. This guarantee is expressed through the joint electronic signature of that data and that time reference with a *Certificate* whose holder is the FNMT-RCM, the provider of the *Time-stamping Service,* whose role in the service is that of *Time-stamping Authority* and trusted third party. The FNMT-RCM rejects any interpretation of the guarantees offered by the time stamps that it issues beyond that expressed above. The *Time-stamping Authority*, which is the FNMT-RCM, is therefore a trusted third party without any particular interest in the documents being time-stamped, although its signature will be proof of existence at a given moment in time.

LIABILITY AND OBLIGATIONS OF THE PARTIES

This *Time-stamp policy* covers the liability and obligations of the parties involved in the provision of the *Time-stamping Service* and in the issuing and use of the *Time Stamps*.

Liability of the parties

To be able to request the issuing of *Time Stamps* and/or verify their validity, one must previously be part of the *Electronic Community,* acquire the status of *User Entity* and be one of the administrations defined in the scope of application of the above-mentioned Law 11/2007 of 22 June. Outside the *Electronic Community* the FNMT-RCM shall not be liable for any damage or loss to any of the parties involved derived from the use of the *Time Stamps* issued under this policy. Therefore, this institution does not recommend trusting the *Time Stamps* in the aforementioned circumstances.

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

Liability of the Certification Services Provider (FNMT-RCM)

The FNMT-RCM shall only be liable for variations in the time reference from to the reference provided by the Time Section of the Royal Institute and Observatory of the Spanish Navy in San Fernando, Cadiz, which is introduced into the time stamps at the time of the request, but not for the data attached to the time reference which appear in the issued time stamp itself or for the consequences derived from their use by a third party.

The FNMT-RCM shall not be liable for the veracity or for the contents represented by the electronic data being time-stamped.

The FNMT-RCM shall not be liable for any damage or losses and/or defective functioning caused by the use of the *Time Stamps* that it issues, whether due to the fault of the interested parties or defects of origin in the elements.

The FNMT-RCM shall not be liable to persons whose conduct in the use of the time-stamping service and/or the *Time Stamps* themselves has been negligent. For this purpose, negligence shall be understood as failure to observe that established in this Time-stamping Policy and Practices Statement, in the [GCPS] and, in particular, in the sections on the obligations and liability of the parties.

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

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

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

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

Liability of the User Entities of the service

Unless otherwise arranged with the FNMT-RCM, it is the *User Entity's* responsibility to verify the *Electronic Signatures* employed in issuing the *Time Stamps* and to check the state of the *Certificates* in the confidence chain, and under no circumstances shall the authenticity of the *Stamps* or *Certificates* be assumed without having made these verifications.

It is the responsibility of the *Requestor* and holder of the *Time Stamps* to re-sign or re-stamp the data object of the *Time Stamp* should the algorithm employed in issuing the *Time Stamp* become obsolete, thus invalidating its evidential and truthful nature.

The *Requestor* and receiver of the *Time Stamp* (*User Entities*) shall be liable to the relying parties for the data object of the time reference included in the *Time Stamp* and for the repercussions of its use by a third party.

Furthermore, the *User Entity* shall be responsible for observing that established in the applicable *Time-stamping Policies and Practices*, the GCPS and any possible future amendments to it, with particular attention to the use restrictions established for the *Time Stamps* in their respective policies.

Liability of the relying parties

Unless otherwise arranged with the FNMT-RCM, it is the *Relying Parties'* responsibility to verify the *Electronic Signatures* employed in issuing the *Time Stamps* and the *Certificates* in the confidence chain, and under no circumstances shall the authenticity of the *Stamps* or *Certificates* be assumed without having made these verifications.

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

If the circumstances point to the need for additional guarantees, the *Relying Party* should obtain additional guarantees to ensure that that trust is reasonable.

Obligations of the parties

Obligations of the Certification Services Provider (FNMT-RCM)

The FNMT-RCM, as *Time-stamping Service Provider* and established *Time-Stamping Authority* through this service, is required to:

- On a general basis, follow the procedures and guidelines set out in this policy and practices statement for the issuing of *Time Stamps*, and in the GCPS.

- Maintain and calibrate the time reference employed in issuing *Time Stamps* with a maximum deviation of 50 ns from the time reference provided by the Time Section of the Royal Institute and Observatory of the Spanish Navy in San Fernando, Cadiz.

- Include in the *Time Stamps* that it issues the necessary elements to determine the date and time in which the stamp in question was issued, and the data being time-stamped received by the *User Entity*, without altering or changing them.

- Manage the *Private Keys* employed in issuing the *Time Stamps* and *Certificates* participating in the service in accordance with that established in the “Management of the lifecycle of the *Certification Services Provider’s Keys*” section of the [GCPS], in such a way that their confidentiality and integrity are ensured.

- Employ a secure signature creation device and a reliable time source as time reference in the *Time Stamp* issuing process.

- Retain all information and documentation relating to the *Time-stamp* requests and the respective replies resulting from the provision of the service for a period of at least fifteen (15) years.

- Make this policy public and freely accessible, and retain the *Time-stamping Policies and Practices* under appropriate security conditions for a period of 15 years after the end of their validity as a result of the publication of a new version.

- Keep a secure and updated *Certificates Directory,* in which the *Certificates* employed in the provision of the service and their validity are identified, including, in the form of *Revocation Lists,* the identification of the *Certificates* which have been revoked or suspended. The integrity of this *Directory* shall be protected by utilising systems in keeping with the specific regulatory provisions adopted in Spain and, as the case may be, in the EU, and access to the *Directory* shall be available as established in the

Specific Certification Policies and Practices corresponding to the *Certificates* in question.

- Provide a consultation service on the validity of the *Certificates*. This service is provided as described in the [GCPS] and in the *Specific Certification Policies and Practices* corresponding to the *Certificates* to be validated.

- Should the calibration of the time reference be or be thought to be compromised, duly advise all the parties and provide a description of the situation.

- Refrain from issuing *Time Stamps* should the *Time-stamping service* operations be or be thought to be compromised (keys, loss of calibration of the clock, etc.). In this case, the FNMT-RCM shall make available to the parties and the competent authority the necessary information to identify the affected *Time Stamps*. The FNMT-RCM shall restore the service as soon as the necessary conditions for doing so are re-established.

Obligations of the User Entities of the service

The parties using the Time-stamping Service (requests) are required to:

- On a general basis, follow the procedures and guidelines set out in this policy and practices statement for the issuing of *Time Stamps* and in the GCPS.

- Be one of the administrations defined in the scope of application of the above-mentioned Law 11/2007 of 22 June, a member of the *Electronic Community* and an established *User Entity*.

- Have signed the respective service use agreement.

- Identify oneself using an electronic *Certificate* with the pertinent characteristics and in force before requesting any time stamp.

- Before placing one's trust in the *Time Stamps*:

  1) Verify that the electronic signature accompanying the *Time Stamps* is the signature of the FNMT-RCM and not another and that it is correct.

  2) Check the validity of the *Certificates* employed in issuing the *Time Stamp* in question through the procedures indicated in the *Specific Certification Policies and Practices* corresponding to the *Certificates* being validated.

- Use the *Time Stamps* within the limits and scope described in this policy.

- Don't rely on the *Time Stamps* as time reference should the *Certification Services Provider* have ceased its activity as *Time-stamping Authority* which issues stamps under this policy and the subrogation provided for in the law has not taken place. In any event, the *User Entity* shall refrain from using the *Time Stamps* in cases where the *Provider's Signature Creation Data* may be threatened and/or compromised and this has been communicated by the *Provider* or, as the case may be, the circumstance is made known to the *Requestor* or holder of the *Stamp*.

- Don't rely on the Time Stamps as time reference beyond the use restrictions established for them in their respective policy.

Obligations of the relying parties

The parties who rely on a *Time Stamp* issued by the FNMT-RCM are required to:

- On a general basis, follow the procedures and guidelines set out in this policy and practices statement for the issuing of *Time Stamps.*

- Be part of the *Electronic Community*.

- Prior to placing one's trust in the Time Stamps:

  1) Verify that the electronic signature accompanying the *Time Stamps* is the signature of the FNMT-RCM and not another and that it is correct.

  2) Check the validity of the *Certificates* employed in issuing the *Time Stamp* in question through the procedures indicated in the *Specific Certification Policies and Practices* corresponding to the *Certificates* being validated.

- Accept the *Time Stamps* within the limits and scope described in this time-stamping policy and practices statement.

MANAGEMENT OF THE LIFECYCLE OF THE CERTIFICATION SERVICES PROVIDER'S KEYS

For the purpose of providing the time-stamping service, the FNMT-RCM carries out the management of the corresponding keys in accordance with that described in the "Management of the lifecycle of the Certification Services Provider's Keys" section of the GCPS.

The *Time Stamps* issued under this policy are signed by specific *Certificates*, which in turn have been issued by the *Certificate* with the distinguished name "CN = AC Public Administration, SERIALNUMBER = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES" and which in turn has been issued by the *Root Certificate* of the *Certification Authority* "AC ROOT FNMT-RCM"

For further information on the "AC ROOT FNMT-RCM" root certificate, please consult the "Certification Chains" section of the GCPS.

The FNMT-RCM has three *Time-stamping* units for issuing *Time Stamps* under this policy.

The *Signature Creation Data* of the first *Time-stamping* unit are associated to the following *Certificate.*

Table 5 – Certificate profile of the first *Time-stamping* unit employed in issuing *Time Stamps* under the AC AP FNMT-RCM policy

FIELD	CONTENT

1. Version	V3	
2. Serial Number	55 a2 08 97 ea 46 c6 cf 4e d6 02 c5 22 89 12 4e	
3. Signature algorithm	sha1withRSAEncryption	

4. Issuer Distinguished Name	CN = AC Public Administration
	SERIALNUMBER = Q2826004J
	OU = CERES
	O = FNMT-RCM
	C = ES	

5. Validity	From: Wednesday, 30 November 2011 11:17:41 To: Monday, 30 November 2015 11:17:41	

6. Subject	CN = DESCRIPTION SERVER TIME STAMP AP TSU 1 – ENTITY FNMTRCM – CIF Q2826004J
	OU = CERES
	O = FNMT-RCM
	C = ES	

7. Subject Public Key Info	(RSA 2048 bits)	

8. subjectAltName	OID.1.3.6.1.4.1.5734.1.8=SERVER TIME STAMP AP TSU 1
	OID.1.3.6.1.4.1.5734.1.14=Fabrica Nacional de Moneda y Timbre Real Casa de la Moneda
	OID.1.3.6.1.4.1.5734.1.15=Q2826004J	

basicConstrains	Type of issue=End entity Route length restriction=None	
keyUsage	Digital signature, without repudiation	

extKeyUsage	Digital dating	YES
subjectKeyIdentifier	37 10 02 1c 7f 39 f0 a1 c7 1e d3 73 36 fe 2e 5a 50 2c 7c b0	
authorityKeyIdentifier	14 11 e2 b5 2b b9 8c 98 ad 68 d3 31 54 40 e4 58 5f 03 1b 7d	
crlDistributionPoints	URL address = ldap://ldapape.cert.fnmt.es/CN=CRL20,CN=AC%20 Administraci%F3n%20P%FAblica,OU=CERES,O= FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint URL address = http://www.cert.fnmt.es/crlsacap/CRL20.crl	

The *Signature Creation Data* of the second *Time-stamping* unit are associated to the following *Certificate.*

Table 6 – Certificate profile of the second *Time-stamping* unit employed in issuing *Time Stamps* under the AC AP FNMT-RCM policy

FIELD	CONTENT
1. Version	V3
2. Serial Number	0a 5c 13 47 b5 91 59 b9 4e bb c9 e4 85 0f 63 4d
3. Signature algorithm	Sha1withRSAEncryption

4. Issuer Distinguished Name	CN = AC Public Administration
	SERIAL NUMBER = Q2826004J
	OU = CERES
	O = FNMT-RCM
	C = ES

5. Validity	From: Thursday, 10 November 2011 13:56:04 To: Tuesday, 10 November 2015 13:56:04

6. Subject	CN = DESCRIPTION SERVER TIME STAMP AP TSU 2 – ENTITY FNMTRCM – CIF Q2826004J
	OU = CERES
	O = FNMT-RCM
	C = ES

7. Subject Public Key Info	(RSA 2048 bits)

8. subjectAltName	OID.1.3.6.1.4.1.5734.1.8=SERVER TIME STAMP AP TSU 2
	OID.1.3.6.1.4.1.5734.1.14=Fabrica Nacional de Moneda y Timbre Real Casa de la Moneda
	OID.1.3.6.1.4.1.5734.1.15=Q2826004J

basicConstrains	Type of issue=End entity Route length restriction=None
keyUsage	Digital signature, Without repudiation

extKeyUsage	Digital dating	YES
subjectKeyIdentifier	52 6e 07 fd 07 f7 05 4c ed 1c b9 3a 59 7e 47 07 16 b6 3c cb	
authorityKeyIdentifier	14 11 e2 b5 2b b9 8c 98 ad 68 d3 31 54 40 e4 58 5f 03 1b 7d	
crlDistributionPoints	URL address = ldap:ldapape.cert.fnmt.es/CN=CRL20,CN=AC%20 Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint URL address= http://www.cert.fnmt.es/crlsacap/CRL20.crl	

119. The *Signature Creation Data* of the third *Time-stamping* unit (employed as a backup to both the above) are associated to the following *Certificate.*

Table 7 – Certificate profile of the third *Time-stamping* unit employed in issuing *Time Stamps* under the AC AP FNMT-RCM policy

FIELD	**CONTENT**
1. Version	V3
2. Serial Number	74 fc ba fl 79 07 9b b4 4e ce 2f 98 b3 87 a2 30
3. Signature algorithm	sha1withRSAEncryption

4. Issuer Distinguished Name	CN = AC Public Administration
	SERIAL NUMBER = Q2826004J
	OU = CERES
	O = FNMT-RCM
	C = ES

5. Validity	From: Thursday, 24 November 2011 12:50:48 To: Tuesday, 24 November 2015 12:50:48	

6. Subject	CN = DESCRIPTION SERVER TIME STAMP AP TSU 3 – ENTITY
	OU = CERES
	O = FNMT-RCM
	C = ES	

7. Subject Public Key Info	(RSA 2048 bits)	

8. subjectAltName	OID.1.3.6.1.4.1.5734.1.8=SERVER TIME STAMP AP TSU 3
	OID.1.3.6.1.4.1.5734.1.14=Fabrica Nacional de Moneda y Timbre Real Casa de la Moneda
	OID.1.3.6.1.4.1.5734.1.15=Q2826004J	

basicConstrains	Type of issue=End entity Route length restriction=None	
keyUsage	Digital signature, without repudiation	
extKeyUsage	Digital dating	YES
subjectKeyIdentifier	95 30 24 ab 35 57 cb 07 b1 dc 7c a0 fe 70 dd 98 72 35 15 3f	
authorityKeyIdentifier	14 11 e2 b5 2b b9 8c 98 ad 68 d3 31 54 40 e4 58 5f 03 1b 7d	
crlDistributionPoints	URL address = ldap:ldapape.cert.fnmt.es/CN=CRL20,CN=AC%20 Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint	

	URL address= http://www.cert.fnmt.es/crlsacap/CRL20.crl	

PROVISION AND AVAILABILITY OF THE TIME-STAMPING SERVICE

The issuing of *Time Stamps* is carried out on request of the *User Entity*. Whenever the *User Entity* wishes to obtain a *Time Stamp* for an electronic document, it should calculate a hash value or set of values based on the document. This generates a small but compact amount of information that is sent to the FNMT-RCM for the corresponding *Time Stamp* to be issued.

This *Time Stamp* will bind the data received to the date and time of reception, through the electronic signature of the FNMT-RCM.

It is worth highlighting that the FNMT-RCM decides whether the hash algorithm used to represent the document is sufficiently secure in accordance with its service policies and, if it is, it will allow the request to be processed. Specifically, the following hash algorithms are accepted:

- SHA-1,
- SHA-256,
- SHA-384,
- SHA-512

The FNMT-RCM will not carry out any verification or processing of the representation of the data received for time-stamping, beyond their inclusion in the *Time Stamp* itself and in the events registration systems. The FNMT-RCM will not verify in any way the content or the veracity of the representation of the data to be time-stamped or their origin.

The *Time-stamping Service* shall be available twenty-four (24) hours a day, every day of the year, unless due to circumstances outside the control of the FNMT-RCM or maintenance operations. The FNMT-RCM shall communicate the aforementioned circumstances through the address http://www.ceres.fnmt.es at least forty-eight (48) hours in advance, and it shall try to solve the problem within a period of twenty-four (24) hours.

Both the *Time-stamp* requests and the replies are managed in accordance with that described in recommendation [RFC 3161].

TIME-STAMP REQUEST

To be able to request a *Time Stamp* one must be part of the *Electronic Community,* hold the status of *User Entity*, be one of the administrations defined in the scope of application of the above-mentioned Law 11/2007 of 22 June, and have signed the respective service use agreement with the FNMT-RCM.

127. Before making a request, the *User Entity* must obtain a *Component Certificate* or an *Electronic Signature Certificate,* which it will use as an identification and authentication mechanism with each *Time-stamp* request.

128. Using the HTTPS protocol and identifying oneself with the aforementioned *Component Certificate*, the *User Entity* will compose a *Time-stamp* request in accordance with recommendation [RFC 3161].

129. The *Time-stamp* requests are sent to the following address:

https://apuseg.cert.fnmt.es/TimeStampAPE

130. encapsulated as Content-Type: application/timestamp-query, encoded in DER and described in ASN.1.

131. The ASN.1 structure corresponding to the request is:

```
TimestampRequest ::= SEQUENCE {
version Integer { v1 (1) },
messageImprint MessageImprint,
reqPolicy PolicyInformation OPTIONAL,
nonce Integer OPTIONAL,
certReq BOOLEAN DEFAULT FALSE,
extensions [0] IMPLICIT Extensions OPTIONAL
}
```

Version Whole. Describes the version of the request. It is currently version 1.

messageImprint Sequence. Structure containing the hash of the document to be date-stamped and the hash algorithm used.

reqPolicy reqPolicy Identifier of the policy requested to be applied in the provision of the service. It is optional and can be omitted, but if used, it should contain the OID of this policy (1.3.6.1.4.1.5734.3.1.2).

nonce Whole. Random number used to link request to reply.

certReq Boolean. If its value is "True" the TSA is required to include its certificate in the reply.

Extensions Sequence. Extensions of the request.

TIME-STAMP REQUEST REPLY

The replies to a *Time-stamp* request are received at the following address:

https://apuseg.cert.fnmt.es/TimeStampAPE

encapsulated as Content-Type: application/timestamp-reply, encoded in DER and described in ASN.1.

The content of the reply is an ASN.1 structure, which includes the result of the operation (status), i.e. whether or not the operation has been carried out satisfactorily, and a CMSSignedData (timeStampToken) structure, which includes the digital dating (TSTInfo) signed by the Digital Dating Authority.

The certificate of the Digital Dating Authority is a certificate issued by the CA with the extension id-kp-timestamping, which indicates that the certificate will be used for the sole purpose of dating digital documents.

```
TimeStampResp ::= SEQUENCE {
status PKIStatusInfo,
timeStampToken TimeStampToken OPTIONAL
}
```

status Sequence. Sequence in which, using three fields, the result of the operation is indicated as whole, one descriptive chain of the result and another descriptive chain used in the event of an error. If the result is not satisfactory, the timeStampToken field will not be present.
timeStampToken Sequence. Type CMSSignedData signed structure which includes the digital dating and its signature. It includes the certificates of the Digital Dating Authority and of the CA if requested in the petition.

```
TSTInfo ::= SEQUENCE {
version INTEGER { v1 (1) },
policy TSAPolicyId,
messageImprint MessageImprint,
serialNumber INTEGER
genTime GeneralizedTime,
accuracy Accuracy OPTIONAL,
ordering BOOLEAN DEFAULT FALSE,
nonce INTEGER OPTIONAL,
tsa [0] GeneralName OPTIONAL,
extensions [1] IMPLICIT Extensions OPTIONAL
}
```

version Whole. Describes the version of the reply. It is currently version 1.

policy Identifier of the policy used to provide the service, i.e. this policy (OID 1.3.6.1.4.1.5734.3.1.2).

messageImprint Sequence. Structure that contains the hash of the date-stamped document and the hash algorithm used and sent by the client. Its value must be exactly the same as the one received in the request.

serialNumber Whole. Whole unique and consecutive number assigned by the TSA to the generated digital Time Stamp.

genTime Date and Time. Date and time assigned by the Time-stamping Authority to the Time Stamp in GMT format.

accuracy Sequence. Represents the precision of the time provided.

ordering If this field is not present or its value is “false”, the genTime field only indicates the moment in which the time stamp was issued. Therefore, ordering two digital Time Stamps is only possible when the difference between both genTime is higher than the sum of the precisions of both. If, on the other hand, the field is present and its value is “true”, then the genTime field may be used to order any digital Time Stamp, without taking the accuracy field into account.

nonce Whole. Random number used to link request to reply. It should be present if it was present in the request.

tsa Sequence. Identifier of the tsa which, if present, should coincide with the subject name included in the certificate of the TSA.

extensions Sequence. Extensions of the reply.

The *Time Stamps* issued under this policy are signed electronically by the *Signature Creation Data* of the FNMT-RCM using the following algorithms:

- SHA-1
- RSA 2048