Renewal of the Registrars Association PKI
Solution

Timestamping Policy

Version 1

Date: 27/10/2010
Page 1 of 20

Renewal of the Registrars Association PKI Timestamping Policy
<table>
<thead>
<tr>
<th>DOCUMENTARY CONTROL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOCUMENT/FILE</strong></td>
</tr>
<tr>
<td>Title: Timestamping Policies</td>
</tr>
<tr>
<td>Code:</td>
</tr>
<tr>
<td>Date: 27/10/2010</td>
</tr>
<tr>
<td>Version: Version 1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RECORD OF CHANGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
</tr>
<tr>
<td>Date:</td>
</tr>
<tr>
<td>1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DOCUMENT DISTRIBUTION LIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DOCUMENT CONTROL</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREPARED BY</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
CONTENTS

1. INTRODUCTION
   1.1. SUMMARY
   1.2. DEFINITIONS AND ABBREVIATIONS
       1.2.1. Definitions
       1.2.2. Abbreviations

2. GENERAL CONSIDERATIONS
   2.1. TIMESTAMPING SERVICE
   2.2. TIMESTAMPING AUTHORITY (TSA)
   2.3. CUSTOMERS

3. TIMESTAMPING POLICY
   3.1. INITIAL CONSIDERATION
   3.2. IDENTIFICATION OF THE TIMESTAMPING POLICY
   3.3. PARTICIPATING ENTITIES
       3.3.1. Certification services provider (CSPS)
       3.3.2. Timestamping Authority (TSA)
       3.3.3. Customer
       3.3.4. Third parties using the time stamps

4. OBLIGATIONS AND RESPONSIBILITIES
   4.1. REGISTRARS CERTIFICATION SERVICE
4.1.1. Obligations
4.1.2. Financial liability
4.1.3. Exemption from liability
4.1.4. Ceasing of the TSA activity

4.2. CUSTOMER

4.3. THIRD PARTIES USING THE TIME STAMPS

5. OPERATIONAL REQUIREMENTS

5.1. OBTAINING A RELIABLE TIME

5.2. TSA CERTIFICATE

5.2.1. Generation of the TSA certificate
5.2.2. Publication of the TSA certificate
5.2.3. Changes in the TSA certificate

5.3. Time stamp requests

5.4. Responding to timestamping requests
1. **INTRODUCTION**

The Registrars Association Certification Service (hereinafter, RCS) is a body belonging to Spanish Association of Land, Business and Personal Property Registrars (hereinafter, CORPME) as a Certification Services Provider that issues certificates recognised pursuant to Spanish Law 59/2003 dated 19 December 2003, on Electronic Signature. It also provides Timestamping services.

This document aims to describe the operation of the **Timestamping Services** provided by the CORPME and establish the conditions of use, obligations and responsibilities of all the entities involved.

Spanish Law 59/2003 on Electronic Signature does not include or regulate the issuing of time stamps. Nonetheless, the CORPME intends to assign to time stamps the status of “Recognised time stamps”, which is equivalent to the condition of “Recognised electronic signatures” insofar as this is possible, and in compliance with the legislation that applies in each case.

This Timestamping Policy is subject to compliance with the General Terms and Conditions set forth in the CORPME **Certification Practices Declaration (CPD)**.

---

1. **SUMMARY**

Timestamping is an online mechanism that provides proof of the existence of a series of data and that they have not been altered from a specific moment in time.

The CORPME is a Timestamping Authority (or TSA) which acts as a trustworthy third party in attesting the existence of electronic data on a specific date and at a specific time.
The timestamping services are not free, and they must be requested beforehand from the CORPME. The timestamping services may be marketed for an agreed term and/or for a specific number of timestamping requests.

The CORPME provides the Timestamping service in the following way:

- **Timestamping Service**: The customer requests the timestamping service, pursuant to regulation RFC 3161 from a CORPME URL and obtains digital proof signed by the CORPME TSA in response.

- **Timestamping Custody Service**: The CORPME stores and safeguards a copy of each item of digital proof generated and makes it available to the customer when necessary.

2. **DEFINITIONS AND ABBREVIATIONS**

1. **Definitions**

   - **Certification Services Provider**: a natural person or body corporate who/which issues electronic certificates or provides other services related to electronic signature.

   - **Time Stamp**: a special type of electronic signature issued by a trustworthy third party that allows the integrity of a document to be guaranteed on a specific date and at a specific time.

   - **Timestamping Authority**: a trustworthy entity which issues time stamps.

   - **Hardware Cryptographic Module**: a hardware device used to perform cryptographic functions and store codes safely.

   - **Hash Function**: an operation performed on a set of data of any size, such that the result obtained is another set of data of a fixed size, irrespective of the original size, which can unequivocally be associated to the initial data.

   - **List of Revoked Certificates**: a list of certificates that have been revoked or suspended.

2. **Abbreviations**

   - **CSP** Certification Services Provider
   - **TSA** Timestamping Authority
   - **TSP** Timestamping Protocol
   - **TST** Timestamp Token
   - **IETF** Internet Engineering Task Force
   - **CEN** European Committee for Standardisation
   - **FIPS** Federal Information Processing Standards
   - **CWA** CEN Workshop Agreement
   - **RFC** Request for comment
   - **UTC** Universal Time Coordinated
<table>
<thead>
<tr>
<th>Renewal of the Registrars Association PKI Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timestamping Policy</strong></td>
</tr>
<tr>
<td>Version 1</td>
</tr>
<tr>
<td>Date: 27/10/2010</td>
</tr>
<tr>
<td>Page 7 of 20</td>
</tr>
</tbody>
</table>

**CRL** Certificate Revocation List  
**HSM** Hardware Security Module
2. GENERAL CONSIDERATIONS

1. TIMESTAMPING SERVICE

Timestamping is an online mechanism that provides proof of the existence of a series of data and that they have not been altered from a specific moment in time.

The implementation of the timestamping policy must comply with the protocol defined in standard RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.

The steps to be followed for creating a time stamp are the following:

- The customer calculates the hash of the document to be stamped
- The customer sends a timestamping request to a specific CORPME URL in accordance with protocol RFC 3161, together with the hash of the document to be stamped
- The CORPME receives the request, checks to verify it is complete and correct and performs an access control based on the customer’s IP.
- If the result is correct, the TSA signs the request, which generates 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 Customer.
- The Customer must validate the stamp signature and keep it safe.
- The TSA will keep a register of stamps issued for future verification for at least 5 years.

2. TIMESTAMPING AUTHORITY (TSA)

A Timestamping Authority (TSA) is a Certification Services Provider that provides proof of the pre-existence of certain electronic documents at a given moment in time.

3. CUSTOMERS

Customers are the users of the service, who send timestamping requests and receive time stamps, pursuant to protocol RFC3161 Time Stamp Protocol (TSP).

In order to make timestamping requests, the customers must adapt their systems. There are public libraries that implement the TSP protocol in different programming languages:

- **BouncyCastle** (http://www.bouncycastle.org): A group of cryptographic libraries that implements the TSP protocol in the Java and C# languages
- **OpenTSA** (http://www.opentsa.org): This is an extension of the OpenSSL cryptographic library that implements the TSP protocol in C language.
- **Digistamp** (http://digistamp.com/toolkitDoc/MSToolKit.htm): A toolkit based on the Microsoft CryptoAPI cryptographic library that implements the TSP protocol in Visual Basic
- **IAIK**: This includes cryptographic libraries in Java that implement the TSP protocol. These libraries are only provided free of charge for non-commercial purposes.
Adobe Reader: The Adobe Reader 8 application enables the validation of time stamps included in PDF documents.
3. **TIMESTAMPING POLICY**

1. **INITIAL CONSIDERATION**

The timestamping services are not free, and they must be requested beforehand from the CORPME. The timestamping services may be marketed for an agreed term and/or for a specific number of timestamping requests.

The CORPME provides two different Timestamping services:

- **Timestamping Service**: The customer presents a request for a time stamp to a CORPME URL (http://tsa.registradores.org or https://tsa.registradores.org) in accordance with the RFC 3161 protocol and obtains digital proof signed by the CORPME TSA in response.

- **Timestamping Custody Service**: The CORPME stores and safeguards a copy of each item of digital proof generated and makes it available to the customer when necessary.

The CORPME timestamping policy is based on the following protocols:

- RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.
- ETSI TS 101 862, Qualified Certificate Profile

2. **IDENTIFICATION OF THE TIMESTAMPING POLICY**

<table>
<thead>
<tr>
<th>Document name</th>
<th>Registrars Association Timestamping Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document version</td>
<td>1.0</td>
</tr>
</tbody>
</table>
3. PARTICIPATING ENTITIES

1. **Certification services provider (PSC)**

Pursuant to the Electronic Signature Law, a Certification Services Provider (CPS) is a natural person or body corporate who/which issues electronic certificates or provides other services related to electronic signature.

2. **Timestamping Authority (TSA)**

The Timestamping Service of the CORPME Registrars Association (RCS) is a CSP that acts as a Timestamping Authority (TSA). The CORPME will provide certification services through the PSC, without authorising them to be provided by any other entity.

The CORPME may use different systems to generate time stamps, thereby giving the service high availability.

3. **Customer**

The CORPME Timestamping Services are not public or provided free of charge. To access the timestamping services, Customers must first register for the service with the CORPME.

The CORPME will perform an access control on the service, based on IP addresses, which means that the Customer must inform the CORPME of the IP addresses from where the requests will be made.

The Customer must adapt its systems to the TSP protocol. The timestamping service provided by the CORPME does not furnish any software or integration libraries to the customer.

4. **Third parties using the time stamps**

Spanish Law 59/2003 on Electronic Signature does not include or regulate the issuing of time stamps. Nonetheless, the CORPME intends to assign to assign to time stamps the status of "Recognised time
stamps”, which is equivalent to the condition of “Recognised electronic signatures” insofar as this is possible, and in compliance with the legislation that applies in each case.

Consequently any user may validate time stamps at any time, putting their trust in the CORPME as a Certification Services Provider that issues recognised certificates.
4. OBLIGATIONS AND RESPONSIBILITIES

1. REGISTRARS CERTIFICATION SERVICE

1. **Obligations**

The CORPME, acting as the Timestamping Authority (TSA), undertakes to:

- Respect the terms of this Timestamping Policy.
- Keep its private passwords safely protected.
- Issue time stamps in accordance with this Policy and the applicable standards.
- Guarantee that the date and time shown on the stamps is within the precision limits established in the contract signed by the customer and the CORPME, which must in no case exceed one second.
- Issue time stamps in accordance with the information sent by the customer, with no data entry errors.
- Issue time stamps whose minimum content is that defined by current legislation, as applicable.
- Publish this Timestamping Policy.
- Inform customers and third parties using the time stamps about all changes made to the Timestamping Policy.
- Establish the necessary mechanisms for generating and safekeeping relevant information on the above activities and protect them from loss, destruction or falsification.
- Safeguard the time stamps issued for customers registering for the timestamping service for 5 years.

In providing its certification services, the CORPME will respond in the event of breach of the terms of this Timestamping Policy as and where applicable, pursuant to the provisions of Law 59/2003 of 19 December 2003 on Electronic Signature or the provisions implementing that Law.

Without prejudice to the foregoing, the CORPME cannot guarantee the algorithms and cryptographic standards used, or respond for damage caused by external attacks on the latter, provided it has applied all due diligence in accordance with the current state of the art, and it has acted in accordance with the terms of these TSA Policies and current legislation, as and where applicable.

2. **Financial liability**

Not applicable due to not being a certificate issuing service recognised by the provisions of Spanish Law de 59/2003 on Electronic Signature. The TSA will not be held liable in the event of transactional losses.

3. **Exemption from liability**
The CORPME will not be liable in any case in the event of any of the following circumstances occurring:

- in the case of war, natural disasters, faulty operation of electrical services, electronic and/or telephone networks or in the computer equipment used by the Customer or Third Parties, or in any other Force Majeure event.
- in the event of incorrect or fraudulent use of the time stamps.
- in the event of incorrect use of the information included in the Certificate or CRL.
- for the content of the stamped messages or documents.
- in relation to actions or omissions by the Customer.
- in the event of the information furnished for issuing the stamp being untrue.
- for negligence in storing access data to the timestamping service, guaranteeing their confidentiality and protecting access or disclosure.
- in the event of exceeding the scope of use of the time stamp, pursuant to the terms of current legislation and this TSA Policy.
- in relation to actions or omissions by third-party users of the certificate.
- in the event of failure to verify suspension or non-validity of the TSA electronic certificate published in the consultation service with respect to the validity of the certificates or failure to check the electronic signature.

4. **Ceasing of the TSA activity**

In the event of ceasing its activity, the TSA will proceed as follows:

- it will notify all subscribers, users or entities with who/which it has agreements or any other type of relationship of the ceasing of its activities at least 2 months in advance, or within the term set by current legislation.
- it will revoke all authorisations granted to subcontracted entities to act on behalf of the TSA in the time stamp issuing procedure.
- it will inform the competent administration, within the stipulated term, of the ceasing of its activity and the use to be given to the time stamps issued until such time, specifying in each case whether the processing thereof will be transferred and to whom.

2. **CUSTOMER**

Customers are obliged to comply with the provisions of the applicable legislation. They will also:

- respect the terms set out in the contractual documents signed with the TSA.
- verify that the electronic signature on the time stamp is correct and check the validity of the TSA certificate at the time of signing it.

- verify that the hash of the time stamp coincides with the one that was sent.

- store and keep the time stamps delivered to it by the TSA. Customers are responsible for storing the time stamps if they consider they may be needed in the future.

3. **THIRD PARTIES USING THE TIME STAMPS**

Users will comply with the terms of the applicable legislation, and in addition:

- verify that the electronic signature on the time stamp is correct and check the validity of the TSA certificate at the time of signing it.
5. OPERATIONAL REQUIREMENTS

1. OBTAINING A RELIABLE TIME

The CORPME will synchronise times with the ROA (Royal Navy Institute and Observatory of San Fernando) through the NTP Protocol over the Internet (RFC 1305 Network Time Protocol). The Time Section of this Institute has the main mission of maintaining the basic Time Unit declared for legal purposes as a National Standard for that unit, and the maintenance and official diffusion of the "Coordinated Universal Time" scale (UTC(ROA)), considered to all effects and purposes as the basis of the legal time throughout Spain (R. D. 1308/1992 of 23 October 1992). To that end, a research project is established consisting of setting up a Time Laboratory at the headquarters of the Royal Observatory for the purpose of establishing, processing and controlling the quality of the time sent through an exclusive communication channel used by the Registrars Association Information Systems Service in Madrid by computerised, from where it is distributed.

2. TSA certificate

   1. Generation of the TSA certificate

The process for issuing the Timestamping Certificate (TSA) will be executed manually, ensuring maximum standards of security in the process.

The Timestamping Certificate (TSA) is issued and revoked by the Central Processing Unit, at the request of the Management Committee.

Pursuant to the certification policy, the TSA certificate must be issued by the Subordinated CAs of the CORPME in accordance with OID 1.3.6.1.4.1.17276.0.3

The certificate structure in reference to the subject extension of the certificate is the one described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>ES</td>
<td>Country</td>
</tr>
<tr>
<td>O</td>
<td>Spanish Association of Land and Business Registrars</td>
<td>Organisation</td>
</tr>
<tr>
<td>OU</td>
<td>Own Certificate</td>
<td></td>
</tr>
<tr>
<td>CN</td>
<td>Spanish Registrars - TSA</td>
<td>Name of Registry</td>
</tr>
</tbody>
</table>
The most relevant fields of the CORPME TSA certificate are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Proposed Content</th>
<th>Critical</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Certificate Policies</td>
<td>Will be used</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Policy Identifier</td>
<td>2.5.29.32.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reference Notice</td>
<td>Certificate subject to the CORPME CPD, provider address <a href="http://pki.registradores.org/normativa/direccion.html">http://pki.registradores.org/normativa/direccion.html</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Subject Alternative Names</td>
<td></td>
<td></td>
<td>[RFC3280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the Email Address attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.</td>
</tr>
<tr>
<td>Rfc822Name = e-mail address</td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3. CRL Distribution Points</td>
<td>(1) HTTP: <a href="http://pki.registradores.org/crls/crl_int_scr.crt">http://pki.registradores.org/crls/crl_int_scr.crt</a></td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2) LDAP: ldap://ldap.registradores.org/ CN=CA%20INTERN, OU=CERTIFICADO%20PROPIO, O=COLEGIO%20DE%20REGISTRADORES, C=ES ?certificateRevocationList?base ?objectclass=cRLDistributionPoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Auth. Information</td>
<td>OCSP: <a href="https://ocsp.registradores.org/">https://ocsp.registradores.org/</a></td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA Raíz: <a href="http://pki.registradores.org/certificados/ca_raiz_scr.crt">http://pki.registradores.org/certificados/ca_raiz_scr.crt</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Key Usage</td>
<td>Digital signature, key agreement, ensures the identity.</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
6. Extended Key Usage OID

| Extended Key Usage OID | 1.3.6.1.5.5.7.3.8 (Time Stamp Signature). | Yes |

The private keys of the TSA are generated and safeguarded in a safe cryptographic device that complies with the requirements set out in FIPS 140-3 level 3 and FIPS 140-2 level 3, as applicable.

The CORPME may have different TSAs to guarantee high availability of the timestamping service.

2. **Publication of the TSA certificate**

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

3. **Changes in TSA certificates**

The TSA certificates can be changed at any time for another equally valid TSA certificate, in accordance with the CORPME **Certificate Certification Policies**.

Such changes will not be communicated to users of the service, and they must use all the stamps issued by the CORPME and signed with valid TSA certificates in accordance with certification hierarchy.

Therefore a user only needs to use the CORPME CA Root and CAs to validate the signatures.

3. **Timestamping requests**

Time stamp requests will be in accordance with the syntax of specification “**RFC3161 Time Stamp Protocol (TSP)**” described in Section 2.3. “Time-Stamp Protocol” of the specification, with the restrictions imposed by regulation ETSI TS 101 862.

As established by the CORPME, the URLs of the Timestamping Service may be:

- [http://tsa.registradores.org](http://tsa.registradores.org)
- [https://tsa.registradores.org](https://tsa.registradores.org)

The algorithms permitted are SHA-1 and MD5.

The format for submitting the requests is based on the following schema:

```
TimeStampReq ::= SEQUENCE {
  Version INTEGER { v1(1) },
  messageImprint MessageImprint,
} 
```
4. Responding to time stamp requests

The format for responding is the following:

```
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),
  systemFailure (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
}