



TSA - SIA

Política de Servicio expedición de sellos electrónicos
cualificados de tiempo (TSA)

OID: 1.3.6.1.4.1.39131.10.1.6

Versión: 1.5



AVISO LEGAL

Toda la información contenida en el presente documento y sus anexos, tiene carácter confidencial, y sólo puede ser utilizada con el fin de ser evaluada por el destinatario (sea cliente, proveedor, colaborador, partner, etc.) de la misma y a los solos efectos de conducir los tratos comerciales, o de otra naturaleza, que motivan el envío del documento (en lo sucesivo, el “Propósito”).

La información aquí presentada es elaborada por SISTEMAS INFORMATICOS ABIERTOS, S.A.U., (en adelante SIA) sociedad perteneciente al Grupo Indra, con C.I.F. A82733262 y domicilio en Av. de Bruselas, 35, 28108 Alcobendas (Madrid), España y anula y sustituye a las anteriores, y es constitutiva de secreto empresarial (también denominado en determinadas jurisdicciones, secreto comercial), y además, puede estar protegida por derechos de autor, derechos afines, patente, modelo de utilidad y/o diseño industrial por lo que queda terminantemente prohibida su divulgación y/o transmisión a terceros sin el permiso previo, expreso y por escrito de SIA.

Se limitará al máximo el acceso a la información confidencial por parte del personal del destinatario de la misma, o del personal de aquellos terceros a los que SIA haya autorizado a acceder a la información confidencial, limitándose únicamente a aquellas personas cuyo acceso resulte estrictamente necesario, y debiendo el destinatario de la información confidencial garantizar que informa a dichas personas del carácter confidencial y propietario de la información así como del Propósito, asegurando que dicho personal trata la información confidencial única y exclusivamente para el Propósito, y absteniéndose de toda divulgación. Una vez finalizado o concluido el Propósito, el cliente debe restituir a SIA toda la información confidencial sin conservar ninguna copia de la misma, no pudiendo utilizar de ninguna manera, ni para ningún fin la información confidencial y/o propietaria facilitada por SIA salvo que haya sido autorizado para ello previa y expresamente por escrito por SIA.

El destinatario de la información confidencial, después de finalizado el Propósito, no podrá utilizar de ninguna manera ni para ningún fin la información confidencial y/o propietaria facilitada por SIA.

Copyright © 2022 SIA. Todos los derechos reservados. España

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

| Revisión | Fecha | Autor | Descripción |
|----------|-------------------------|-------|---|
| 1.0 | 22 de octubre de 2015 | SIA | Primera versión del documento |
| 1.1 | 18 de febrero de 2017 | SIA | Se alinea perfil y política de certificación con eIDAS, nuevas normas técnicas y RFCs. |
| 1.2 | 11 de junio de 2019 | SIA | Corrección sobre los puntos de distribución de CRLs. |
| 1.3 | 17 de noviembre de 2020 | SIA | Revisión erratas. Adecuación a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. |
| 1.4 | 20 de mayo de 2022 | SIA | Se incluye nuevo certificado de TSU TSAQC 2022 de SIA |
| 1.5 | 16 de enero de 2023 | SIA | Cambio de plantilla y actualización de domicilio social |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

INDICE

| | |
|--|-----------|
| 1. INTRODUCCIÓN | 7 |
| 1.1 RESUMEN | 7 |
| 1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN | 7 |
| 1.3 ENTIDADES Y PERSONAS INTERVINIENTES | 8 |
| 1.3.1 Autoridad de Certificación / Prestador cualificado de Servicios de Confianza | 8 |
| 1.3.2 Autoridades de Sellado de tiempo | 8 |
| 1.3.3 Suscriptor | 9 |
| 1.3.4 Terceras Partes | 9 |
| 1.4 USO DE LOS SELLADOS DE TIEMPO | 9 |
| 1.4.1 Usos apropiados y permitidos de los sellados de tiempo | 9 |
| 1.4.2 Limitaciones y restricciones en el uso de los sellados de tiempo | 9 |
| 1.5 ADMINISTRACIÓN DE POLÍTICAS | 10 |
| 1.5.1 Organización responsable | 10 |
| 2. ASPECTOS GENERALES | 11 |
| 2.1 SERVICIO DE SELLADO DE TIEMPO | 11 |
| 2.1.1 Componentes del servicio | 11 |
| 2.1.2 Acceso al servicio | 11 |
| 2.2 FUENTES DE TIEMPO FIABLE | 11 |
| 2.2.1 Precisión en la emisión de sellos de tiempo | 12 |
| 2.3 GENERACIÓN DE CLAVES DE LA TSA | 12 |
| 3. PROCESO DEL SELLADO DE TIEMPO | 13 |
| 3.1 SERVICIOS | 13 |

| | |
|--|-----------|
| 3.2 EMISIÓN DE PETICIONES | 13 |
| 3.2.1 Formato de petición | 13 |
| 3.3 GENERACIÓN DE RESPUESTAS | 13 |
| 3.3.1 Formato de respuesta..... | 14 |
| 3.3.2 Verificación de un sellado de tiempo..... | 15 |
| 4. PERFILES DEL CERTIFICADO | 16 |
| 4.1 PERFIL DE CERTIFICADO | 16 |
| 4.1.1 Número de versión | 16 |
| 4.1.2 Extensiones del certificado | 16 |
| 4.1.3 Identificadores de objeto (OID) de los algoritmos | 17 |
| 4.1.4 Formatos de nombre | 17 |
| 4.1.5 Identificador de objeto (OID) de la Política de Certificación | 17 |
| 4.1.6 Sintaxis y semántica de los “PolicyQualifier” | 17 |
| 4.1.7 Tratamiento semántico para la extensión “Certificate Policy” | 18 |
| 4.2 CERTIFICADOS DE SERVICIO DE EXPEDICIÓN DE SELLOS ELECTRÓNICOS CUALIFICADOS DE TIEMPO (TSA) | 18 |
| 4.2.1 Certificado de TSU TSA QC..... | 18 |
| 4.2.2 Certificado de TSU TSA QC 2022 | 20 |
| 5. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD | 23 |
| 5.1 TARIFAS | 23 |
| 5.1.1 Tarifas de emisión de sellos de tiempo o renovación | 23 |
| 5.1.2 Política de reembolso..... | 23 |

RELACION DE TABLAS

| | |
|--|----|
| Tabla 1 - Datos identificación Política de sellado de tiempo | 8 |
| Tabla 2 - Organización responsable | 10 |
| Tabla 3 - Formato emisión de peticiones | 13 |
| Tabla 4 - Formato de respuestas..... | 15 |
| Tabla 5 - OID política de certificados de sellado de tiempo | 17 |
| Tabla 6 - Perfil certificado | 20 |
| Tabla 7 - Perfil certificado TSAQC 2022 | 22 |

1. Introducción

1.1 Resumen

El presente documento recoge la Política correspondiente al servicio de sellado de tiempo de la Autoridad de Certificación (en adelante AC) del prestador de servicios de confianza (TSP), Sistemas Informáticos Abiertos Sociedad Anónima (en adelante SIA), que emite certificados cualificados según:

- Reglamento (UE) N° 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 (en adelante eIDAS) y por el 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.

En este contexto, se establecen las reglas a emplear por el Servicio de expedición de sellos electrónicos cualificados de tiempo, conforme a la norma ETSI 319 421 “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”, ETSI 319 422 “Time-stamping protocol and time-stamp token profiles” y al documento RFC-3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol”.

Esta política, sirve de guía en la relación entre SIA y las partes conjuntas a los suscriptores de los servicios telemáticos. En consecuencia, todas las partes involucradas tienen la obligación de conocer esta política y ajustar su actividad a lo dispuesto en la misma.

En esta Política se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (en adelante DPC) del Prestador de Servicios de Confianza SIA, conteniendo las reglas a las que se sujeta el uso del servicio definido, así como el ámbito de aplicación y las características técnicas.

Esta PC asume que el lector conoce los conceptos básicos de PKI, certificado y firma electrónica, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2 Nombre del documento e identificación

| | |
|-----------------------|---|
| Nombre del documento | Política de Servicio expedición de sellos electrónicos cualificados de tiempo |
| Versión del documento | 1.5 |
| Estado del documento | Vigente |
| Fecha de emisión | 16/01/2023 |
| Fecha de caducidad | No aplicable |

| | |
|--------------------------|---|
| OID | 1.3.6.1.4.1.39131.10.1.6 |
| Ubicación de la Política | https://psc.sia.es/ |
| DPC relacionada | Declaración de Prácticas de Certificación de la PKI de SIA OID 1.3.6.1.4.1.39131.10.1.1.1.0 Disponible en https://psc.sia.es/ |

Tabla 1 - Datos identificación Política de sellado de tiempo

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

- SIA como Autoridad de Certificación / Prestador de Servicios de Confianza, emisor del certificado de TSA.
- SIA como órgano competente de la Autoridad de Sellado de Tiempo (TSA).
- Los Suscriptores.
- Las Terceras partes aceptantes de los certificados y sellos de tiempo emitidos.

1.3.1 Autoridad de Certificación / Prestador cualificado de Servicios de Confianza

SIA actúa como Autoridad de Certificación (AC) relacionando una determinada clave pública con un sujeto o entidad concretos a través de la emisión de certificados electrónicos.

Las Autoridades de Certificación que componen la PKI de SIA son:

- “AC raíz” Autoridad de Certificación de primer nivel. Esta AC solo emite certificados para sí misma y sus AC Subordinadas, la excepción de la emisión del certificado de validación de OCSP y la emisión de la ARL. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.
- “AC subordinada”: Autoridad de Certificación subordinada de “AC raíz”. Su función es la emisión de certificados electrónicos, como por ejemplo la emisión del Certificado de Servicio expedición de sellos electrónicos cualificados de tiempo (TSA).

1.3.2 Autoridades de Sellado de tiempo

La Autoridad de Sellado de Tiempo, es el elemento de confianza, que actúa como tercera parte vinculando una representación de un dato electrónico a una fecha y hora concretos, garantizando que el dato electrónico existió en un determinado tiempo mediante la expedición de tokens de sellos de tiempo.

1.3.3 Suscriptor

Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sellado de Tiempo. Por medio de un convenio podrán solicitar sellos durante un periodo de tiempo estipulado, o bien si acuerdan otras condiciones de contratación, por ejemplo por volumen de sellos solicitados.

1.3.4 Terceras Partes

Las terceras partes aceptantes, son las personas físicas o entidades que deciden aceptar y confiar en un sello de tiempo emitido por la autoridad de sellado de tiempo de SIA. Y como tales, les es de aplicación lo establecido por la presente Política de sellado de tiempo cuando deciden confiar en estos.

1.4 Uso de los sellados de tiempo

Un sello emitido por la Autoridad de sellado de tiempo de SIA sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en esta Política y en la correspondiente Declaración de Prácticas de Certificación, por lo que existen ciertas limitaciones en el uso de estos, dado que se emplean para garantizar la existencia de datos electrónicos en un determinado tiempo de cualquier organismo o entidad con el que se haya formalizado un convenio de certificación.

Los certificados emitidos bajo los criterios de esta política están indicados para soportar firma electrónica avanzada con certificados cualificados, tal y como está definido en los artículos 36 y 37 de eIDAS, garantizando lo siguiente para todas las firmas:

- a) estar vinculada al firmante de manera única;
- b) permitir la identificación del creador de la firma;
- c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
- d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

1.4.1 Usos apropiados y permitidos de los sellados de tiempo

El sellado deben emplearse para cualquier tipo de documento firmado o no electrónicamente, y para cualquier tipo de objeto digital, inclusive código ejecutable, garantizándose la existencia de dicho contenido en un determinado tiempo.

Otro uso permitido de sellado, es para el resellado, es decir, solicitud de un sello sobre otro anteriormente expedido.

1.4.2 Limitaciones y restricciones en el uso de los sellados de tiempo

De forma general según lo establecido en la Declaración de Prácticas de Certificación de SIA, y tras aceptar sus condiciones de uso.

De forma específica, cabe reseñar que este sello de tiempo será utilizado por los firmantes en las relaciones que mantengan con terceros que confían, y en conformidad con sus limitaciones de uso.

1.5 Administración de Políticas

1.5.1 Organización responsable

Esta Política es propiedad de SIA.

| Nombre | SIA |
|------------------|---|
| Dirección correo | psc@sia.es |
| Dirección postal | Avenida de Bruselas, 35 28108 Alcobendas - Madrid (España) |
| Teléfono | +34 91 307 79 97 |

Tabla 2 - Organización responsable

2. Aspectos Generales

2.1 Servicio de sellado de tiempo

El sellado de tiempo 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. Este protocolo se describe en el RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol” y está en el registro de estándares de Internet.

Una Autoridad de Sellado de Tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos y normalmente se apoya en un software generador de tokens de tiempo.

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

- El cliente calcula el hash del documento a sellar. Los algoritmos de hashes soportados actualmente son SHA-1, SHA-256 y SHA-512.
- El cliente envía una solicitud de sello de tiempo a una URL determinada siguiendo el protocolo RFC 3161, incluyendo el hash del documento a sellar.
- La TSA recibe la petición, revisa si la petición está completa y correcta.
- 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 guardarlo debidamente.
- La TSA mantiene un registro de los sellos emitidos para su futura verificación.

2.1.1 Componentes del servicio

Los dos componentes de la TSA, en que se resumen principalmente la prestación del servicio son:

- TSU, componente del sistema de TSA encargado de proteger y generar los Sellos de Tiempo en nombre de la TSA.
- Fuente de tiempo fiable, que determine el instante de creación de dicho sello de tiempo de manera fehaciente.

2.1.2 Acceso al servicio

Todo acceso al servicio, va a ser filtrado por medio de una conexión TLS con autenticación con certificado de cliente. Y contrastando el direccionamiento IP Origen, dando solamente acceso a aquellos que hayan firmado el convenio con el prestador de servicios de confianza.

2.2 Fuentes de tiempo fiable

La TSA cuenta con acceso a una fuente de tiempo que garantice la fiabilidad en el proceso de obtención del instante temporal empleado en la creación del sello de tiempo. Para ellos la TSA de

SIA está conectada con una fuente de tiempo “stratum 1”, a través del protocolo NTP. Esta fuente de tiempo provee precisión a nivel del microsegundo utilizando sincronización con sistemas vía satélite. El sistema de sincronización está preparado para realizar ajustes de segundo intercalar siempre el que la fuente de tiempo fiable notifique la necesidad de dicho ajuste.

2.2.1 Precisión en la emisión de sellos de tiempo

La TSA emite sellados de tiempo con una precisión de tiempo contando con un desfase permitido por debajo del segundo. Esta precisión esta monitorizada constantemente para evitar desvinculaciones derivadas de latencias anormales en la sincronización con la fuente o desfases en los relojes internos de los equipos. En caso de detectar una desincronización horaria, el servicio de sellado de tiempo se parará.

2.3 Generación de claves de la TSA

La TSA de SIA, ha generado sus claves criptográficas bajo el exclusivo control del personal de confianza de la propia Autoridad de Certificación SIA. Para ello, dichas claves han sido creadas dentro de un módulo criptográfico de seguridad hardware (HSM) cumpliendo con FIPS 140-2 Nivel 3, dichos dispositivos son resistentes a manipulaciones intrusivas a nivel hardware (tamper protection).

La copia de seguridad de las claves se realiza en las mismas condiciones de seguridad en las que fueron creadas.

De acuerdo con las prácticas comunes se utilizaran los Algoritmos criptográficos apropiados para la creación de la clave de firma y su longitud correspondiente.

Para los procesos de cese, la clave será destruida. Siendo el certificado asociado revocado previamente en el caso de que la fecha de expiración del mismo siga siendo válida.

En todo momento sólo existirá un único par de claves activo en el dispositivo criptográfico para la creación de sellados de tiempo. Este par de claves sólo será accedido y utilizado por la TSA.

3. Proceso del Sellado de Tiempo

3.1 Servicios

La plataforma de TimeStamp está orientada a Servicio mediante protocolo HTTPS y formato ASN1; se puede encontrar la siguiente funcionalidad:

Generación de sellos de tiempo en formato ASN1 conforme al RFC3161.

En el caso que las claves o el certificado estén caducados, el servicio de TimeStamp no estará disponible.

3.2 Emisión de peticiones

Los clientes deben enviar sus peticiones a través del protocolo https, conformando una petición de sellado de tiempo (time-stamping request) en formato ASN1 y enviarla según corresponda a la URL:

- Para TSAQC: <https://host:port/tspTSA>
- Para TSAQC 2022: <https://host:port/tspTSA2022>

3.2.1 Formato de petición

El formato de la petición se define en el RFC3161 y debe ser una estructura ASN1 definida como:

```

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 }

TSAPolicyId ::= OBJECT IDENTIFIER
  
```

Tabla 3 - Formato emisión de peticiones

3.3 Generación de respuestas

El módulo de TimeStamp, una vez validada la petición, genera una respuesta ASN1. Para la emisión de la respuesta, es preciso que el certificado esté disponible y se encuentre dentro de su periodo de validez.

3.3.1 Formato de respuesta

El formato de la 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),
    addInfoNotAvailable (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
}

Accuracy ::= SEQUENCE {

```

| | | |
|---------|----------------------|------------|
| seconds | INTEGER | OPTIONAL, |
| millis | [0] INTEGER (1..999) | OPTIONAL, |
| micros | [1] INTEGER (1..999) | OPTIONAL } |

Tabla 4 - Formato de respuestas

En el campo extensions del token se incorpora la información de que se trata de un sellado de tiempo cualificado y emitido conforme a la norma 910/2014 (eIDAS):

esi4-qtstStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-tsts-EuQCompliance }

3.3.2 Verificación de un sellado de tiempo

La verificación de un sellado de tiempo emitido por este servicio requiere de las siguientes tareas:

- Verificación de la integridad del sellado. La firma ha de ser correcta.
- Verificación el periodo de validez del certificado. El servicio no emite sellados con el certificado caducado, pero los terceros deben verificar que no se ha empleado un certificado fuera del periodo de validez establecido por la TSA.
- Verificación del estado de revocación del certificado de sellado, así como de las extensiones del mismo que indican que su uso es el de sellado de tiempo.

4. Perfiles Del Certificado

4.1 Perfil de certificado

Se ha tenido en cuenta los siguientes estándares y normas europeas en la definición de los certificados de sellado de tiempo emitidos por los sistemas de SIA:

- ETSI EN 319 421: “Policy and Security Requirements for Trust Service Providers issuing Time- Stamps”.
- RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”.
- ETSI EN 319 422 “Time-stamping protocol and time-stamp token profiles”.
- ETSI EN 319 412-1 “Certificate Profiles; Part 1: Overview and common data structures”.
- ETSI EN 319 412-3 “Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons”.
- ETSI EN 319 412-5 “Certificate Profiles; Part 5: QCStatements”.
- ETSI TS 119 312 “Cryptographic Suites”.

4.1.1 Número de versión

El certificado sigue el estándar definido X.509 versión 3.

4.1.2 Extensiones del certificado

Los certificados emitidos por SIA de sellado de tiempo, vinculan la identidad de la entidad de sellado de tiempo a una determinada clave pública, sin incluir ningún tipo de atributos en el mismo. Para garantizar la autenticidad y no repudio, toda esta información estará firmada electrónicamente por el prestador de servicios de certificación encargado de la emisión.

Los campos singulares para identificar al certificado de sellado de tiempo son:

- Versión.
- Serial Number.
- Signature.
- Issuer (Emisor).
- Validity.
- Subject (Asunto).
- Subject Public Key Info.

Las extensiones utilizadas en los certificados son:

- Authority Key Identifier.
- Subject Key Identifier.

- KeyUsage. Calificada como crítica.
- ExtKeyUsage.
- CRL Distribution Point.
- Authority Information Access.
- CertificatePolicies.

4.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador del algoritmo criptográfico con Objeto (OID): SHA-256 with RSA Encryption (1.2.840.113549.1.1.11) de 2048 Bits para TSAQC.

Identificador del algoritmo criptográfico con Objeto (OID): SHA-256 with RSA Encryption (1.2.840.113549.1.1.11) de 3072 Bits para TSAQC 2022.

4.1.4 Formatos de nombre

Los certificados emitidos por SIA contienen el “distinguished name X.500” del emisor y del titular del certificado en los campos “issuer” y “subject” respectivamente.

4.1.5 Identificador de objeto (OID) de la Política de Certificación

El OID de la presente PC es 1.3.6.1.4.1.39131.10.1.6.

Los identificadores de los certificados expedidos para la presenta Política de sellado de tiempo son los siguientes:

| | |
|--|---------------------------|
| Política del certificado de sellado de tiempo TSAQC | 1.3.6.1.4.1.39131.10.1.14 |
| QCP-I | 0.4.0.194112.1.1 |
| Política del certificado de sellado de tiempo TSAQC 2022 | 1.3.6.1.4.1.39131.10.1.25 |
| NCP+ | 0.4.0.2042.1.2 |

Tabla 5 - OID política de certificados de sellado de tiempo

En cumplimiento con el apartado 5.2 de ETSI EN 319 421, el OID de esta política identifica a la misma como “best-practices-ts-policy”.

4.1.6 Sintaxis y semántica de los “PolicyQualifier”

La extensión “Certificate Policies” contiene los siguientes “Policy Qualifiers”:

- URL DPC: contiene la URL donde puede obtener la última versión de la DPC y de las Políticas de Certificación asociadas.

- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

4.1.7 Tratamiento semántico para la extensión “Certificate Policy”

La extensión “Certificate Policy” permite identificar la política y el tipo de certificado asociado al certificado.

4.2 Certificados de Servicio de expedición de sellos electrónicos cualificados de tiempo (TSA)

e)

4.2.1 Certificado de TSU TSA QC

| Certificado de sellado de tiempo (TSA) | | |
|--|---|---------------|
| Nombre atributo | Valor | Observaciones |
| Campos x509 v1 | | |
| Versión | V3 | |
| Serial Number | Número secuencial único, asignado automáticamente por la AC subordinada emisora | |
| Signature Algorithm | SHA-256 con RSA-2048 | |
| Issuer Distinguished Name (Emisor) | | |
| Country (C) | ES | |
| Organization (O) | SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA | |
| Organizational Unit (OU) | QUALIFIED CA | |
| Serial Number (serialNumber) | A82733262 | |
| Common Name (CN) | SIA SUB01 | |
| Validity | | |
| Not Before | Fecha de emisión del certificado | |
| Not After | Fecha de emisión + 3 años | |
| Subject (Asunto) | | |
| Country (C) | ES | |

| | | |
|-------------------------------------|---|--|
| Organization (O) | SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA | |
| Organizational Unit (OU) | QUALIFIED CA | |
| Organization Identifier (OI) | VATES-<NIF de la ENTIDAD> | |
| Common Name (CN) | TSAQC | |
| Subject Public Key Info | Clave pública (RSA-2048 Bits), codificada de acuerdo con el algoritmo criptográfico | |
| Extensiones x509 v3 | | |
| Authority Key Identifier | Identificador de la clave pública del emisor | |
| Subject Key Identifier | Identificador de la clave pública del firmante del certificado | |
| KeyUsage | | Marcado como crítica |
| Digital Signature | 1 (seleccionado) | SI |
| Content Commitment (nonRepudiation) | 1 (seleccionado) | SI |
| Key Encipherment | 0 (no seleccionado) | |
| Data Encipherment | 0 (no seleccionado) | |
| Key Agreement | 0 (no seleccionado) | |
| Key Certificate Signature | 0 (no seleccionado) | |
| CRL Signature | 0 (no seleccionado) | |
| EncipherOnly | 0 (no seleccionado) | |
| DecipherOnly | 0 (no seleccionado) | |
| ExtendedKeyUsage | | Marcado como crítica |
| Impresión de fecha | OID: 1.3.6.1.5.5.7.3.8 | SI |
| CRL Distribution Point | | |
| Distribution Point 1 | http://psc.sia.es/crlc[N].crl | N es el número correspondiente a la CRL particionada |
| Distribution Point 2 | https://psc.sia.es/crlc[N].crl | N es el número correspondiente a |

| | | |
|----------------------------------|--|-------------------------|
| | | la CRL particionada |
| Authority Info Access | | |
| Access Method | id-ad-calssuers | |
| Access Method | https://psc.sia.es/ac_sub01.crt | |
| Access Method | Id-ad-ocsp | |
| Access Location | https://psc.sia.es/ocsp | |
| Qualified Certificate Statements | | |
| QcCompliance | OID 0.4.0.1862.1.1 | Certificado cualificado |
| QcEuRetentionPeriod | 15 años | Duración custodia |
| QCSyntax-v2 | OID 1.3.6.1.5.5.7.11.2 | |
| id-etsi-qcs-SemanticsId-Legal | OID 0.4.0.194121.1.2 | |
| QcType | OID 0.4.0.1862.1.6 | |
| id-etsi-qct-eseal | OID 0.4.0.1862.1.6.2 | Certificado de sello |
| QcPDS | OID 0.4.0.1862.1.5 | |
| PdsLocation | https://psc.sia.es/en (en) | |
| Certificate Policies | | |
| Policy Qualifier ID | Especificación de la DPC | |
| CPS Pointer | https://psc.sia.es | |
| User Notice | “Certificado de servicio expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: https://psc.sia.es ” | |
| Policy Identifier | QCP-l | |
| Policy Identifier | 1.3.6.1.4.1.39131.10.1.14 | |

Tabla 6 - Perfil certificado

4.2.2 Certificado de TSU TSA QC 2022

Será renovado a los 5 años.

| Certificado de sellado de tiempo (TSA) | | |
|--|-------|---------------|
| Nombre atributo | Valor | Observaciones |
| Campos x509 v1 | | |

| | | |
|------------------------------------|---|----------------------|
| Versión | V3 | |
| Serial Number | Número secuencial único, asignado automáticamente por la AC subordinada emisora | |
| Signature Algorithm | SHA-256 con RSA-3072 | |
| Issuer Distinguished Name (Emisor) | | |
| Country (C) | ES | |
| Organization (O) | SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA | |
| Organizational Unit (OU) | QUALIFIED CA | |
| Serial Number (serialNumber) | A82733262 | |
| Common Name (CN) | SIA SUB01 | |
| Validity | | |
| Not Before | Fecha de emisión del certificado | |
| Not After | Fecha de emisión + <=10 años | |
| Subject (Asunto) | | |
| Country (C) | ES | |
| Organization (O) | SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA | |
| Organizational Unit (OU) | QUALIFIED CA | |
| Organization Identifier (OI) | VATES-<NIF de la ENTIDAD> | |
| | | |
| Common Name (CN) | TSAQC 2022 | |
| Subject Public Key Info | Clave pública (RSA-3072 Bits), codificada de acuerdo con el algoritmo criptográfico | |
| Extensiones x509 v3 | | |
| Authority Key Identifier | Identificador de la clave pública del emisor | |
| Subject Key Identifier | Identificador de la clave pública del firmante del certificado | |
| KeyUsage | | Marcado como crítica |
| Digital Signature | 1 (seleccionado) | SI |

| | | |
|-------------------------------------|--|--|
| Content Commitment (nonRepudiation) | 1 (seleccionado) | SI |
| Key Encipherment | 0 (no seleccionado) | |
| Data Encipherment | 0 (no seleccionado) | |
| Key Agreement | 0 (no seleccionado) | |
| Key Certificate Signature | 0 (no seleccionado) | |
| CRL Signature | 0 (no seleccionado) | |
| EncipherOnly | 0 (no seleccionado) | |
| DecipherOnly | 0 (no seleccionado) | |
| ExtendedKeyUsage | | Marcado como crítica |
| Impresión de fecha | OID: 1.3.6.1.5.5.7.3.8 | SI |
| CRL Distribution Point | | |
| Distribution Point 1 | http://psc.sia.es/crlc[N].crl | N es el número correspondiente a la CRL particionada |
| Distribution Point 2 | https://psc.sia.es/crlc[N].crl | N es el número correspondiente a la CRL particionada |
| Authority Info Access | | |
| Access Method | id-ad-calssuers | |
| Access Method | https://psc.sia.es/ac_sub01.crt | |
| Access Method | Id-ad-ocsp | |
| Access Location | https://psc.sia.es/ocsp | |
| Certificate Policies | | |
| Policy Qualifier ID | Especificación de la DPC | |
| CPS Pointer | https://psc.sia.es | |
| User Notice | “Certificado de servicio expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: https://psc.sia.es ” | |
| Policy Identifier | 0.4.0.2042.1.2 | |
| Policy Identifier | 1.3.6.1.4.1.39131.10.1.25 | |

Tabla 7 - Perfil certificado TSAQC 2022

5. Otras Cuestiones Legales y de Actividad

5.1 Tarifas

5.1.1 Tarifas de emisión de sellos de tiempo o renovación

SIA como autoridad de sellado de tiempo (TSA) aplicará a los organismos o entidades las tarifas aprobadas para la prestación de dicho servicio o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizados para tal efecto.

5.1.2 Política de reembolso

La política de reembolso vendrá detallada, como parte de las tarifas acordadas, en el convenio o encomienda de gestión formalizados para tal efecto.



An Indra company

Persona de contacto
psc@sia.es

Av. de Bruselas, 35
28108 Alcobendas, Madrid
T +34 91 307 79 97

sia.es