

# CORPME TIME STAMPING PRACTICES AND POLICIES

## Trust Service Provider



**Information Systems Service**

June 30<sup>th</sup> 2023

**DOCUMENTAL CONTROL**

DOCUMENT / FILE	
<b>Title: CORPME Time Stamping Practices and Policies</b>	File/s name: REG-PKI-DPC04v.1.3.2 CORPME Time Stamping Practices and Policies.pdf
<b>Code: REG-PKI-DPC04</b>	Logical Support: MS-DOCX y PDF
<b>Date: 30/06/2023</b>	Physical location: <a href="http://pki.registradores.org/normativa/index.htm">http://pki.registradores.org/normativa/index.htm</a>
<b>Version: 1.3.2</b>	

**CHANGE RETENTION**

<b>Version</b>	<b>Date</b>	<b>Reason for change</b>
1.0.0	20/06/2016	Document creation
1.0.1	19/09/2016	Modification LFE/2016/0071
1.0.2	29/05/2017	Adaptation to eIDAS Regulation
1.1.0	26/06/2017	Adaptation as a result of audit according to ETSI standards
1.2.0	23/08/2017	Minor corrections
1.3.0	27/05/2019	Further detail about TSA Certificate contents. Definition of a bounded list of allowed hash algorithms used for timestamps requests.
1.3.1	12/03/2021	Update of the new law on trust services. Inclusion of time stamp verification methods.
1.3.2	30/06/2023	Acceptance of accepted hash algorithms and limitation of liability for their use.

# INDEX

<b>1</b>	<b>INTRODUCTION</b>	<b>6</b>
1.1	OVERVIEW	6
1.2	TIME STAMPING SERVICE	6
1.3	DEFINITIONS AND ABBREVIATIONS	7
1.3.1	<i>Definitions</i>	7
1.3.2	<i>Abbreviations</i>	7
1.3.3	<i>References</i>	8
<b>2</b>	<b>TIME STAMPING PRACTICES AND POLICIES</b>	<b>9</b>
2.1	INITIAL VIEW	9
2.2	TIME STAMPING PRACTICES AND POLICIES IDENTIFICATION	9
2.3	PARTICIPANT ENTITIES	10
2.3.1	<i>Trust Service Provider (TSP)</i>	10
2.3.2	<i>Time Stamping Authority (TSA)</i>	10
2.3.3	<i>Client</i>	10
2.3.4	<i>Third party who trust in time stamps</i>	11
<b>3</b>	<b>OPERATIONAL REQUIREMENTS</b>	<b>12</b>
3.1	OBTAINING RELIABLE TIME	12
3.2	TSA CERTIFICATE	12
3.2.1	<i>TSA Certificate Generation</i>	12
3.2.2	<i>TSA Certificate Publication</i>	14
3.2.3	<i>Changing TSA Certificate</i>	14
3.3	APPLYING FOR TIME STAMPS	15
3.4	RESPONSE TO TIME STAMPS REQUEST	15
3.5	VALIDATION OF TIME STAMPS	17
<b>4</b>	<b>PHYSICAL SECURITY CONTROLS</b>	<b>18</b>
4.1	PHYSICAL CONTROLS	18
4.1.1	<i>CORPME Facilities</i>	18
4.1.2	<i>Physical access</i>	18
4.1.3	<i>CORPME Facilities</i>	18
4.1.4	<i>Exposure to water</i>	18
4.1.5	<i>Measures against fires and floods</i>	18
4.1.6	<i>Storage system</i>	18
4.1.7	<i>Waste Disposal</i>	18
4.1.8	<i>Information Backup Policy</i>	18
4.2	PROCEDURAL CONTROLS	18
4.2.1	<i>Responsible Roles for CORPME PKI control and management</i>	19
4.2.2	<i>Number of persons required per task</i>	19
4.2.3	<i>Roles requiring segregation of functions</i>	19
4.3	PERSONNEL CONTROLS	19
4.3.1	<i>Requirement for professional qualifications, knowledge and experience</i>	19
4.3.2	<i>Background Check Procedures</i>	19
4.3.3	<i>Training requirements</i>	19
4.3.4	<i>Requirements and Frequency of Training Update</i>	19
4.3.5	<i>Frequency and rotation sequence of tasks</i>	19
4.3.6	<i>Penalties for unauthorized actions</i>	19

4.3.7	<i>Requirements for contracting third parties</i>	19
4.3.8	<i>Documentation provided to staff</i>	20
4.4	SECURITY AUDIT PROCEDURES	20
4.4.1	<i>Registered event types</i>	20
4.4.2	<i>Frequency of processing audit record</i>	20
4.4.3	<i>Audit records Retention period</i>	20
4.4.4	<i>Audit records protection</i>	20
4.4.5	<i>Procedures for supporting audit record</i>	20
4.4.6	<i>Notification to subject causing the event</i>	20
4.4.7	<i>Vulnerability analysis</i>	20
4.4.8	<i>Legal proceedings</i>	20
4.5	ARCHIVING RECORDS	20
4.5.1	<i>Archived events Types</i>	21
4.5.2	<i>Record retention period</i>	21
4.5.3	<i>File protection</i>	21
4.5.4	<i>File Backup Procedures</i>	21
4.5.5	<i>Requirements for time stamping of records</i>	21
4.5.6	<i>File information system (internal vs. external)</i>	21
4.5.7	<i>Procedures for obtaining and verifying archived information</i>	21
4.6	CHANGE OF KEYS	21
4.7	RECOVERY FROM KEY OR CATASTROPHIC COMMITMENT	21
4.7.1	<i>Incident and commitment management procedures</i>	21
4.7.2	<i>Alteration of Hardware, software and / or data resources</i>	21
4.7.3	<i>Procedures of action against the commitment of the authority private key</i>	23
4.7.4	<i>Installation after natural disaster or other catastrophe</i>	23
4.8	TSA TERMINATION	23
<b>5</b>	<b>TECHNICAL SECURITY CONTROLS</b>	<b>24</b>
5.1	COMPUTER SECURITY CONTROLS	24
5.1.1	<i>Specific technical security requirements</i>	24
5.1.2	<i>Computer security assessment</i>	24
5.2	LIFECYCLE SECURITY CONTROLS	24
5.2.1	<i>System Development Controls</i>	24
5.2.2	<i>Security Management Controls</i>	24
5.2.3	<i>Lifecycle security controls</i>	24
5.3	NETWORK SECURITY CONTROLS	24
<b>6</b>	<b>COMPLIANCE AUDITS AND OTHER CONTOLS</b>	<b>25</b>
6.1	FREQUENCY OR CIRCUMSTANCES OF CONTROLS FOR EACH AUTHORITY	25
6.2	AUDITOR IDENTIFICATION / QUALIFICATION	25
6.3	RELATIONSHIP BETWEEN AUDITOR AND AUDITED AUTHORITY	25
6.4	ASPECTS COVERED BY CONTROLS	25
6.5	ACTIONS TO BE TAKEN BECAUSE OF DEFICIENCIES DETECTION	25
6.6	RESULTS COMMUNICATION	25
<b>7</b>	<b>OTHER LEGAL AND ACTIVITY ISSUES</b>	<b>26</b>
7.1	RATES	26
7.1.1	<i>Time Stamping services rates</i>	26
7.1.2	<i>Refund Policy</i>	26
7.2	ECONOMIC RESPONSIBILITIES	26
7.3	CONFIDENTIALITY INFORMATION	26

7.3.1	<i>Confidential information scopes</i>	26
7.3.2	<i>No confidential information</i>	26
7.3.3	<i>Professional Secrecy Duty</i>	26
7.4	PERSONAL INFORMATION PROTECTION	26
7.5	INTELLECTUAL PROPERTY RIGHTS	27
7.6	REPRESENTATION AND WARRANTIES	27
7.6.1	<i>TSA Obligations</i>	27
7.6.2	<i>Obligation of time stamp clients</i>	27
7.6.3	<i>Obligations of third parties who trust in time stamps</i>	28
7.6.4	<i>Obligations of external organizations</i>	28
7.6.5	<i>Other participant obligations</i>	28
7.7	DISCLAIMER	28
7.8	LIMITATIONS OF RESPONSIBILITIES	28
7.9	INDEMNIFICATION	28
7.10	VALIDITY PERIOD	29
7.10.1	<i>Time Limit</i>	29
7.10.2	<i>Time Stamping Policy Replacement and repeal</i>	29
7.10.3	<i>Completion Effects</i>	29
7.11	INDIVIDUAL NOTIFICATIONS AND COMMUNICATIONS WITH PARTICIPANTS	29
7.12	SPECIFICATIONS CHANGES PROCEDURES	29
7.12.1	<i>Changes Procedures</i>	29
7.12.2	<i>Circumstances in which OID must be changed</i>	29
7.13	CLAIMS	29
7.14	APPLICABLE REGULATIONS	30
7.15	COMPLIANCE WITH APPLICABLE REGULATIONS	30
7.16	VARIOUS STIPULATIONS	30
7.16.1	<i>Full Acceptance Clause</i>	30
7.16.2	<i>Independence</i>	30
7.16.3	<i>Judicial resolution</i>	30
7.17	OTHER STIPULATIONS	30

# 1 INTRODUCTION

## 1.1 Overview

The Trust Service Provider (TSP) from the Public Corporation of Land and Business Registers of Spain, Colegio de Registradores de la Propiedad y Mercantiles de España (hereinafter CORPME), issues certificates qualified according to EU regulations 910/2014 related to electronic identification and trust services, according to Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, and also offers Time Stamping services.

This document aims to describe Time Stamping services operation offered by CORPME and to establish the use conditions, obligations and responsibilities for the different entities involved.

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, does not collect or regulate the issuance of time stamps. However, it is CORPME's intention to provide issued time stamps with the status of "Qualified Time Stamps" equivalent to the status of "Qualified Electronic Signatures complying with the applicable legislation in each case.

These Time Stamping Practices and Policies are subject to compliance with the General Conditions included in the CORPME Certification Practice Statement (CPS).

## 1.2 Time Stamping Service

Time Stamping is an online mechanism that allows to demonstrate that a data series have existed and have not been altered from a specific time.

The CORPME is a Time Stamping Authority (TSA or Time Stamping Authority) that acts as a trusted third party testifying existence of such electronic data at a specific date and time.

The Time Stamping services are not free, so it will be necessary to contract the service previously with the CORPME. Time Stamping services may be sell under the temporary limitation agreed upon and / or number of Time Stamping requests. In any case, the TSA's billing conditions are reviewed, guaranteeing that no additional charges are applied to those established in the contracts.

CORPME offers Time Stamping service as follows:

- **Time Stamping Service:** Client performs a Time Stamping request according to RFC 3161 to a CORPME URL, obtaining in response a digital evidence signed by CORPME TSA.

Time Stamping Practices and Policies implementation must comply with protocol defined in **RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"**.

The CORPME's TSA allows the generation of time stamps on any type of document or object, with or without electronic signature of any kind.

The steps to generate a time stamp are as follows:

- The client calculates the hash of the document or object to be stamped.
- The client sends a time stamp request to a specific CORPME URL following the protocol RFC 3161, including the hash of the document to be stamped.
- CORPME receives the request, checks whether the request is complete and correct and performs an access control based on the client's IP.

- If the result is correct, the TSA signs the request by generating a time stamp (including the hash of the document, the date and time obtained from a reliable source and the electronic signature of the TSA).
- The time stamp is sent back to the client.
- The client must validate the signature of the stamp and properly guard it.
- The TSA will maintain a record of the issued stamps for future verification for at least 5 years.

The CORPME records the following information regarding the Time Stamping Service:

- Relevant events of the TSU key life cycle.
- Relevant events in the life cycle of TSU certificates.
- TSU clock synchronization events with UTC, including clock recalibration information.
- Events related to synchronization loss detection.

## 1.3 Definitions and abbreviations

### 1.3.1 Definitions

- **Electronic signature qualified certificate:** Electronic signature certificate issued by a qualified provider of trusted services meeting the requirements of the Regulation (EU) 910/2014, Annex I.
- **Hardware Security Cryptographic Module (HSM):** Hardware module used to perform cryptographic functions and storing keys in safe mode.
- **Hash:** Fixed-size result obtained after applying a hash function to a message fulfilling the property of being uniquely associated with the initial data.
- **Qualified Certificate:** Certificate issued by a Trust Services Provider in compliance with the Law in terms applicant's identity and other circumstances verification as well as reliability and guarantees of the services they provide.
- **Revoked Certificate Lists:** List of revoked or suspended certificates.
- **Time stamp:** Special type of electronic signature issued by a trusted third party who guarantees the integrity of a document at a certain date and time.
- **Time Stamping Authority:** A trusted entity who emits time stamps.
- **Trust Service Provider:** Natural or Legal person, who, in accordance with the legislation on Electronic Signature, issues Electronic Certificates, is also able to provide other services in relation to the Electronic Signature.

### 1.3.2 Abbreviations

**CRL:** Certificate Revocation List.

**CWA:** CEN Workshop Agreement.

**FIPS:** Federal Information Processing Standards.

**HSM:** Hardware Security Module. Cryptographic security module used for key storage and safe cryptographic operations.

**IETF:** Internet Engineering Task Force (Internet Standardization Organization).

**RFC:** Request For Comments. Standard developed by the IETF.

**ROA:** Real Observatorio de la Armada Española(Royal Observatory of the Spanish Navy).

**TSA:** Time Stamping Authority.

**TSC:** Time Stamping Certificate.

**TSP:** Time Stamping Protocol.

**TST:** Time Stamp Token.

**TSU:** Time Stamping Unit.

**UTC:** Universal Time Coordinated.

### 1.3.3 References

- **ETSI EN 319 401** – General Policy Requirements for Trust Service Providers.
- **RFC 3161** – Internet x.509 Public Key Infrastructure – Time Stamp Protocol (TSP).
- **RFC 3628** – Policy Requirements for Time Stamping Authorities (TSAs).
- **ETSI EN 319 421** – Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- **ETSI EN 319 422** – Time-stamping protocol and time-stamp token profiles.



## 2 TIME STAMPING PRACTICES AND POLICIES

### 2.1 Initial view

The Time Stamping services are not free, so it will be necessary to contract service previously with the CORPME. Time Stamping services may be sell under the temporary limitation and / or time-stamping number requests to be agreed upon.

The CORPME offers the Time Stamping Service as follows:

- **Time Stamping Service:** Client performs a Time Stamping request according to RFC 3161 to a CORPME URL (<http://tsa.registradores.org> or <https://tsa.registradores.org>) obtaining in response a digital evidence signed by CORPME TSA.

CORPME Time Stamping Practices and Policies are based on standards:

- CWA 14167 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements.
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers.
- RFC 3161 – Internet x.509 Public Key Infrastructure – Time Stamp Protocol (TSP).
- RFC 3628 – Policy Requirements for Time Stamping Authorities (TSAs).
- ETSI EN 319 421 – Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 – Time-stamping protocol and time-stamp token profiles.

### 2.2 Time Stamping Practices and Policies Identification

<b>Document's name</b>	CORPME Time Stamping Practices and Policies
<b>Document's version</b>	1.3.2
<b>Document status</b>	Version
<b>Emission Date</b>	30/06/2023
<b>Expiration date</b>	Not applicable
<b>OID (Object Identifier)</b>	1.3.6.1.4.1.17276.0.3.3.1
<b>CP Location</b>	<a href="http://pki.registradores.org/normativa/index.htm">http://pki.registradores.org/normativa/index.htm</a>
<b>Related CPS</b>	Certification Practice Statement

CORPME Time Stamping Practices and Policies are compliant with the standard ETSI EN 319 421.

The TSA is composed of a single Time Stamping Unit (TSU) that issues the time stamps in accordance with BTSP time stamping policy (OID 0.4.0.2023.1.1) described in ETSI EN 319 421.

## 2.3 Participant entities

### 2.3.1 Trust Service Provider (TSP)

According to Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, Natural or Legal person who, in accordance with the legislation on Electronic Signature, issues Electronic Certificates, is able to also provide other services in relation to the Electronic Signature.

### 2.3.2 Time Stamping Authority (TSA)

The CORPME acts as a Time Stamping Authority (TSA). The CORPME will offer the time stamping services only through the TSP, without delegating them to any other entity.

TSA provides certainty about pre-existence of certain electronic documents at any given time.

CORPME will use different systems to generate time stamps, providing high availability to the service.

### 2.3.3 Client

The CORPME Time Stamping services are not public or free. To be able to access the Time Stamping services, the Client must contract previously with the CORPME.

The CORPME will perform access control to the service based on IP addresses, therefore, the Client must inform on which IP addresses requests will be made.

The client must adapt their systems to the TSP protocol in order to make time-stamping requests. The time-stamping service offered by CORPME does not provide any software or customer integration libraries. To adapt systems, there are public libraries that implement TSP protocol in various programming languages:

- **BouncyCastle** (<http://www.bouncycastle.org>): Set of cryptographic libraries that implement the TSP protocol in Java and C #
- **OpenSSL TS** (<https://www.openssl.org>): OpenSSL cryptographic library module that implements TSP protocol in C language.
- **Digistamp** (<http://digistamp.com/toolkitDoc/MSToolKit.htm>): Toolkit based on the Microsoft CryptoAPI cryptographic library those implements the TSP protocol in Visual Basic.
- **IAIK**: Includes cryptographic libraries in Java that implement the TSP protocol. These libraries are free for non-commercial purposes only.
- **Adobe Reader**: The Adobe Reader 8 application allows the validation of time stamps included in PDF documents.

### 2.3.4 Third party who trust in time stamps

Neither Electronic Identification, EU 910/2014 nor Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza collect nor regulate time stamps issuance. However, it is CORPME's intention to endow the issued time stamps with the status of "Qualified Time Stamps" equivalent to the status of "Qualified Electronic Signatures", complying with the applicable legislation in each case.

Therefore, any user may validate the time stamps freely based on trust in the CORPME as a TSP who issues qualified certificates.

## 3 OPERATIONAL REQUIREMENTS

### 3.1 Obtaining Reliable Time

The CORPME performs time synchronization with the ROA through the Internet Protocol NTP (*RFC 1305 Network Time Protocol*). The ROA has as main mission the time basic unit maintenance, declared for legal purposes as National Pattern, as well as the maintenance and official dissemination of The Coordinated Universal Time (UTC) scale, considered for all purposes as the basis of the legal time throughout the national territory (RD 23 October 1992, No. 1308/1992).

To perform this time synchronization, a research project is established by means of the constitution of a Time Laboratory at the headquarters of the ROA where the quality of time is obtained, processed and controlled by electronic means and sent through a channel of exclusive communication to the Information Systems Service of the CORPME, and from where it is distributed.

The CORPME TSA provides one-second accuracy.

### 3.2 TSA Certificate

#### 3.2.1 TSA Certificate Generation

The process of issuing a Certificate of Time Stamping Certificate (TSC) will be carried out manually following the maximum security guarantees.

Time Stamp Certificate (TSC) is issued and revoked by Central Processing Unit, by a Steering Committee request.

The CORPME Internal Subordinate CA must issue the TSA certificate, following the certification policy.

The structure of the certificate, referring to certificate *Subject* field, is the one described in the following table:

Field	Value	Description
C	ES	Country.
organizationIdentifier	VATES-Q2863012G	NIF (Required by ETSI 319 412-2).
O	Colegio de Registradores de la Propiedad y Mercantiles	Organization.
CN	Autoridad de Certificación de los Registradores - TSA – 01	Common Name.

These are the CORPME TSA X.509 v3 certificate fields and extensions:

Field / Extension	Content	Critical	Observations
<b>Version</b>	v3		
<b>Serial Number</b>	4d6ed20347f836b95cd01767dd43f241		
<b>Signature Algorithm</b>	sha256WithRSAEncryption		OID: <b>1.2.840.113549.1.1.11</b> Standard PKCS#1 v2.1 y RFC 3447.
<b>Issuer</b>	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		All <i>DirectoryString</i> coded in UTF8. Attribute "C" ( <i>countryName</i> ) is coded according "ISO 3166-1-alpha-2 code elements", in <i>PrintableString</i> .
<b>Valid From</b>	Monday, May 6th of 2019 13:15:51		Validity period Start date.
<b>Valid To</b>	Friday, May 6th of 2022 13:15:51		End date of the validity period.
<b>Subject</b>	CN = Autoridad de Certificación de los Registradores - TSA - 01 O = Colegio de Registradores de la Propiedad y Mercantiles organizationIdentifier = VATES-Q2863012G C = ES		All <i>DirectoryString</i> coded in UTF8. Attribute "C" ( <i>countryName</i> ) is coded according "ISO 3166-1-alpha-2 code elements", in <i>PrintableString</i> . The attribute <i>SerialNumber</i> will be coded in <i>PrintableString</i> .
<b>Subject Public Key</b>	Algorithm: RSA Encryption Length: 2048 bits		
<b>Subject Key Identifier</b>	Function hash sha1 for the subject public key	NO	
<b>Authority Key Identifier</b>	Function hash sha1 for the AC public key issuer	NO	
<b>Certificate Policies</b>	It will be used		
- Policy Identifier	1.3.6.1.4.1.17276.0.1.10.1		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	<a href="http://pki.registradores.org/normativa/index.htm">http://pki.registradores.org/normativa/index.htm</a>	NO	
-- Policy Qualifier Id (User Notice)	Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Field coded in UTF8.

<b>Subject Alternative Name</b>	No utilizado	NO	
<b>CRL Distribution Points</b>	<p>(1) <b>HTTP:</b>  <a href="http://pki.registradores.org/crls/crl_int_psc_corpme.crl">http://pki.registradores.org/crls/crl_int_psc_corpme.crl</a></p> <p>(2) <b>LDAP:</b>  ldap://ldap.registradores.org/  CN=AC%20INTERNA,  O=Colegio%20de%20Registradores%  20-%20Q2863012G,  C=ES?certificateRevocationList?base  ?objectclass=cRLDistributionPoint</p>	NO	The latest versions of Microsoft CryptoAPI do not support either HTTP or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
<b>Authority Information Access (AIA)</b>	<p><b>Access Method:</b> id-ad-ocsp  <b>Alternative Name (Access Location):</b>  <a href="http://ocsp.registradores.org/">http://ocsp.registradores.org/</a></p> <p><b>Access Method:</b> id-ad-calssuers  <b>Alternative Name (Access Location)</b>  (AC Subordinada Interna):  <a href="http://pki.registradores.org/certificados/a_c_int_psc_corpme.crt">http://pki.registradores.org/certificados/a_c_int_psc_corpme.crt</a></p>	NO	The latest versions of Microsoft CryptoAPI do not support either HTTPS or LDAPS. Therefore, the HTTP and LDAP protocols will be used.
<b>Key Usage</b>	Digital Signature Non Repudiation	YES	
<b>ExtendedKey Usage</b>	Time Stamping (1.3.6.1.5.5.7.3.8)	YES	

The TSU private keys are generated and guarded in a secure cryptographic device meeting requirements detailed in FIPS 140-3 level 3 and FIPS 140-2 level 3 where applicable, ensuring compliance with the requirements of the EAL4 + in accordance with ISO / IEC 15408. The cryptographic device is not handled during transport or when stored.

In the case of a possible TSU algorithm or key size weakness, its certificate will be revoked, new TSU keys will be generated with a more secure algorithm and key size, and a new TSA certificate will be issued.

CORPME has several servers to guarantee the high time-stamping service availability. It also reserves the right to establish as many time-stamping units as deemed appropriate and their management according to the particular procedures established to guarantee at all times the adequate provision of the service.

At the end of the validity period, TSU private keys and their backups are safely destroyed when they are removed from the device, so that they cannot be recovered, in order to avoid their inappropriate use

### 3.2.2 TSA Certificate Publication

The TSA certificate is attached to the response of each Time Stamp that is issued.

### 3.2.3 Changing TSA Certificate

The TSA certificate may be changed at any time by another TSA certificate equally valid under the CORPME Certification Policies.

This change will not be communicated to the users of the service, who should trust all the stamps issued by CORPME and signed with valid TSC certificates within the certification hierarchy.

Therefore, a user only needs to rely on the CA Root certificate and the CORPME CAs to validate the signatures.

### 3.3 Applying for time stamps

Stamp applications will adhere to the syntax of "RFC3161 Time Stamp Protocol (TSP)" specification described in Section 2.4.1.

According to CORPME, the URLs of the Time Stamping Service may be: <http://tsa.registradores.org> or <https://tsa.registradores.org>.

In line with the best security practices, the use of the following HASH algorithms is recommended to guarantee the integrity of the sealed documents in the long term.

- SHA-224
- SHA-256
- SHA-384
- SHA-512
- SHA3-256
- SHA3-384
- SHA3-512

However, CORPME does not impose any specific restriction on the HASH algorithms used by applicants. It is the responsibility of the applicants to select the algorithm they consider most appropriate, and CORPME is not responsible for any type of incident related to the security of the chosen HASH algorithm.

The format for sending the requests follows the following scheme:

```
TimeStampReq ::= SEQUENCE {
    Version INTEGER { v1(1) },
    messageImprint MessageImprint,
    reqPolicy TSAPolicyId OPTIONAL,
    nonce INTEGER OPTIONAL,
    certReq BOOLEAN DEFAULT FALSE,
    extensions [0]IMPLICIT Extensions OPTIONAL }
```

```
MessageImprint ::= SEQUENCE {
    hashAlgorithm AlgorithmIdentifier,
    hashedMessage OCTET STRING }
```

### 3.4 Response to time stamps request

The response format is as follows:

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

```

PKIStatusInfo ::= SEQUENCE {
    status          PKIStatus,
    statusString    PKIFreeText OPTIONAL,
    failInfo        PKIFailureInfo OPTIONAL
}
PKIStatus ::= INTEGER {
    granted (0),
    grantedWithMods (1)
    rejection (2),
    waiting (3),
    revocationWarning (4),
    revocationNotification (5)
}
PKIFailureInfo ::= BIT STRING {
    badAlg (0),
    badRequest (2),
    badDataFormat (5),
    timeNotAvailable (14),
    unacceptedPolicy (15),
    unacceptedExtension (16),
    ddInfoNotAvailable (17)
    ystemFailure (25)
}
TimeStampToken ::= ContentInfo
    -- contentType is id-signedData as defined in [CMS]
    -- content is SignedData as defined in([CMS])
    -- eContentType within SignedData is id-ct-TSTInfo
    -- eContent within SignedData is TSTInfo

id-ct-TSTInfo OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}

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 }

```

### 3.5 Validation of time stamps

To validate a time stamp, the relying parties will verify the Electronic Stamp that accompanies the electronic Time Stamps using the “messageImprint” field described in the previous section, as well as the validity status of the TSU Certificate that can be verified. Through the two certificate validation mechanisms that CORPME makes available to users, through the consultation of the Certificate Revocation Lists (CRLs) or through the information service and consultation of the status of the certificates (protocol OCSP).

In addition, it must be verified that the hash contained in the time stamp matches the one that was sent and the correctness of the digital signature of the time stamp.

## **4 PHYSICAL SECURITY CONTROLS**

### **4.1 Physical controls**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.1.1 CORPME Facilities**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.1.2 Physical access**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.1.3 CORPME Facilities**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.1.4 Exposure to water**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.1.5 Measures against fires and floods**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.1.6 Storage system**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.1.7 Waste Disposal**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.1.8 Information Backup Policy**

As specified in CORPME Certification Practice Statement (CPS).

### **4.2 Procedural controls**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.2.1 Responsible Roles for CORPME PKI control and management**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.2.2 Number of persons required per task**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.2.3 Roles requiring segregation of functions**

As specified in CORPME Certification Practice Statement (CPS).

### **4.3 Personnel controls**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.3.1 Requirement for professional qualifications, knowledge and experience**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.3.2 Background Check Procedures**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.3.3 Training requirements**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.3.4 Requirements and Frequency of Training Update**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.3.5 Frequency and rotation sequence of tasks**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.3.6 Penalties for unauthorized actions**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.3.7 Requirements for contracting third parties**

As specified in CORPME Certification Practice Statement (CPS).

### **4.3.8 Documentation provided to staff**

As specified in CORPME Certification Practice Statement (CPS).

## **4.4 Security Audit Procedures**

As specified in CORPME Certification Practice Statement (CPS).

### **4.4.1 Registered event types**

As specified in CORPME Certification Practice Statement (CPS).

### **4.4.2 Frequency of processing audit record**

As specified in CORPME Certification Practice Statement (CPS).

### **4.4.3 Audit records Retention period**

As specified in CORPME Certification Practice Statement (CPS).

### **4.4.4 Audit records protection**

As specified in CORPME Certification Practice Statement (CPS).

### **4.4.5 Procedures for supporting audit record**

As specified in CORPME Certification Practice Statement (CPS).

### **4.4.6 Notification to subject causing the event**

As specified in CORPME Certification Practice Statement (CPS).

### **4.4.7 Vulnerability analysis**

As specified in CORPME Certification Practice Statement (CPS).

### **4.4.8 Legal proceedings**

As specified in CORPME Certification Practice Statement (CPS).

## **4.5 Archiving records**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.5.1 Archived events Types**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.5.2 Record retention period**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.5.3 File protection**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.5.4 File Backup Procedures**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.5.5 Requirements for time stamping of records**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.5.6 File information system (internal vs. external)**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.5.7 Procedures for obtaining and verifying archived information**

As specified in CORPME Certification Practice Statement (CPS).

### **4.6 Change of keys**

The procedures for providing a new TSA public key in the event of a key change are the same as providing the current public key.

### **4.7 Recovery from key or catastrophic commitment**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.7.1 Incident and commitment management procedures**

As specified in CORPME Certification Practice Statement (CPS).

#### **4.7.2 Alteration of Hardware, software and / or data resources**

As specified in CORPME Certification Practice Statement (CPS).



### 4.7.3 Procedures of action against the commitment of the authority private key

In the event of compromise of private key of the TSA, it will proceed to immediate revocation. Next, the corresponding CRL will be generated and published, ceasing the operation of the TSA activity and proceeding to the generation, certification and start-up of a new Authority with the same name as the one eliminated and with a new key pair.

### 4.7.4 Installation after natural disaster or other catastrophe

As specified in CORPME Certification Practice Statement (CPS).

## 4.8 TSA Termination

Before the TSA ceases its activity, the following actions will be carried out:

- Inform all subscribers, users or entities with whom it has agreements or other type of relation, of the cessation with the minimum anticipation of 2 months, or the period established by the current legislation.
- Revoke any authorization to subcontractors to act on behalf of the TSA in the time stamp issuance procedure.
- Inform the competent administration, in advanced, of the cessation of its activity and the destination to be given to the time stamps issued to date, specifying, if applicable, if the management is to be transferred and to whom.
- It will keep the TSA certificate active, as well as the verification system (Validation Authority) and revocation until the expiration of the certificate itself.
- It will process the revocation of the TSA certificate.
- It will destroy or disable the private keys of the TSA certificate, including their backup copies, in such a way that they cannot be recovered.
- It will forward to the Ministry of Industry, Commerce and Tourism, prior to the definitive cessation of its activity, the information related to the TSA certificate whose validity has expired so that it can take charge of its custody.

In the event of transfer of the activity to another TSA, CORPME:

- It will publish the transfer agreements and an explanatory document of the conditions that will regulate the relations between the subscriber and the PSC to which the certificates are transferred. This communication will be made by any means that guarantees the sending and receipt of the notification, with a minimum notice of two (2) months before the cessation of its activity, or the period established by current legislation.
- It will transfer all important databases, files, documents, event and audit records to the designated entity within 24 hours of its completion, or the period established by current legislation.
- It will transfer the obligation to make available to subscribers, users or entities the public information necessary for the provision of services, such as the public key of the certificates.

## **5 TECHNICAL SECURITY CONTROLS**

### **5.1 Computer security controls**

#### **5.1.1 Specific technical security requirements**

As specified in CORPME Certification Practice Statement (CPS).

#### **5.1.2 Computer security assessment**

As specified in CORPME Certification Practice Statement (CPS).

### **5.2 Lifecycle security controls**

#### **5.2.1 System Development Controls**

As specified in CORPME Certification Practice Statement (CPS).

#### **5.2.2 Security Management Controls**

As specified in CORPME Certification Practice Statement (CPS).

#### **5.2.3 Lifecycle security controls**

As specified in CORPME Certification Practice Statement (CPS).

### **5.3 Network Security Controls**

As specified in CORPME Certification Practice Statement (CPS).



## **6 COMPLIANCE AUDITS AND OTHER CONTROLS**

### **6.1 Frequency or circumstances of controls for each Authority**

As specified in CORPME Certification Practice Statement (CPS).

### **6.2 Auditor Identification / Qualification**

As specified in CORPME Certification Practice Statement (CPS).

### **6.3 Relationship between auditor and audited authority**

As specified in CORPME Certification Practice Statement (CPS).

### **6.4 Aspects covered by controls**

As specified in CORPME Certification Practice Statement (CPS)..

### **6.5 Actions to be taken because of deficiencies detection**

As specified in CORPME Certification Practice Statement (CPS).

### **6.6 Results Communication**

As specified in CORPME Certification Practice Statement (CPS).

## **7 OTHER LEGAL AND ACTIVITY ISSUES**

### **7.1 Rates**

#### **7.1.1 Time Stamping services rates**

Time Stamping services are not free, so it will be necessary to contract the service previously with CORPME. Time Stamping services may be marketed under the temporary limitation agreed upon and/or number of time stamping requests. In any case, the TSA's billing conditions are reviewed, guaranteeing that no additional charges are applied to those established in the contracts.

#### **7.1.2 Refund Policy**

The Time Stamping Service will be reimbursed under the conditions established in each type of contract.

### **7.2 Economic Responsibilities**

Not applicable because it is not a qualified certificates issuance service according to the stipulated in the Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. The TSA is not liable in case of transaction losses.

### **7.3 Confidentiality information**

As specified in CORPME Certification Practice Statement (CPS).

#### **7.3.1 Confidential information scopes**

As specified in CORPME Certification Practice Statement (CPS).

#### **7.3.2 No confidential information**

As specified in CORPME Certification Practice Statement (CPS).

#### **7.3.3 Professional Secrecy Duty**

As specified in CORPME Certification Practice Statement (CPS).

### **7.4 Personal Information Protection**

As specified in CORPME Certification Practice Statement (CPS).

## 7.5 Intellectual Property Rights

As specified in CORPME Certification Practice Statement (CPS).

## 7.6 Representation and Warranties

### 7.6.1 TSA Obligations

The CORPME, acting as Time Stamping Authority (TSA) is obliged to:

- Respect the provisions of these Time Stamping Practices and Policies.
- Protect private keys securely.
- Issuance of time stamps in accordance with these Practices and Policies and the application standards.
- Ensure the time and date included in the stamps are kept within the precision margins of the temporary reference provided by ROA, not exceeding a maximum of 1 (one) second deviation.
- Issuance of time stamps according the information sent by the customer without data entry errors.
- Issuance of time stamps including the minimum content defined by current legislation, when applicable.
- Publishing these Time Stamping Practices and Policies.
- Report on changes to these Time Stamping Practices and Policies to customers and third parties who rely on time stamps.
- Establish mechanisms for the relevant information generation and custody in the activities described, protecting them from loss, destruction or falsification.
- Guard the time stamps issued for the clients who contract the service during 5 years.
- Do not issue time stamps in the event of a compromise of service operations, including key compromise, loss of calibration or timing accuracy, and timing failure of watches.

The CORPME, in the provision of certification services, will be responsible for non-compliance with the provisions of these Time Stamping Practices and Policies and, where applicable, pursuant to Ley 59/2003, de 19 de diciembre, de firma electrónica or related normative.

Notwithstanding the foregoing, the CORPME will neither guarantee the cryptographic algorithms and standards used nor be liable for damages caused by external attacks, provided that it has applied due diligence according to the state of the art at any time, and acted in accordance with TSA Practices and Policies and current legislation, where applicable.

### 7.6.2 Obligation of time stamp clients

The client shall be bound to comply with the provisions of the regulations and in addition to:

- Respect the contractual documents signed with TSA.
- Verify time stamp the digital signature correctness and validity of the TSA certificate at the time of signing it.
- Verify that hash contained in the time stamp matches the one that was sent.
- Storage and conservation of time stamps delivered by the TSA. It is the Client's responsibility to store the time stamps, if he/she anticipates they will be necessary in the future.

### **7.6.3 Obligations of third parties who trust in time stamps**

It shall be the obligation of the users to comply with the provisions of current regulations and:

- Verify time stamp signature correctness and TSA certificate validity at the time of signing it.

### **7.6.4 Obligations of external organizations**

As specified in CORPME Certification Practice Statement (CPS).

### **7.6.5 Other participant obligations**

As specified in CORPME Certification Practice Statement (CPS).

## **7.7 Disclaimer**

The CORPME will not be responsible in any case in any of these circumstances:

- State of War, natural disasters, malfunction of electrical services, telematics and / or telephone networks or computer equipment used by the client or third parties, or any other case of force majeure.
- For improper or fraudulent use of time stamps.
- For the improper use of the information contained in the Certificate or in the CRL.
- For the content of stamped messages or documents.
- In relation to actions or omissions of the client.
- Information veracity lack in information provided to issue the stamp.
- Negligence in the preservation of access data to the Time Stamp Service, in the assurance of the confidentiality and in the protection of all access or disclosures.
- Excessive use of the time stamp, as provided in current regulations and in these TSA Practices and Policies.
- In relation to actions or omissions of the user, third party who relies on the certificate.
- Failure to check the suspension or loss of validity of the TSA electronic certificate published in consultation service regarding the validity of the certificates or lack of verification of the electronic signature.

## **7.8 Limitations of Responsibilities**

As specified in CORPME Certification Practice Statement (CPS).

## **7.9 Indemnification**

As specified in CORPME Certification Practice Statement (CPS).

## **7.10 Validity Period**

### **7.10.1 Time Limit**

This Practices and Policies document will come into effect from the moment of its publication in the CORPME's web directory and will be in force as long as it is not expressly revoked by the issuance of a new version.

### **7.10.2 Time Stamping Policy Replacement and repeal**

These Practices and Policies will be replaced by a new version regardless of the significance of the changes made in it, so that it will always be fully applicable.

When these Practices and Policies is revoked, it will be removed from the CORPME web directory, although it will be kept for fifteen (15) years.

### **7.10.3 Completion Effects**

The obligations and restrictions established by these Practices and Policies, in reference to audits, confidential information, obligations and responsibilities of the CORPME TSP, born under its validity, will survive after its replacement or repeal by a new version in everything in which it does not oppose this one.

## **7.11 Individual notifications and communications with participants**

As specified in CORPME Certification Practice Statement (CPS).

## **7.12 Specifications Changes Procedures**

### **7.12.1 Changes Procedures**

As specified in CORPME Certification Practice Statement (CPS).

### **7.12.2 Circumstances in which OID must be changed**

As specified in CORPME Certification Practice Statement (CPS).

## **7.13 Claims**

As specified in CORPME Certification Practice Statement (CPS).

## 7.14 Applicable regulations

The operations of the CORPME TSP, as well as Time Stamping Practices and Policies, will be subject to the applicable regulations, specially:

- 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.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

## 7.15 Compliance with applicable regulations

The Policy Approval Authority has the responsibility to ensure compliance with the applicable legislation contained in the previous section

## 7.16 Various Stipulations

### 7.16.1 Full Acceptance Clause

All Third Parties that Trust fully assume the content of the latest version of these Practices and Policies.

### 7.16.2 Independence

In the event that any of the sections contained in these Practices and Policies are declared, partially or totally, void or illegal, it will not affect this circumstance to the rest of the document.

### 7.16.3 Judicial resolution

The disputing party to CORPME shall communicate all claims between users and CORPME, in order to attempt to resolve it between the same parties.

For the resolution of any conflict that may arise in relation to these Practices and Policies, the parties, with waiver of any other jurisdiction that may correspond, are submitted to the Spanish Courts and Tribunals, regardless of where they were used the certificates issued.

## 7.17 Other Stipulations

As specified in CORPME Certification Practice Statement (CPS).