Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLICIES AND PRACTICES OF THE QUALIFIED TIME STAMPING SERVICE

	NAME	DATE
Prepared by:	FNMT-RCM	19/06/2020
Reviewed by:	FNMT-RCM	29/06/2020
Approved by:	FNMT-RCM	29/06/2020

DOCUMENT HISTORY			
Version	**Date**	**Description**	**Author**
1.0	03/01/2017	Creation of the document	FNMT-RCM
1.1	22/12/2017	Annual revision of the document	FNMT-RCM
1.2	12/11/2019	Inclusion of a new AC Unidades de Sellado de Tiempo for the issuance of TSU certificates	FNMT-RCM
1.3	29/06/2020	Inclusion of TSU 2020 certificate issued by AC Unidades de Sellado de Tiempo.	FNMT-RCM

Reference number: DPSCST/DPSCST0103/SGPSC/2020

Document classified as: *Public*

CONTENTS

INDEX OF TABLES

1. REFERENCES

[TSPS] Trust Services Practices and Electronic Certification Statement (http://www.cert.fnmt.es/dpcs/)

[ETSI EN 319 401] - General Policy Requirements for Trusted Service Providers

[ETSI EN 319 421] - Policy and Security Requirements for Trusted Service Providers issuing Time-Stamps

[ETSI EN 319 422] - Time-stamping protocol and time-stamp token profiles

[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 interpretation of this document, the following definitions have been added to those established in the TSPS:

   - *Qualified Electronic Time Stamp:* An *electronic time stamp* that links the date and time of a set of data in such a way that the data cannot be modified without that modification being detected. The time stamp is based on a time information source that is linked to the Coordinated Universal Time (UTC), which has been signed / stamped by the advanced electronic signature / stamp of a *Qualified Trusted Service Provider.*

   (The terms expressed in italics are defined in this document or in the Trust Services Practices and Electronic Certification Statement)

3. INTRODUCTION AND PURPOSE

2. The Royal Spanish Mint (Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda), hereinafter referred to as the FNMT-RCM, is a *Qualified Trust Services Provider* of *Time Stamping Services,* whose aim is to attest to the existence of a set of data at a specific moment in time. To this end, the FNMT-RCM uses the time reference provided by the Time Section of the Spanish Royal Navy's Institute and Observatory (ROA) in San Fernando as the time information source for Coordinated Universal Time (UTC), under the agreement reached between that Entity and the FNMT-RCM for the continuous synchronisation of their systems. One of the missions of the ROA is the maintenance of the basic unit of time (it is officially recognised as the National Standard of that unit), as well as the maintenance and official dissemination of the "Coordinated Universal Time" scale (UTC -ROA-), which is considered, for all purposes, as the basis for official time across the whole Spanish territory (Royal Decree 1308/1992, dated 23 October 1992).

3. The provision of this service by the FNMT-RCM requires the party requesting the *Time Stamp* to file a request in advance (by sending a representation of the set of data), which will be answered with the corresponding electronic evidence (the *Electronic time stamp*). The aforementioned representation of the set of data received by the FNMT-RCM consists of a

hash function of the data, in such a way that the data itself cannot be identified. Therefore, the FNMT-RCM does not have access to the information over which it creates the *Electronic Time Stamp.*

4. This *Qualified Time Stamping Service* is offered by the FNMT-RCM in accordance with (EU) Regulation No 910-2014, issued by the European Parliament and Council on 23 July 2014, relating to electronic identification and trusted services for electronic transactions in the internal market and in relation to which Directive 1999/93/CE (eIDAS Regulation) was repealed.

4. ORGANIZATION OF THE DOCUMENT

5. This document, governing the Policies and Practices of the *Qualified Time Stamping Service*, forms an integral part of the *Trust Services Practices and Electronic Certification Statement* (TSPS) issued by the FNMT-RCM, as the *Trusted Service Provider* (TSP), and reflects the obligations and procedures that the FNMT undertakes to fulfil in relation to the provision of the *Qualified Time Stamping Service.* Therefore, this document contains the *Time Stamping Policy* and the *Statement of Practices for the Time Stamping Service*, hereinafter referred to as the PST and DPST, respectively.

6. This is a declaratory document and it describes the most significant aspects of the *Time Stamping Service* and the procedures employed and/or defined for its management and use. Similarly, it provides a self-declaration of the measures in place to safeguard the infrastructure and of the technical and non-technical security controls applied to the systems used in the provision of the service.

7. Meanwhile, the PST and the DPST contain the set of conditions of use, responsibilities and obligations of the parties, and limitations of the *Qualified Time Stamping Service* applicable under the framework of the *Electronic Community* once the corresponding agreements of use have been signed.

8. In conclusion, the purpose of this document is to provide public information about the conditions and characteristics of the *Qualified Time Stamping Service* rendered by the FNMT-RCM as the PSC. It details the obligations that the FNMT-RCM undertakes to fulfil regarding the management of the *Data for the Creation and Verification of the Signature /Stamp* and of the *Certificates* employed to offer the service and the conditions that apply to the request, dispatch, use and extinction of the validity of *Qualified Electronic Time Stamps*, as well as the rights and obligations of all of the parties that place their trust in and accept the service.

9. Since the provision of the *Qualified Time Stamping Service* forms part of the Trusted Services rendered by the FNMT-RCM, the rules established in the [TSPS] apply regarding: the liability framework applicable to members of the *Electronic Community* and third parties who place their trust in those services ; the security controls applied to their procedures and facilities; the protection of data of a personal nature; and other information-related questions associated with the aforementioned service.

5. ORDER OF PRIORITY

10. The FNMT-RCM is constituted as the *Time Stamping Authority* (TSA); and, with the aim of guaranteeing the provision of its *Time Stamping Services,* it may establish as many Time Stamping Units (TSU) as it deems appropriate and manage them in accordance with the specific and differentiated policies and practices. Nevertheless, this Policies and Practices document refers to the *Qualified Time Stamping Service*, whose Policies are perfectly identified by their corresponding OID and which is offered by a specific TSU.

11. Within this framework of action, the following order of priority is established (from highest to lowest) for the documentation of statements from the *Qualified Time Stamping Service* :

    1) The *Time Stamping Policies and Practices* contained herein, which are applicable to the provision of the *Qualified Time Stamping Service* and which are expressed in their entirety in this document, shall prevail over the general conditions governing the provision of trusted services by the FNMT-RCM and described in the [TSPS] document].

    2) The [TSPS], which applies, in a general way, to any trusted services rendered by the FNMT-RCM shall apply in addition and as an alternative to the document referred to in Section 1 above.

6. AVAILABILITY OF INFORMATION AND CONTACT METHOD

12. Refer to the [TSPS]

7. SECURITY CONTROLS, REGISTRATION OF EVENTS AND AUDITS

13. Refer to the [TSPS]

14. In addition, the FNMT-RCM implements specific measures to avoid threats related to the calibration of the clock used in this service, which are described in the following sections.

7.1. TIME SOURCE USED FOR THE PROVISION OF THE QUALIFIED SERVICE

15. The aim of the Royal Navy Observatory's (SS-ROA) Synchronisation System, which is installed at the FNMT-RCM's Data Processing Centre (CPD), is to provide a time reference source that is traceable to the UTC (ROA) time scale, for the provision of the FNMT-RCM's *Qualified Time Stamping Service.*

16. The SS-ROA mainly consists of: a Rubidium frequency pattern, a time and frequency comparison system that operates by means of a GPS satellite navigation system and two External Synchronisation Centres.

17. This set of equipment produces a series of files containing the data for the monitoring performed on a given day and are used by the ROA to prepare reports about differences between the pattern phase and the UTC (ROA) scale.

18. The reference date and time are supplied to the network through the External Synchronisation Centres via an NTP service. The time reference is supplied via a signal from the rubidium frequency pattern.

7.2. AGREEMENT WITH ROA TO GUARANTEE THE CLOCK CALIBRATION

19. The agreement of the FNMT-RCM with the ROA, cited above, guarantees that any change in the calibration of the synchronism control unit is detected by the monitoring system of said Royal Navy Observatory's, leaving traceability of said event and correcting said Sync error.

7.3. PRECISION OF THE SYNCHRONISATION FOR THE ISSUANCE OF THE ELECTRONIC TIME STAMP

20. The FNMT-RCM synchronizes its TSU with the synchronization center of the ROA, monitoring the synchronization at all times.

21. The declared precision for the synchronisation of the TSU with the UTC is 100 milliseconds, which more than complies with the standard European requirements [ETSI EN 319 421]. The FNMT-RCM's *Qualified Time Stamping Service* shall not issue any *Qualified Electronic Time Stamp* in any time period during which there is a mismatch of more than 100 milliseconds between the TSU's clocks and the ROA's UTC time source.

7.4. GENERATION, STORAGE AND SAFEGUARD OF TSU PRIVATE KEYS

22. The TSU *Private keys* used by the FNMT-RCM *Qualified Time Stamping Service* are generated and guarded by a cryptographic device that meets the FIPS PUB 140-2 Level 3 security requirements, with algorithms and parameters suitable for the use of the key (Time stamp) and the expected duration, according to the recommendations of ETSI TS 119 312 or equivalent national regulations. The technical components necessary for the creation of *Keys* are designed so that a *Key* is only generated once, and so that a *Private Key* cannot be calculated from its *Public Key.*

23. The activity of creating *Qualified Electronic Time Stamps* is carried out within the cryptographic device, which provides *Confidentiality* to the *Seal creation data* of the *Trust Services Provider*. When the *Seal creation data* is outside the cryptographic device, the FNMT-RCM applies the appropriate technical and organizational measures to guarantee its *Confidentiality*.

24. Copy, save, or retrieve of the *Seal creation data* is performed under the exclusive control of authorized personnel, using at least dual control and in a secure environment.

25. A copy of the files and components necessary for the restoration of the security environment of the cryptographic device is kept, in case they have to be used, in security envelopes properly guarded inside a fireproof cabinet, which can only be obtained by authorized personnel.

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

26. Refer to the [TSPS]

9. INTELLECTUAL AND INDUSTRIAL PROPERTY

27. Refer to the [TSPS]

10. PROHIBITION OF RESERVICE WITH OR WITHOUT RESALE

28. The FNMT-RCM's *Qualified Time Stamping Service* may not be subject to re-service, with or without resale, unless added value is generated as a result. In the event that added value is generated for third parties, based on the service rendered by the FNMT-RCM, a request should be made to that entity to sign a contract for a wholesale tranche.

29. The FNMT-RCM shall be exempt from liability for actions taken by people, entities and organisations that proceed to provide such services for third parties without signing a contract for the wholesale tranche. All of this is notwithstanding any legal action that may be taken.

11. APPLICABLE LAW, INTERPRETATION AND GOVERNING JURISDICTION

30. Refer to the [TSPS]

12. MODIFICATION OF THE PST AND THE DPST

31. Refer to the [TSPS]

13. THE FNMT'S TIME STAMPING POLICY

13.1. IDENTIFICATION

32. This *Policy for the FNMT-RCM's Qualified Time Stamping Service* for the issuance of *Qualified Electronic Time Stamps* has the following identification reference:

Table 1 Identification of the Policy for the FNMT's Qualified Time Stamping Service

Name	*Policy for the FNMT's Qualified Time Stamping Service*
Reference/OID	0.4.0.2023.1.1
Version	1.3
Location	http://www.cert.fnmt.es/dpcs/
Related CPS	Trust Services Practices and Electronic Certification Statement
Location	http://www.cert.fnmt.es/dpcs/

33. This policy is applicable to the different time stamping units (TSU) that the FNMT-RCM may establish for the provision of the *Qualified Time Stamping Service* and is identified and referenced by *OID* number 0.4.0.2023.1.1 corresponding to the best-practices-ts-policy defined in the European standard ETSI EN 319 421.

34. The *Qualified Time Stamping Service* rendered by the FNMT-RCM, as the *Qualified Trusted Service Provider*, is rendered in accordance with the requirements of the eIDAS Regulations and the European standard ETSI EN 319 401 "General Policy Requirements for Trusted Service Providers".

13.2. COMMUNITY AND SCOPE OF APPLICATION

35. This policy is applicable to the issuance of *Qualified Electronic Time Stamps* that have the following characteristics:

- They are issued by the FNMT-RCM as the PSC in compliance with the criteria established by the technical standards EESSI, specifically [ETSI EN 319 421].
- They are issued on the basis of the criteria established for that purpose by the technical standards [ETSI EN 319 422] and [RFC 3161].
- They are signed electronically with *Signature Creation Data / Stamp* from the FNMT-RCM, specifically under the *Chain of Certification* of the *Certification Authority* with roots in CN=AC RAIZ FNMT-RCM.
- The policy defined through the "policy" field of the *Qualified Electronic Time Stamp* expresses adherence to the general policy of the European standard ETSI EN 319 421 (best practices policy for time-stamp).
- They are issued upon request by the *User Entities* that form part of the *Electronic Community,* as defined in the ***Definitions*** section of the [TSPS].

13.3. LIMITS REGARDING THE USE OF THE TIME STAMPING SERVICE AND TIME STAMPS

36. In order to be entitled to use the service in the appropriate way, users must first: form part of the *Electronic Community*; register as a *User Entity;* and have signed the corresponding agreement governing the use of the service. Only under this operating framework shall the *User Entity* obtain sufficient instructions and privileges to send data in an electronic format to the FNMT-RCM for the purposes of creating an *Electronic Time Stamp* for that data.

37. Meanwhile, for the purposes of enabling a third party to place its trust in an *Electronic Time Stamp* issued by the FNMT-RCM, the FNMT itself provides an *Information and query service regarding the status of certificates* through which third parties may consult the status of the *Certificate* employed to construct the *stamp* in question.

38. Therefore, a third party should not trust an *Electronic Time Stamp* issued under this *Time Stamp Policy* by the FNMT-RCM without performing the relevant checks. In such a case, no coverage would be obtained from the policy contained herein and any claims or legal actions filed against the FNMT-RCM for damages, harm or conflicts resulting from the use of or trust placed in this service would lack legitimacy.

39. The FNMT-RCM does not vouch for the truthfulness of the content represented by the electronic data subject to the *Time Stamp,* or for its author. Similarly, it does not endorse the content, or participate in its creation in any way, nor is it responsible for any use that may be made of it or of the effects that it may have on interested and/or third parties. The FNMT-RCM does not have any links whatsoever to the origin or causality of the aforementioned electronic data.

40. Through its *Time Stamping Service*, the FNMT-RCM exclusively guarantees the existence of certain data, which may be a particular representation of other data, at the specific moment in time at which it receives the request and determined by the time reference employed. This guarantee is expressed through the *Electronic Stamp* together with that data and that time reference with a *Certificate*, which is owned by the FNMT-RCM, as the provider of the *Qualified Time Stamping Service* and whose role in this process is that of *Time Stamping Authority* and trusted third party. The FNMT-RCM rejects any interpretation of the guarantees provided by the *Time Stamps* that it issues beyond those expressed above. The FNMT-RCM's *Time Stamping Authority* is, therefore, a trusted third party, without any particular interest in the documents that it dates, even though its *Electronic stamp* shall prove the existence of the documents at a specific moment in time.

13.4. RESPONSIBILITIES AND OBLIGATIONS OF THE PARTIES

41. This *Time Stamp* policy details the responsibilities and obligations of the parties involved in the provision of the *Qualified Time Stamping Service* and in the issuance and use of *Electronic Time Stamps*.

13.4.1. Responsibilities of the parties

42. In order to be entitled to request the issue of *Electronic Time Stamps,* a user must first form part of the *Electronic Community* and register as a *User Entity*.

13.4.1.1. Responsibilities of the Trusted Service Provider (FNMT-RCM)

43. The FNMT-RCM is responsible for any variation in the time reference, in relation to the source supplied by the Time Section of the Spanish Royal Navy's Institute and Observatory, which is introduced into the *Electronic Time Stamps* when the request is made, and has no responsibility whatsoever for the truthfulness and contents represented by the electronic data sent by the entities using the service that are subject to the *Electronic Time Stamp* issued.

44. The FNMT-RCM shall not be held responsible for any damage or harm and/or defective operations that the *Electronic Time Stamps* that it issues cause as a result of the uses that are made of them, either due to the fault of interested parties or defects in the original data.

45. The FNMT-RCM shall not be liable to anyone whose behaviour when using the *Qualified Time Stamping Service* and/or the *Electronic Time Stamps* themselves is negligent. For these purposes, and in all cases, failure to observe the provisions established in these Policies and Practices for the *Qualified Time Stamping Service,* in the [TSPS] and, in particular, the provisions in the sections relating to the obligations and responsibilities of the parties, shall be deemed to constitute negligence

46. The FNMT-RCM shall not be liable in the event of unforeseen circumstances, force majeure, terrorist attacks, wildcat strikes, or in the case of events involving actions that constitute a crime or failure that affects the underlying infrastructure, except in the event that the entity itself committed a serious breach. In any case, in the corresponding contracts and/or agreements, the FNMT-RCM may establish additional liability limitation clauses to those reflected in this document.

47. The FNMT-RCM shall not be responsible for any software that it has not supplied directly.

48. The FNMT-RCM does not guarantee the cryptographic algorithms and shall not be held liable for any damage caused by successful external attacks on the cryptographic algorithms used, provided it maintains due care over them, in accordance with the current status of the technique, and acts in accordance with the provisions of the applicable *Policies and Practices for Trusted Services and Electronic Certifications* and the Law.

49. In any case and by means of a penalty clause, the amounts that the FNMT-RCM must pay to each third party or member of the *Electronic Community* for damages and harm, in the absence of any specific regulations in the contracts and agreements, shall be limited to a maximum of SIX THOUSAND EUROS (€6,000).

13.4.1.2. Responsibilities of the service's User Entities

50. The *User Entity* shall be responsible for verifying the *Electronic Stamps* employed for the issuance of the *Electronic Time Stamps*, as well as for checking the status of the existing *Certificates* in the *Chain of Certification,* unless it is willing and able to contract these obligations directly with the FNMT-RCM. Under no circumstances may the authenticity of the *Stamps* or *Certificates* be presumed until these checks have been performed.

51. The *Requester and* owner of the *Electronic Time Stamps* shall be responsible for re-signing or re-stamping annexed data (appendices) to the *Electronic Time Stamp* in those cases in which the *Certificate* employed for the construction of that *Time Stamp* is no longer valid (for example, if it has expired, has been revoked or the algorithm has become obsolete), which would therefore compromise its reliability and accuracy.

52. The *Time Stamp Requester* and recipient of the *Electronic Time Stamp (User Entities)* shall be responsible against the relying parties for any data annexed to the time reference included in the aforementioned *Time Stamp* and for the implications that its use by a third party may have.

53. Similarly, the *User Entity* shall be responsible for observing the provisions of the applicable *Policies and Practices of the Qualified Time Stamping Service*, as well as of the [TSPS] and its possible future modifications, paying special attention to the limits of use established for the *Electronic Time Stamps* in their corresponding policies.

13.4.1.3. Responsibilities of the relying parties

54. The relying parties shall be responsible for verifying the *Electronic Stamps* employed for the issuance of the *Electronic Time Stamps*, as well as for the revocation status of the existing *Certificates* in the *Chain of Certification,* unless it is willing and able to contract these

obligations directly with the FNMT-RCM. Under no circumstances may the authenticity of the *Stamps* or *Certificates* be presumed until these checks have been performed.

55. The relying party cannot be considered to have acted with minimum due care if it trusts in an *Electronic Stamp* based on a *Certificate* issued by the FNMT-RCM without having observed the provisions established in the applicable *Policies and Practices for Trusted Services and Electronic Certifications* and checked that this *Electronic Stamp* may be verified by referring to a valid *Chain of Certification* .

56. If the circumstances require the need for additional guarantees, the relying party must obtain those guarantees to ensure that it has the trust that it deems reasonable.

13.4.2. Obligations of the parties

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

57. The FNMT-RCM, as the provider of the *Qualified Time Stamping Service* and the *Time Stamping Authority* in which it is constituted through this service, has the obligation to:

- In general, follow the procedures and guidelines set out in this Statement of Policies and Practices of the *Qualified Time Stamping Service*, as well as in the [TSPS].
- Maintain and calibrate the time reference employed for the issuance of *Electronic Time Stamps* with a deviation that does not exceed the time defined in the section corresponding to the precision of the synchronisation for the issuance of an *Electronic Time Stamp,* with respect to the time reference supplied by the Time Section of the Spanish Royal Navy's Institute and Observatory.
- Include the elements necessary to determine the date and time on which the *Stamp* in question has been issued in the *Electronic Time Stamps* that it issues, as well as the representation of the data to be dated, received from the *User Entity* , without making any alteration or modification whatsoever to that data.
- Manage the *Private Passwords* employed for the issue of *Electronic Time Stamps* and *Certificates* participating in the service, in accordance with the provisions of the section about the "Management of the lifecycle of the *Passwords"* of the *Trusted Service Provider* **"** of the [TSPS], and in such a way that ensures their confidentiality and integrity.
- Employ a reliable time source as a time reference in the process for issuing *Electronic Time Stamps.*
- Retain all of the information and documentation relating to requests for *Time Stamps* and the corresponding answers, for the purposes of rendering the service for at least fifteen (15) years.
- Make public and freely accessible the policy contained herein and retain the Policies and Practices for the *Qualified Time Stamping Service* for 15 years from the end of its validity, for the publication of a new version of them, in the appropriate security conditions.

- Maintain a secure and up-to-date *Directory* of *Certificates,* detailing the *Certificates* employed for the provision of the service, as well as their validity, including *Revocation Lists* containing the details of the *Certificates* that have been revoked or suspended. The integrity of this *Directory* shall be protected through the use of systems in accordance with the specific regulatory provisions established for this purpose in Spain and, where appropriate, in the EU; and it may be accessed in accordance with the provisions established in the *Individual Certification Policies and Practices corresponding to the Certificates* in question.
- Operate a query service regarding the validity of the *Certificates*. This service is rendered in accordance with the provision of the [TSPS] and the Individual Certification Policies and Practices corresponding to the Certificates to be validated.
- In the event that the calibration of the time reference is, or is suspected to have been compromised, all of the parties must be notified accordingly, and provided with a description of the situation.
- Not issue *Electronic time stamps* with a TSU whose *Electronic Certificate* is not in force, either by expiration or revocation of the same, and in case of expiration of the period of time of use of its *Private key*.
- Not issue *Electronic time stamps* in the event that the operations of the *Qualified Time Stamping Service* have been, or are suspected to have been comprised (any breach of the passwords, loss of calibration over the time, etc.). In this case, the FNMT-RCM shall provide the parties and the relevant authorities with the information necessary to identify the *Electronic Time Stamps* affected. The FNMT-RCM will restore the service when the necessary conditions have been established to enable it to do so.

13.4.2.2. Obligations of the service's User Entities

58. The parties that make use of the *Qualified Time Stamping Service* (requests) have the obligation to:

- In general, follow the procedures and guidelines set out in these Policies and Practices for the issuance of *Electronic Time Stamps*, as well as in the [TSPS].
- Be a member of the *Electronic Community* and to be constituted as a *User Entity.*
- Have signed the corresponding agreement in order to use the service.
- Authenticate itself through a valid electronic *Certificate* containing the relevant characteristics, prior to requesting any *Time Stamp.*
- As a step prior to placing trust in the *Electronic Time Stamps* :
    1) Verify that the *Electronic Stamp* that accompanies the *Electronic Time Stamps* has been issued by the FNMT-RCM and not any other party, and moreover, that it is correct.
    2) Check the validity of the *Certificates* employed for the issuance of the *Electronic Time Stamp* in question, through the procedures indicated in the

Individual Certification Policies and Practices corresponding to the *Certificates* to be validated.

- Use the *Electronic Time Stamps* within the limits and scope described in the Policies and Practices for the *Qualified Time Stamping Service*.
- Not allow the *Electronic Time Stamps* from serving as a time reference in the event that the *Trusted Service Provider* ceases its activity as the *Time Stamping Authority* that issues *Stamps,* under this policy, and the subrogation provided for by law has not been effected. In any case, *Electronic Time Stamps* shall not be used in those cases in which the *Provider's Signature Creation Data* may be threatened and/or compromised, and the *Provider* has been notified accordingly or, where appropriate, the *Requester* or holder of the *Electronic Time Stamp* has been notified of these circumstances.
- Not allow *Electronic Time Stamps* to serve as a time reference beyond the limits of use established for them in their corresponding policies.

13.4.2.3. Obligations of the relying parties

59. The parties that place their trust in an *Electronic Time Stamp* issued by the FNMT-RCM have the obligation to:

- In general, follow the procedures and guidelines set out in these Policies and Practices for the *Qualified Time Stamping Service.*
- Prior to depositing their trust in the *Electronic Time Stamps*, they should
    1) Verify that the *Electronic Stamp* that accompanies the *Electronic Time Stamps* has been issued by the FNMT-RCM and no other party, and that it is correct.
    2) Check the validity of the *Certificates* employed for the issuance of the *Electronic Time Stamp* in question, through the procedures indicated in the Individual Certification Policies and Practices corresponding to the *Certificates* to be validated.
- Accept the *Electronic Time Stamps* within the limits and scope described in these Policies and Practices for the *Qualified Time Stamping Service*.

13.5. MANAGING THE LIFE CYCLE OF THE PASSWORDS OF THE TRUSTED SERVICE PROVIDER

60. With the aim of providing the *Qualified Time Stamping Service,* the FNMT-RCM takes responsibility for managing the corresponding passwords, in accordance with the provisions of the section "Managing the life cycle of the passwords of the Trusted Service Provider " of the [TSPS].

61. *Electronic Time Stamps* issued under this policy are *stamped* by specific *Certificates*, which have in turn been issued under the *Chain of Certification* of the *Certification Authority* rooted in the CN=AC RAIZ FNMT-RCM.

62. To obtain more information about the aforementioned *Chain of Certification* from the *Certification Authority*, consult the "Chains of Certification" section of the [TSPS].

63. The *Seal creation data* from the *Time Stamp* unit are linked to the following *Certificate.*

14. TSU CERTIFICATE

64. The *Qualified Time Stamping Service* will use the following *TSU Electronic certificates* in accordance with the European standard ETSI EN 319 411-1:

1. TSU electronic certificate with the policy OID 1.3.6.1.4.1.5734.3.9.20, issued with the *Certification Authority* "AC Componentes Informáticos". This *Certificate* and the particular certification practices and policies of the Certification Authority "AC Componentes Informáticos" are available for download and consultation at http://www.ceres.fnmt.es/dpcs.

   - The characteristics of this *Certificate* are as follows:

     Subject: CN = AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016, organizationIdentifier = VATES-Q2826004J, OU = CERES, O = FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA, C = ES

     Issuer: "AC Componentes Informáticos"

     Algorithm and length of the key: RSA 3072

     Validity: 6 years. Until November 25, 2022.

     Period of use of the *Private key*: 5 years. Until November 25, 2021.

2. TSU electronic certificate with the policy OID 1.3.6.1.4.1.5734.3.18.1, issued with the Certification Authority "AC Unidades de Sellado de Tiempo". This Certificate and the particular certification practices and policies are included in the *DGPC* which are available for download and consultation at http://www.ceres.fnmt.es/dpcs.

   - The characteristics of this *Certificate* are as follows:

     Subject: CN=AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2020, organizationIdentifier=VATES-Q2826004J, OU=CERES, O=FNMT-RCM, C=ES

     Issuer: "AC Unidades de Sellado de Tiempo"

     Algorithm and length of the key: RSA 3072

     Validity: 5 years. Until June 19, 2025.

     Period of use of the Private key: 4 years. Until June 19, 2024.

65. The mentioned TSU *Electronic certificates* includes, following the recommendations of ETSI EN 319 421 and ETSI EN 319 422, the extension privateKeyUsage, which limits the use of the *Private Key* by setting an expiration date prior to the *Public key*, so as to ensure sufficient time for the renewal of the seals issued by a TSU prior to the expiration of its certificate.

66. The *Seal creation data* from the *Time Stamp Unit* are linked to the *Certificate* from the *Time Stamping Authority*, in accordance with standard X.509, version 3, whose profile may be consulted on the website: http://www.cert.fnmt.es/dpcs/.

15. PRACTICES OF THE QUALIFIED TIME STAMP SERVICE

15.1. PROVISION AND AVAILABILITY OF THE QUALIFIED TIME STAMPING SERVICE

67. The issuance of *Electronic Time Stamps* shall be performed upon request by a *User entity*. When a User Entity wishes to obtain an *Electronic Time Stamp* for an electronic document, it will calculate a value or set of hash values from it. This produces a small but compact quantity of information that is sent to the FNMT–RCM so that it can issue the corresponding *Electronic Time Stamp*.

68. This *Electronic Time Stamp* will link the data received to the date and time of receipt, through the FNMT-RCM's *Electronic Stamp*.

69. It is worth noting that the FNMT-RCM decides whether the hash algorithm used to represent the data to be stamped is sufficiently secure in accordance with its service policies and if it is, it accepts the request for processing. Specifically, the following hash algorithms will be accepted:

- SHA-256
- SHA-384
- SHA-512

70. The FNMT-RCM does not perform any verification or treatment whatsoever of the representation of the data received to be stamped beyond including them in the *Electronic Time Stamp* itself and in the events registration systems. The FNMT-RCM does not verify, in any way, the contents or the truthfulness of the representation of the data to be stamped or its origin.

71. The *Qualified Time Stamping Service* shall be available twenty-four (24) hours a day, 365 days of the year, except in the case of extenuating circumstances that arise beyond the control of the FNMT-RCM and maintenance work. The FNMT-RCM shall notify users in the case of the latter circumstance at the following address: http://www.ceres.fnmt.es at least forty-eight (48) hours in advance and will try to resolve it in a period of no more than twenty-four (24) hours.

72. All *Time Stamp* requests and responses are managed in accordance with the provisions of recommendation number [RFC 3161].

15.2. REQUEST FOR AN ELECTRONIC TIME STAMP

73. In order to request an *Electronic Time Stamp,* a user must form part of the *Electronic Community* and be registered as a *User Entity.* It must also have signed the corresponding agreement with the FNMT-RCM to use the service.

74. Prior to submitting its requests, the *User Entity* must obtain a *Certificate* of those admitted by the FNMT-RCM for such purposes, which will be used as a mechanism for identifying and authenticating each *Time Stamp* request.

75. The *User Entity*, using the HTTPS protocol and authenticating itself with the aforementioned *Certificate*, will compose a *Time Stamp* request in accordance with recommendation [RFC 3161].

76. *Time Stamp* requests shall be sent to the address https://qtsa.cert.fnmt.es/ or https://qets.cert.fnmt.es encapsulated as Content-Type: application/timestamp-query, codified in DER and described in ASN.1 (Refer to [RFC 3161]).

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

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

`version` Integer. Describe the version of the request. It is currently version 1.

`messageImprint` Sequence. The structure that contains the hash of the document to be dated and the hash algorithm used.

`reqPolicy` Identifier of the policy that is requested to be applied in the provision of the service. It is optional and may be omitted, but in the event that it is used, it must contain the OID of the policy contained herein. In this case, the OID used is 0.4.0.2023.1.1 corresponding to the best-practices-ts-policy defined in the European standard ETSI EN 319 421.

`nonce` Integer. Optional random number used to connect the request with the response.

`certReq` Boolean. If its value is "True", it requires the TSA to include its certificate in the response.

`extensions` Sequence. Request extensions.

15.3. RESPONSE TO A TIME STAMP REQUEST

78. Responses to *Time Stamp* requests received from the address https://qtsa.cert.fnmt.es/ or https://qets.cert.fnmt.es encapsulated as Content-Type: application/timestamp-reply, codified in DER and described in ASN.1.

79. The content of the response takes an ASN.1 structure, in which the result of the operation (status) is included, in other words, whether the operation has been performed in a satisfactory way or not, and a CMSSignedData (timeStampToken) structure, in which the *Time Stamp* (TSTInfo) stamped by the *Time Stamping Authority* is included.

80. The *Certificate* from the *Time Stamping Authority* is issued by the CA with the following extension: id-kp-timestamping, which indicates that this certificate will be used exclusively for the purposes of issuing *Electronic Time Stamps.*

```
TimeStampResp ::= SEQUENCE {
```

```
status PKIStatusInfo,
timeStampToken OPTIONAL
}
```

`status` Sequence. Sequence in which, making use of three fields, the result of the operation is indicated in its entirety, a descriptive chain of the result and another descriptive chain, which is used in the event of error. If the result is not satisfactory, the timeStampToken field will not appear.

`timeStampToken` Sequenec. Signed structure of the CMSSignedData type, which includes the corresponding *Time Stamp* and *Electronic Time Stamp.* Includes the *Certificates* from the *Time Stamping Authority* and from the CA in the event that it has been asked for in the request.

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

`version` Describe the version of the response. It is currently version 1.

`policy` Identifier of the policy used to render the service, in other words, the policy contained herein corresponding to best-practices-ts-policy defined in the European standard ETSI EN 319 421 (OID 0.4.0.2023.1.1).

`messageImprint` Structure that contains the hash of the dated document and the hash algorithm used and sent by the client. Its value is exactly equal to that received in the request.

`serialNumber` Whole unique number assigned by the TSU to the *Time Stamp* generated.

`genTime` Time stamp assigned by the *Time Stamping Authority* . It includes the fractional term to the nearest millisecond. According to RFC 3161, fractional terms ending in zero are not included.

`accuracy` Indicates the precision of the time provided.

`ordering` False value. It will only be possible to order two *Time Stamps* when the difference between the two genTime exceeds the sum of the precisions of the two.

`nonce` Integer. Random number used to connect the request with the response. It must be present if it appeared in the request.

`tsa` TSA identifier, which ties with the subject of the certificate of the *Time Stamping Authority.*

`extensions` Response extensions. The QCStatements extension is included, thus identifying the *Electronic Time Stamp* as qualified, as specified in the ETSI standard EN 319 422.

81. *Electronic Time Stamps* issued under this policy are stamped electronically by the FNMT-RCM's *Seal creation data* making use of the following algorithms:

- SHA-256
- RSA 3072

15.4. VALIDATION OF THE ELECTRONIC TIME SEAL

82. In order to validate a time stamp, the relying parties shall verify the *Electronic seal* that accompanies the *Electronic Time Stamps* by making use of the "messageImprint" field described in the previous section, as well as the valid status of the TSU *Certificate* through *Information and consultation service on the state of validity of the certificates* (OCSP protocol) in accordance with the procedures indicated in the particular Certification Policies and Practices corresponding to said Certificate (Particular Certification Policies and Practices of the Component Certificates "AC Componentes Informáticos"), which can be consulted at www.cert.fnmt.es/dpcs.

16. AUDITS

83. In this section, the provisions of the *Trust Services Practices and Electronic Certification Statement* will apply, in addition to the rules described in this section.

84. The *Qualified Time Stamping Service* offered by the FNMT-RCM is subject to periodic audits, in accordance with the certification scheme for *Trusted Service Providers*, in terms of compliance with the requirements defined by the European standards ETSI EN 319 401 "General Policy Requirements for Trusted Service Providers", ETSI EN 319 421 "Trusted Service Providers issuing Time-Stamps" and ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles".

85. The audits referred to in the section above are performed on an annual basis by an organisation authorised for that purpose.

17. RATES

86. The FNMT-RCM will charge the Public Administrations the rates approved by the Under-Secretary, upon whom the provision of trusted services depends or, in their absence, the rates established in the agreement or management contract formalised for that purpose.

87. The tariffs that apply to the private sector are governed by the contract signed for the provision of the *Qualified Time Stamping Service.* In addition, the FNMT-RCM may establish rates and payment methods that it deems appropriate at any given time. Prices and payment terms can be found on the FNMT-RCM's website or can be provided by the corresponding sales team upon request by sending an email to the following address: comercial.ceres@fnmt.es.

88. The policy requirements defined in this document are not meant any restrictions on charging for *Qualified Time Stamping Service*.