Registradores DE ESPAÑA

PRÁCTICAS Y POLÍTICAS DE SELLADO DE TIEMPO DEL CORPME

Prestador del Servicio de Certificación del Colegio de Registradores

Servicio de Sistemas de la Información
28 de febrero de 2023

COLEGIO DE REGISTRADORES DE ESPAÑA
Diego de León, 21 - 28006 Madrid
Tel.: +34 91 270 16 99 - Fax: +34 91 562 67 37

CONTROL DOCUMENTAL

DOCUMENTO / ARCHIVO	
Título: Prácticas y Políticas de Sellado de Tiempo del CORPME	Nombre Archivo/s: REG-PKI-DPC04v.1.3.2Prácticas y Políticas de Sellado de Tiempo del CORPME.pdf
Código: REG-PKI-DPC04	Soporte lógico: MS-DOCX y PDF
Fecha: 28/02/2023	Ubicación física: http://pki.registradores.org/normativa/index.htm
Versión: 1.3.2	

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo del cambio**
1.0.0	20/06/2016	Creación del documento
1.0.1	19/09/2016	Modificaciones LFE/2016/0071
1.0.2	29/05/2017	Adaptación al Reglamento eIDAS
1.1.0	26/06/2017	Adaptación debido a la auditoría de acuerdo a las normas ETSI
1.2.0	23/08/2017	Correcciones menores
1.3.0	27/05/2019	Inclusión de detalle sobre el contenido de certificado de sellado de tiempo. Definición de una lista acotada de algoritmos de hash que se pueden usar para el sello de tiempo.
1.3.1	12/03/2021	Actualización de la nueva ley de servicios de confianza. Inclusión de métodos de verificación de sellos de tiempo.
1.3.2	28/02/2023	Actualización de los datos del certificado de TSA

ÍNDICE

1 INTRODUCCIÓN

1.1 Visión general

El Prestador de Servicios de Certificación del Colegio de Registradores (en adelante, PSC), órgano del Colegio de Registradores de la Propiedad y Mercantiles de España (en adelante, CORPME) como Prestador Cualificado de Servicios de Confianza que emite certificados cualificados según la normativa EU 910/2014 relativa a la identificación electrónica y a los servicios de confianza, y según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza; también ofrece servicios de Sellado de Tiempo.

Este documento tiene como objetivo describir el funcionamiento los Servicios de Sellado de Tiempo ofrecidos por el CORPME y establecer las condiciones de uso, obligaciones y responsabilidades de las distintas entidades involucradas.

La Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza no recoge ni regula la emisión de sellos de tiempo. Sin embargo, es intención del CORPME dotar a los sellos de tiempo emitidos la condición de "Sellos de Tiempo cualificados" equivalente a la condición de "Firmas electrónicas cualificadas", en la medida que esto sea posible y comprometiéndose a cumplir con la legislación aplicable en cada caso.

Este documento de Prácticas y Políticas de Sellado de Tiempo está subordinado al cumplimiento de las Condiciones Generales expuestas en la Declaración de Prácticas de Certificación (en adelante, DPC) del CORPME.

1.2 Servicio de Sellado de Tiempo

El sellado de tiempo (*Time Stamping*) es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

El CORPME es una Autoridad de Sellado de Tiempo (TSA o Time Stamping Authority) que actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

Los servicios de sellado de tiempo no son gratuitos, por lo que será necesario contratar el servicio previamente con CORPME. Los servicios de sellado de tiempo se podrán comercializar bajo la limitación temporal que se acuerde y/o de número de peticiones de sellado de tiempo. En todo caso, las condiciones de facturación de la TSA son revisadas, garantizando que no se aplican cargas adicionales a las establecidas en los contratos.

El CORPME ofrece el servicio de Sellado de Tiempo de la siguiente forma:

- **Servicio de Sellado de Tiempo**: El cliente realiza una petición de Sellado de Tiempo según la norma RFC 3161 a una URL del CORPME, obteniendo como respuesta una evidencia digital firmada por la TSA de CORPME.

La implementación de las Prácticas y Políticas de Sellado de Tiempo debe cumplir con el protocolo definido en la norma ***RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".***

La TSA del CORPME permite generar sellos de tiempo sobre cualquier tipo de documento u objeto, con o sin firma electrónica de cualquier tipo.

Los pasos para generar un sello de tiempo son los siguientes:

- El cliente calcula el hash del documento u objeto a sellar.

- El cliente envía una solicitud de sello de tiempo a una URL determinada del CORPME siguiendo el protocolo RFC 3161, incluyendo el hash del documento a sellar.
- El CORPME recibe la petición, revisa si la si la petición está completa y correcta y realiza un control de acceso en función de la IP del cliente.
- Si el resultado es correcto, la TSA firma la petición generando un Sello de Tiempo (incluyendo el hash del documento, la fecha y hora obtenida de una fuente fiable y la firma electrónica de la TSA).
- El sello de tiempo se envía de vuelta al Cliente.
- El Cliente debe validar la firma del sello y custodiarlo debidamente.
- La TSA mantendrá un registro de los sellos emitidos para su futura verificación durante al menos 5 años.

El CORPME registra la siguiente información relativa al Servicio de Sellado de Tiempo:

- Eventos relevantes del ciclo de vida de las claves de la TSU.
- Eventos relevantes del ciclo de vida de los certificados TSU.
- Eventos de sincronización del reloj de la TSU con el UTC, incluyendo información de recalibración de relojes.
- Eventos relacionados con la detección de pérdida de sincronización.

1.3 Definiciones y abreviaturas

1.3.1 Definiciones

- **Prestador de Servicios de Certificación**: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- **Sello de Tiempo**: Es un tipo especial de firma electrónica emitida por un tercero de confianza que permite garantizar la integridad de un documento en una fecha y hora determinadas.
- **Autoridad de Sellado de Tiempo**: Entidad de confianza que emite sellos de tiempo.
- **Módulo Criptográfico Hardware**: Módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.
- **Función Hash**: Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.
- **Listas de Certificados Revocados**: Lista donde figuran las relaciones de certificados revocados o suspendidos.
- **Certificado cualificado**: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.
- **Certificado cualificado de firma electrónica**: Un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014.

1.3.2 Abreviaturas

CRL: Certificate Revocation List (Lista de Revocación de Certificados).

CWA: CEN Workshop Agreement.

FIPS: Federal Information Processing Standards.

HSM: Hardware Security Module. Módulo de seguridad criptográfica empleado para el almacenamiento de claves y realización de operaciones criptográficas seguras.

IETF: Internet Engineering Task Force (Organismo de estandarización de Internet).

PSC: Prestador de Servicios de Certificación.

RFC: Request For Comments. Standard desarrollado por el IETF.

ROA: Real Observatorio de la Armada Española.

TSA: Time Stamping Authority (Autoridad de Sellado de Tiempo).

TSP: Time Stamping Protocol (Protocolo de Sellado de Tiempo).

TST: Time Stamp Token (Token de Sellado de Tiempo).

TSU: Time Stamping Unit (Unidad de Sellado de Tiempo).

UTC: Universal Time Coordinated.

1.3.3 Referencias

- **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 PRÁCTICAS Y POLÍTICAS DE SELLADO DE TIEMPO

2.1 Vista Inicial

Los servicios de sellado de tiempo no son gratuitos, por lo que será necesario contratar el servicio previamente con el CORPME. Los servicios de sellado de tiempo se podrán comercializar bajo la limitación temporal y/o de número de peticiones de sellado de tiempo que se acuerde.

El CORPME ofrece el servicio de Sellado de Tiempo de la siguiente forma:

- **Servicio de Sellado de Tiempo**: El cliente realiza una petición de sellado de tiempo según la norma RFC 3161 a una URL del CORPME (http://tsa.registradores.org o https://tsa.registradores.org), obteniendo como respuesta una evidencia digital firmada por la TSA del CORPME.

Las Prácticas y Políticas de Sellado de Tiempo del CORPME se basan en los estándares:

- 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 Identificación de las Prácticas y Políticas de Sellado de Tiempo

Nombre del documento	Prácticas y Políticas de Sellado de Tiempo del CORPME
Versión del documento	1.3.2
Estado del documento	Versión
Fecha de emisión	28/02/2023
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.3.3.1
Ubicación del documento	http://pki.registradores.org/normativa/index.htm
DPC Relacionada	Declaración de Prácticas de Certificación

Las Prácticas y Políticas de Sellado de Tiempo del CORPME cumplen con el estándar ETSI EN 319 421.

La TSA está compuesta de una única Unidad de Sellado de Tiempo (TSU o Time Stamping Unit) que emite los sellos de tiempo conforme a la política de sellado de tiempo BTSP (OID 0.4.0.2023.1.1) descrita en ETSI EN 319 421.

2.3 Entidades Participantes

2.3.1 Prestador de servicios de certificación (PSC)

Según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, se denomina Prestador de Servicios de Certificación (PSC) la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

2.3.2 Autoridad de Sellado de Tiempo (TSA)

El Prestador de Servicios de Certificación del Colegio de Registradores (órgano del CORPME), es un PSC que actúa como Autoridad de Sellado de Tiempo (TSA). El CORPME ofrecerá los servicios de sellado de tiempo únicamente a través del PSC, sin delegarlos en ninguna otra entidad.

La TSA proporciona certeza sobre la preexistencia de determinados documentos electrónicos en un momento dado.

El CORPME utilizará diferentes sistemas para generar sellos de tiempo, proporcionando alta disponibilidad al servicio.

2.3.3 Cliente

Los servicios de Sellado de Tiempo del CORPME no son públicos ni gratuitos. Para poder acceder a los servicios de sellado de tiempo, el Cliente deberá contratar previamente el servicio con el CORPME.

El CORPME realizará un control de acceso al servicio basado en direcciones IP, por lo tanto, el Cliente deberá informar al CORPME de las direcciones IP desde donde se realizarán las peticiones.

El cliente debe adaptar sus sistemas al protocolo TSP para poder realizar peticiones de sellado de tiempo. El servicio de sellado de tiempo ofrecido por el CORPME no proporciona ningún software ni librerías de integración al cliente. Para adaptar los sistemas, existen librerías públicas que implantan el protocolo TSP en diversos lenguajes de programación:

- **BouncyCastle** (http://www.bouncycastle.org): Conjunto de librerías criptográficas que implementan el protocolo TSP en los lenguajes Java y C#
- **OpenSSL TS** (https://www.openssl.org): Es un módulo de la librería criptográfica OpenSSL que implementa el protocolo TSP en lenguaje C.
- **Digistamp** (http://digistamp.com/toolkitDoc/MSToolKit.htm): Toolkit basado en la librería criptográfica CryptoAPI de Microsoft que implementa el protocolo TSP en Visual Basic
- **IAIK**: Incluye librerías criptográficas en Java que implementan el protocolo TSP. Estas librerías son gratuitas únicamente para propósitos no comerciales.
- **Adobe Reader**: La aplicación Adobe Reader 8 permite validar sellos de tiempo incluidos en documentos PDF.

2.3.4 Tercero que confía en los sellos de tiempo

Ni la normativa EU 910/2014 de identificación electrónica ni la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza no recogen ni regulan la emisión de sellos de tiempo. Sin embargo, es intención del CORPME dotar a los sellos de tiempo emitidos la condición de “Sellos de Tiempo Cualificados” equivalente a la condición de “Firmas electrónicas Cualificadas”, en la medida que esto sea posible y comprometiéndose a cumplir con la legislación aplicable en cada caso.

Por lo tanto, cualquier usuario podrá validar los sellos de tiempo libremente basándose en la confianza en el CORPME como Prestador de Servicios de Certificación que emite certificados cualificados.

3 REQUERIMIENTOS OPERACIONALES

3.1 Obtención del Tiempo Fiable

El CORPME realiza una sincronización de tiempo con el ROA mediante el Protocolo NTP a través de Internet (RFC 1305 *Network Time Protocol*). La Sección de Hora del **Real Observatorio de la Armada Española (ROA)** tiene como misión principal el mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC (ROA)), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (R. D. 23 octubre 1992, núm. 1308/1992).

Para ello se establece un proyecto de investigación por medio de la constitución de un Laboratorio de Tiempo en la sede del Real Observatorio desde el que se obtenga, trate y controle por medios informáticos la calidad del tiempo, que se enviará, a través de un canal de comunicación exclusivo y dedicado al Servicio de Sistemas de Información del Colegio de Registradores en Madrid, y desde el cual es distribuido.

La TSA del CORPME proporciona una precisión de un segundo.

3.2 Certificado de TSA

3.2.1 Generación del certificado de TSA

El proceso de emisión de Certificado de Sellado de Tiempo (TSA) se realizarán de manera manual siguiendo las máximas garantías de seguridad en el proceso.

El certificado de Sellado de Tiempo (TSA) se emite y revoca por la Unidad de Tramitación Central, a petición de la Comisión Directora.

El certificado de TSA ha de ser emitido por la CA Subordinada Interna del CORPME, siguiendo la correspondiente política de certificación.

La estructura del certificado, referente al campo *Subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País.
organizationIdentifier	VATES-Q2863012G	NIF (Requerido por ETSI 319 412-2).
O	Colegio de Registradores de la Propiedad y Mercantiles	Organización.
CN	Autoridad de Certificación de los Registradores - TSA – 01	Nombre Común.

A continuación se presentan los campos y extensiones del certificado X.509 v3 de la TSA de CORPME:

Campo / Extensión	Contenido	Crítica	Observaciones
Version	v3		
Serial Number	635da992b19ab176624eb7484e718f6f		
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Norma PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements"*, en *PrintableString*.
Valid From	jueves, 7 de abril de 2022 11:04:55		Fecha de inicio del periodo de validez.
Valid To	lunes, 7 de abril de 2025 11:04:55		Fecha de final del periodo de validez.
Subject	CN = Autoridad de Certificación de los Registradores - TSA - 01 O = Colegio de Registradores de la Propiedad y Mercantiles organizationIdentifier = VATES-Q2863012G C = ES		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements"*, en *PrintableString*.
Subject Public Key	Algoritmo: RSA Encryption Longitud: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto	NO	
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora	NO	
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.10.1		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- 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)		Campo codificado en UTF8.
Subject Alternative Name	No utilizado	NO	

CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20INTERNA, O=Colegio%20de%20Registradores%20–%20Q2863012G, C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Alternative Name (Access Location):** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Alternative Name (Access Location)** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Key Usage	Digital Signature Non Repudiation	SI	
Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)	SI	

Las claves privadas de la TSU se generan y custodian en un dispositivo criptográfico seguro que cumple los requerimientos que se detallan en FIPS 140-3 nivel 3 y FIPS 140-2 nivel 3 en su caso, garantizando el cumplimiento de los requisitos del criterio EAL4+ de acuerdo con la normativa ISO/IEC 15408. El dispositivo criptográfico no se manipula durante el transporte ni cuando está almacenado.

En caso de posible debilidad del algoritmo o del tamaño de las claves de la TSU, su certificado será revocado, se generarán nuevas claves de la TSU con un algoritmo y tamaño más seguros y se emitirá un nuevo certificado de TSA.

El CORPME dispone de diversos servidores para garantizar la alta disponibilidad del servicio de sellado de tiempo. Así mismo se reserva el derecho de establecer cuantas unidades de sellado de tiempo se considere oportunas y su gestión conforme a los procedimientos particulares establecidos para garantizar en todo momento la adecuada prestación del servicio.

Al finalizar el periodo de validez, las claves privadas de las TSU y sus copias de seguridad son destruidas de manera segura al retirarse del dispositivo, de tal forma que no puedan ser recuperadas, con la finalidad de evitar su uso inapropiado.

3.2.2 Publicación del certificado de TSA

El certificado de la TSA se adjunta en la respuesta de cada Sellado de Tiempo que se emite.

3.2.3 Cambio de certificado de TSA

El certificado de la TSA puede ser cambiado en cualquier momento por otro certificado de TSA igualmente válido según las Políticas de Certificación de Certificados del CORPME.

Este cambio no se comunicará a los usuarios del servicio, los cuales deberían confiar en todos los sellos emitidos por del CORPME y firmados con certificados válidos de TSA dentro de la jerarquía de certificación.

Por lo tanto, un usuario únicamente necesita confiar en el certificado de CA Raíz y las CA´s del CORPME para validar las firmas.

3.3 Solicitud de sellos de tiempo

Las solicitudes de sellos se adherirán a la sintaxis de la especificación “RFC3161 Time Stamp Protocol (TSP)” descrito en el Apartado 2.4.1.

Según disponga el CORPME las URLs del servicio de Sellado de Tiempo podrán ser: http://tsa.registradores.org o bien https://tsa.registradores.org.

Los algoritmos de HASH admitidos son:

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

Quedando totalmente prohibido el uso de cualquier algoritmo de hash distinto de los identificados en la lista anterior.

El formato de envío de las solicitudes sigue el siguiente esquema:

```
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 Respuesta a la solicitud de sellos de tiempo

El formato de respuesta es el siguiente:

```
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 Validación de sellos de tiempo

Para validar un sello de tiempo, las partes confiantes verificarán el Sello electrónico que acompaña a los Sellos de tiempo electrónicos haciendo uso del campo “messageImprint” descrito en el apartado anterior, así como el estado de validez del Certificado de la TSU que podrá ser verificado a través de los dos mecanismos de validación de certificados que el CORPME pone a disposición de los usuarios, a través de la consulta de las Listas de revocación de certificados (CRLs) o a través del servicio de información y consulta del estado de los certificados (protocolo OCSP).
Además, se debe verificar que el hash contenido en el sello de tiempo coincide con el que envió y la corrección de la firma digital del sello de tiempo.

4 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

4.1 Seguridad física

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.1.1 Ubicación y medidas de seguridad física de las instalaciones de CORPME

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.1.2 Acceso físico

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.1.3 Suministro eléctrico y acondicionamiento ambiental de las instalaciones del CORPME

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.1.4 Exposición al agua

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.1.5 Medidas contra incendios e inundaciones.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.1.6 Sistema de almacenamiento

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.1.7 Eliminación de residuos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.1.8 Política de Respaldo de Información.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.2 Controles de procedimiento

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.2.1 Roles responsables del control y gestión de la PKI del CORPME

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.2.2 Número de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.2.3 Roles que requieren segregación de funciones

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3 Controles de personal

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.2 Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.3 Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.4 Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.5 Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.6 Sanciones por actuaciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.7 Requisitos de contratación de terceros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.8 Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4 Procedimientos de auditoría de seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.1 Tipos de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.2 Frecuencia de procesado de registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.3 Periodo de conservación de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.4 Protección de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.5 Procedimientos de respaldo de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.6 Notificación al sujeto causa del evento

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.7 Análisis de vulnerabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.8 Procedimientos legales

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5 Archivado de registros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5.1 Tipo de eventos archivados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5.2 Periodo de conservación de registros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5.3 Protección del archivo

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5.4 Procedimientos de copia de respaldo del archivo

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5.5 Requerimientos para el sellado de tiempo de los registros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5.6 Sistema de archivo de información (interno vs externo)

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5.7 Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.6 Cambio de claves

Los procedimientos para proporcionar, en caso de cambio de claves, una nueva clave pública de TSA son los mismos que para proporcionar la clave pública en vigor.

4.7 Recuperación ante compromiso de clave o catástrofe

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.7.1 Procedimientos de gestión de incidentes y compromisos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.7.2 Alteración de los recursos hardware, software y/o datos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.7.3 Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad

En el caso de compromiso de la clave privada de la TSA se procederá a su revocación inmediata. Seguidamente, se generará y publicará la correspondiente CRL, cesando el funcionamiento de actividad de la TSA y se procederá a la generación, certificación y puesta en marcha de una nueva Autoridad con la misma denominación que la eliminada y con un nuevo par de claves.

4.7.4 Instalación después de un desastre natural u otro tipo de catástrofe

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.8 Cese de una TSA

Antes del cese de su actividad la TSA realizará las siguientes actuaciones:

- Informará a todos los suscriptores, usuarios o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la TSA en el procedimiento de emisión de sellos de tiempo.
- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los sellos de tiempo emitidos hasta la fecha, especificando, en su caso, si se va a transferir la gestión y a quien.
- Mantendrá el certificado de la TSA activo, así como el sistema de verificación (Autoridad de Validación) y revocación hasta la extinción del propio certificado.
- Tramitará la revocación del certificado de la TSA.
- Destruirá o deshabilitará las claves privadas del certificado de la TSA, incluidas sus copias de seguridad, de tal manera que no puedan ser recuperadas.
- Remitirá al Ministerio de Industria, Comercio y Turismo con carácter previo al cese definitivo de su actividad la información relativa al certificado de la TSA cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia.

En caso de transferencia de la actividad a otra TSA, el CORPME:

- Publicará los acuerdos de transferencia y un documento explicativo de las condiciones que regularán las relaciones entre el suscriptor y el PSC al cual se transfieren los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y la recepción de la notificación, con una antelación mínima de dos (2) meses al cese de su actividad, o el periodo que establezca la legislación vigente.
- Transferirá todas las bases de datos importantes, archivos, documentos, registros de eventos y auditoría a la entidad designada durante las 24 horas siguientes a su terminación, o el periodo que establezca la legislación vigente.
- Transferirá la obligación de poner a disposición de los suscriptores, usuarios o entidades la información pública necesaria para la prestación de los servicios, como la clave pública de los certificados.

5 CONTROLES DE SEGURIDAD TÉCNICA

5.1 Controles de seguridad informática

5.1.1 Requerimientos técnicos de seguridad específicos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.2 Evaluación de la seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.2 Controles de seguridad del ciclo de vida

5.2.1 Controles de desarrollo de sistemas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.2.2 Controles de gestión de seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.2.3 Controles de seguridad del ciclo de vida

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3 Controles de seguridad de la red

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

6.1 Frecuencia o circunstancias de los controles para cada Autoridad

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.2 Identificación/cualificación del auditor

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.3 Relación entre el auditor y la Autoridad auditada

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.4 Aspectos cubiertos por los controles

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.5 Acciones a tomar como resultado de la detección de deficiencias

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.6 Comunicación de resultados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7 OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

7.1 Tarifas

7.1.1 Tarifas de los servicios de sellado de tiempo

Los servicios de sellado de tiempo no son gratuitos, por lo que será necesario contratar el servicio previamente con CORPME. Los servicios de sellado de tiempo se podrán comercializar bajo la limitación temporal que se acuerde y/o de número de peticiones de sellado de tiempo. En todo caso, las condiciones de facturación de la TSA son revisadas, garantizando que no se aplican cargas adicionales a las establecidas en los contratos.

7.1.2 Política de reembolso

Los servicios de sellado de tiempo se reembolsarán bajo las condiciones establecidas en cada tipo de contrato.

7.2 Responsabilidades económicas

No aplicable por no tratarse de un servicio de emisión de certificados cualificados según lo estipulado en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. La TSA no se hace responsable en caso de pérdidas por transacciones.

7.3 Confidencialidad de la información

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.3.1 Ámbito de la información confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.3.2 Información no confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.3.3 Deber de secreto profesional

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.4 Protección de la información personal

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.5 Derechos de propiedad intelectual

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.6 Representaciones y garantías

7.6.1 Obligaciones de la TSA

El CORPME, actuando como Autoridad de Sellado de Tiempo (TSA) se obliga a:

- Respetar lo dispuesto en estas Prácticas y Políticas de Sellado de Tiempo.
- Proteger sus claves privadas de forma segura.
- Emitir sellos de tiempo conforme a estas Prácticas y Políticas y a los estándares de aplicación.
- Garantizar que la hora y fecha incluidas en los sellos se mantienen dentro de los márgenes de precisión de la referencia temporal proporcionada por la Sección de Hora del Real Observatorio de la Armada Española, que en ningún caso podrán superar una desviación máxima de un segundo.
- Emitir sellos de tiempo según la información enviada por el cliente y libres de errores de entrada de datos.
- Emitir sellos de tiempo cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.
- Publicar estas Prácticas y Políticas de Sellado de Tiempo.
- Informar sobre las modificaciones de las Prácticas y Políticas de Sellado de Tiempo a clientes y terceros que confían en los sellos de tiempo.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
- Custodiar los sellos de tiempo emitidos para los clientes que contraten el servicio de sellado de tiempo durante 5 años.
- No emitir sellos de tiempo en caso de que exista un compromiso de las operaciones del servicio, incluyendo el compromiso de las claves, la pérdida de calibración o precisión temporal, y el fallo de sincronización de los relojes.

El CORPME, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en estas Prácticas y Políticas de Sellado de Tiempo y, allí donde sea aplicable, por lo que dispone la Ley 59/2003, de 19 de diciembre, de firma electrónica o su normativa de desarrollo.

Sin perjuicio de lo anterior el CORPME no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en el presente documento Prácticas y Políticas de la TSA y en la legislación vigente, donde sea aplicable.

7.6.2 Obligaciones de los clientes de los sellos de tiempo

El Cliente estará obligado a cumplir con lo dispuesto por la normativa y además a:

- Respetar lo dispuesto en los documentos contractuales firmados con la TSA.
- Verificar la corrección de la firma digital del sello de tiempo y la validez del certificado de la TSA en el momento de firmarlo.
- Verificar que el hash contenido en el sello de tiempo coincide con el que envió.

- Almacenamiento y conservación de los sellos de tiempo entregados por la TSA. Es responsabilidad del Cliente almacenar los sellos de tiempo, si prevé que le serán necesarios en el futuro.

7.6.3 Obligaciones de los terceros que confían en los sellos de tiempo

Será obligación de los Usuarios cumplir con lo dispuesto por la normativa vigente y además:

- Verificar la corrección de la firma del sello de tiempo y la validez del certificado de la TSA en el momento de firmarlo.

7.6.4 Obligaciones de organizaciones externas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.6.5 Obligaciones de otros participantes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.7 Exención de responsabilidades

El CORPME no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Cliente o por los Terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento de los sellos de tiempo.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.
- Por el contenido de los mensajes o documentos sellados.
- En relación a acciones u omisiones del Cliente.
- Falta de veracidad de la información suministrada para emitir el sello.
- Negligencia en la conservación de sus datos de acceso al servicio de sellado de tiempo, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- Extralimitación en el uso del sello de tiempo, según lo dispuesto en la normativa vigente y en el presente documento de Prácticas y Políticas de la TSA.
- En relación a acciones u omisiones del usuario, tercero que confía en el certificado.
- Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico de la TSA publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

7.8 Limitaciones de las responsabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.9 Indemnizaciones

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.10 Período de validez

7.10.1 Plazo

Este documento de Prácticas y Políticas entra en vigor desde el momento de su publicación en el directorio web del PSC del CORPME y se mantendrá vigente mientras no se derogue expresamente por la emisión de una nueva versión.

7.10.2 Sustitución y derogación

Este documento de Prácticas y Políticas será sustituido por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando el documento de Prácticas y Políticas quede derogado se retirará del directorio web del PSC del CORPME, si bien se conservará durante quince (15) años.

7.10.3 Efectos de la finalización

Las obligaciones y restricciones que establece este documento de Prácticas y Políticas, en referencia a auditorías, información confidencial, obligaciones y responsabilidades del PSC del CORPME, nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

7.11 Notificaciones individuales y comunicaciones con los participantes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.12 Procedimientos de cambios en las especificaciones

7.12.1 Procedimiento para los cambios

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.12.2 Circunstancias en las que el OID debe ser cambiado

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.13 Reclamaciones

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.14 Normativa aplicable

Las operaciones y funcionamiento de la TSA del CORPME, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Reglamento UE 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

7.15 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas Cumplimiento de la normativa aplicable

La Autoridad de Aprobación de Políticas tiene la responsabilidad de velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

7.16 Estipulaciones diversas

7.16.1 Cláusula de aceptación completa

Todos los Terceros que Confían asumen en su totalidad el contenido de la última versión de este documento de Prácticas y Políticas.

7.16.2 Independencia

En el caso de que una o más estipulaciones de este documento de Prácticas y Políticas sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas del documento de Prácticas y Políticas careciera ésta de toda eficacia.

7.16.3 Resolución por la vía judicial

Todas las reclamaciones entre usuarios y CORPME deberán ser comunicadas por la parte en disputa a CORPME, con el fin de intentar resolverlo entre las mismas partes.

Para la resolución de cualquier conflicto que pudiera surgir con relación a este documento de Prácticas y Políticas, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Juzgados y Tribunales españoles, con independencia del lugar dónde se hubieran utilizado los certificados emitidos.

7.17 Otras estipulaciones

No estipulado.