CORPME TRUST SERVICE PROVIDER

TIME STAMPING SERVICE
TSA DISCLOSURE STATEMENT

This document constitutes an extract of the rights and obligations contained in Time Stamping Practices and Policies of the Colegio de Registradores de la Propiedad y Mercantiles de España, CORPME, The Public Corporation of Land and Business Registers of Spain (hereinafter CORPME) and applies to the **Time Stamping Service.** This Disclosure Statement summarize Time Stamping Practices and Policies published.

The legal effects of the service, as well as the related rights and obligations, will be interpreted in all cases according to the current legislation, Time Stamping Practices and Policies in the version allocated in the following URL: http://pki.registradores.org/normativa/index.htm.

Before making use of the service, it is recommended to read this Disclosure Statement, in order to assess the trust offered by it. Ignorance of this Disclosure Statement may not be claimed to exempt from the responsibilities or to require them elsewhere.

1. Trust service provider contact Information

Colegio de Registradores de la Propiedad y Mercantiles de España.

Prestador del Servicio de Certificación del CORPME.

C/ DIEGO DE LEON, 21.

28006-MADRID

Teléfono: 902181442 / 912701699

Email: psc@registradores.org

Web: http://pki.registradores.org/normativa/index.htm

2. Time Stamping Service description

The 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.

Currently, the TSA is composed of a single Time Stamping Unit (TSU) that issues the time stamps under the policy with OID 1.3.6.1.4.1.17276.0.3.1.1 described in the Practices and Policies of Time Stamping.

The TSA is composed of a single Time Stamping Unit (TSU) that issues the time stamps under the policy with OID 1.3.6.1.4.1.17276.0.3.1.1, in accordance with BTSP time stamping policy (OID 0.4.0.2023.1.1) described in ETSI EN 319 421.

The TSA guarantees that the time and date included in the stamps remain within the margins of precision of the temporary reference provided by the Time Section of the Royal Institute and Observatory of the Navy in San Fernando, which in any case may exceed a maximum deviation of one second. Therefore, the CORPME TSA provides one-second accuracy.

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.

3. Limits of use

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 supported HASH algorithms are: SHA-224, SHA-256, SHA-384 and SHA-512, SHA3-256, SHA3-384, SHA3-512.

The Time Stampimg 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.

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 #
- **OpenTSA** (http://www.opentsa.org): OpenSSL cryptographic library extension 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.

Any signed documents related to rights and obligations for the participants in the CORPME TSP, as well as the associated audit records, shall be stored for a minimum period of fifteen (15) years.

The CORPME will use different systems to generate time stamps, providing high availability to the service. In addition, the certificate status information service, in its two variants (CRLs and OCSPs), is available 24 hours every day of the year, both for third parties who trust and for certificates holders or other parts require them.

4. *Obligations of the client*

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.

5. *Obligations of the third parties*

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.

6. *Limitations of liability*

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 Stamping 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. *Applicable agreements and Time Stamping Practices and Policies*

Time Stamping Practices and Policies, published at http://pki.registradores.org/normativa/index.htm, include the public information of the Terms and Conditions and characteristics of the certification services provided by the CORPME as TSP, containing the obligations and procedures in relation to the issuance of **Time Stamping Service.**

The activities that the CORPME may subcontract to carry out its activity as TSP are carried out contractually according to the CPS. In these cases, the access to the information owned by the CORPME follows the protocol defined in the Security Policy, in terms of the identification of risks, establishment of security controls to protect access formalizing confidentiality agreements and, if applicable, processing of personal data in compliance with current regulations.

8. Return Policy

The time stamp services will be reimbursed under the conditions established in each type of contract.

9. Applicable Law, claims and dispute resolution

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

➢ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

➢ 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 59/2003, de 19 de diciembre, de firma electrónica.

➢ Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

All claims between users and the CORPME shall be communicated by the disputing party to the CORPME, in order to attempt to resolve it.

For the resolution of any dispute regarding the provision of certification services, the parties are submitted to the Spanish courts and tribunals, regardless of where the certificates were issued.

10. Licensing and repository, trusted brands and audit

The CORPME, as TSP, maintains several accreditations and certifications for its trust services, especially remarkable for the Time Stamping Service:

➢ ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" y ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles".

The inclusion of qualified certificates issued by CORPME in the list of trusted service providers (TSL) in Spain can be checked through the following link:

https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.

In addition, the CORPME is registered as a qualified provider in the Ministry of Energy, Tourism and Digital Agenda:

http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/Prestadores.aspx.

In accordance with EU Regulation 910/2014, the CORPME will conduct biennial audits.

Madrid, June 2019.