CONFIRMA

POLÍTICA DE CERTIFICACIÓN DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO DEL PCSC CONFIRMA S.A.

VERSIÓN: 1.0

CLASE: PÚBLICO

CONTROL DOCUMENTAL

NOMBRE DEL ARCHIVO:	
POLITICA DE CERTIFICACION DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO DEL PCSC CONFIRMA S.A.	
CÓDIGO: **DOC-PC -SCTE**	**VERSIÓN:** **1.0**
UBICACIÓN FISICA: **CONFIRMA S.A.**	**FECHA:** **18/03/24**
CLASIFICACION DE SEGURIDAD: **Público**	

CONTROL DE VERSIONES			
FECHA	**VERSION**	**RESPONSABLES**	**MOTIVO DE CAMBIO**
18/03/24	1.0	CONFIRMA S.A.	Primera Edición del Documento

DISTRIBUCIÓN DEL DOCUMENTO	
ÁREA	**NOMBRES**
Personal con Rol de Confianza establecidos en la DPC del PCSC CONFIRMA S.A.	PCSC de CONFIRMA S.A.
Documento Público	https://www.confirma.com.py/wp-content/uploads/2024/03/PC_Politica_de_Certificacion_SelloTiempo_Confirma_SA.pdf

PREPARADO POR:	REVISADO POR:	APROBADO POR:
UANATACA S.A.	CONFIRMA S.A.	CONFIRMA S.A.

INDICE

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Este documento forma parte de un conjunto de normas técnicas elaboradas a los efectos de reglamentar la creación, verificación y validación de sellos cualificados de tiempo electrónicos (SCTE), y certificados relativos a este servicio, en el ámbito de la ICPP. Este conjunto consta de las siguientes documentaciones:

a) REQUISITOS MÍNIMOS PARA LA DECLARACIÓN DE PRÁCTICAS DE SELLO CUALIFICADO DE TIEMPO DE LA ICPP; DOC-ICPP-25[1]

b) REQUISITOS MÍNIMOS PARA LA POLÍTICA DE SELLO CUALIFICADO DE

TIEMPO ELECTRÓNICO DE LA ICPP; DOC-ICPP-26

c) NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA ICPP; DOC-ICPP-06 [2]

Para la prestación del servicio el Prestador requerirá contar con un certificado emitido por la AC Raíz-Py.

Aprobada la habilitación del servicio de Sello Cualificado de Tiempo Electrónico (SCTE), el PCSC CONFIRMA S.A. emitirá un certificado electrónico para el Servidor de Sello Cualificado de Tiempo Electrónico (SSTE) conforme al perfil indicado en el ítem 7 del presente documento.

Sello de tiempo electrónico, conforme la Ley N° 6822/2021, se define como datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

Sello Cualificado de Tiempo Electrónico (SCTE) se denomina a un sello de tiempo electrónico que debe vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte, basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado y haber sido firmada mediante el uso de una firma electrónica o sellada con un sello electrónico del Prestador Cualificado de Servicios de Confianza (PCSC) o por cualquier método equivalente. El SCTE garantiza y da certeza de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas. Este servicio no tiene acceso a la información sobre la cual se crea el SCTE. La prestación de este servicio requiere una petición previa por parte del suscriptor de SCTE (remisión de conjunto de datos) a lo que se debe contestar con la evidencia electrónica correspondiente.

Los SCTE son emitidos por los PCSC, cuyas operaciones deben ser debidamente documentadas y auditadas periódicamente por un OEC acreditado en el marco de la ICPP y cumplir con los requisitos siguientes:

a) Vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte.
b) Basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado.
c) Haber sido firmada mediante el uso de una firma electrónica o sellada con un sello electrónico de un PCSC.

CONFIRMA S.A. declara en este documento la Fuente Confiable de Tiempo (FCT) que utiliza, la misma podrá consumir de una fuente oficial de tiempo establecida en la República del Paraguay o extranjera y al igual que su Servidor de Sello de Tiempo (SSTE) debe contar con la

autorización correspondiente de la Autoridad de Aplicación. Los relojes de los SSTE deben ser auditados y sincronizados por el PCSC conforme lo dispuesto en el ítem 6.5.5 del DOCICPP-25 [1]

El uso de SCTE en el ámbito de ICPP es opcional. El documento firmado o sellado con firma electrónica cualificada o sello electrónico cualificado con una clave privada, correspondiente a certificados cualificados en el ámbito de la ICPP son válidos con o sin sello cualificado de tiempo electrónico.

Este documento denominado PC-SCTE describe las prácticas y procedimientos adoptados por el PCSC CONFIRMA S.A. en el desempeño de sus funciones y en la prestación del servicio de expedición de sello cualificado de tiempo electrónico. De modo general, la política de sellos cualificado de tiempo electrónico indica "lo que debe lograrse", mientras que una declaración de práctica indica "cómo cumplir", es decir, los procesos que utilizará el PCSC para crear sellos de tiempo y mantener su reloj preciso.

Este documento se basa en las reglas de RFC 3628 y 3161, del IETF y los estandares ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Timestamping protocol and time-stamp token profiles y ETSI EN 319 421 V1.2.1 (2023-05) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre del Documento	POLITICA DE CERTIFICACION DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO DEL PCSC CONFIRMA S.A.
Versión del Documento	V1.0
Fecha de Aprobación	18/03/2024
OID (Object Identifier):	1.3.6.1.4.1.58404.1.4.1.1
Ubicación de la DPC relacionada	https://www.confirma.com.py/wp-content/uploads/2024/03/PC_Politica_de_Certificacion_SelloTiempo_Confirma_SA.pdf

1.3. PARTICIPANTES DE LA ICPP

1.3.1. PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA (PCSC)

El PCSC integrante de la ICPP a la que se refiere esta PC – SCTE es el PCSC CONFIRMA S.A.

1.3.2. AGENTE DE ATENCIÓN DEL SERVICIO

La figura del Agente de atención al servicio que es el Personal vinculado al PCSC CONFIRMA S.A. mediante un contrato cuya función es la recepción y trámite de solicitudes vinculadas al servicio.

1.3.3. SUSCRIPTORES

Son todas las personas físicas o jurídicas que podrán solicitar SCTE emitidos por el PCSC CONFIRMA S.A., de conformidad con esta PC-SCTE y que acepta los términos del servicio.

1.3.4. PARTE USUARIA

Se refiere a un tercero (persona física o jurídica) que confía en el contenido, vigencia y aplicabilidad del SCTE emitido en el marco de la ICPP. La Parte Usuaria debe verificar la validez de los certificados en la cadena de certificación.

1.3.5. PRESTADOR DE SERVICIOS DE SOPORTE (PSS)

Los PSS son entidades externas a las que recurre el PCSC para desempeñar todas o parte de las actividades descritas en esta PC-SCTE. Los PSS se clasifican en tres categorías, conforme al tipo de actividades prestadas;

a) disponibilización de infraestructura física y lógica;

b) disponibilización de recursos humanos especializados; y

c) disponibilización de infraestructura física y lógica y de recursos humanos especializados.

El funcionamiento de un PSS vinculado a un PCSC mediante un acuerdo operacional deberá ser autorizado por la AC Raíz-Py.

El PCSC mantiene publicada información referente a:

- Lista de todos los PSSs habilitados

https://www.confirma.com.py/prestadores-de-servicios-de-soporte/

- Lista de los PSSs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

1.4. USO DEL CERTIFICADO

El PCSC COMFIRMA S.A. implementa las siguientes políticas de certificación:

https://www.confirma.com.py/wp-content/uploads/2024/03/PC_Politica_de_Certificacion_SelloTiempo_Confirma_SA.pdf

1.5. ADMINISTRACION DE LA POLITICA

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre: CONFIRMA S.A.

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

Teléfono: (+595 21) 218 0 218

Dirección de correo electrónico: info@confirma.com.py

Página Web: https://www.confirma.com.py/

1.5.2 PERSONA DE CONTACTO

Nombre: GERENTE DE CONFIRMA S.A.

Teléfono: (+595 21) 218 0 218

Página web: https://www.confirma.com.py/

E-mail: info@confirma.com.py

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

1.5.3 PERSONA QUE DETERMINA LA ADECUACIÓN DEL PCSC A LA PC

Nombre: GERENTE DE CONFIRMA S.A.

Teléfono: (+595 21) 218 0 218

Página web: https://www.confirma.com.py/

E-mail: info@confirma.com.py

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA PC-SCTE

Toda PC-SCTE debe ser presentada para su aprobación ante la AC Raíz-Py de la ICPP:

- durante el proceso de habilitación como PCSC

● cuando sufriera modificaciones/actualizaciones, presentando la solicitud correspondiente. Cada ítem objeto de modificación/actualización debe ser detallado en el apartado correspondiente del propio documento o en la solicitud pertinente.

1.6. DEFINICIONES, SIGLAS Y ACRONIMOS

1.6.1. DEFINICIONES

1. Autenticación: proceso técnico que permite determinar la identidad de la persona física o jurídica.

2. Autoridad de Aplicación: Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.

3. Autoridad de Certificación: entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC.

4. Autoridad de Certificación Raíz del Paraguay: órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado auto firmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la Autoridad de Aplicación.

5. **Agente de Atención del Servicio**: personal vinculado al PCSC mediante un contrato cuya función es la recepción y trámite de solicitudes vinculadas al servicio.

6. Cadena de certificación: lista ordenada de certificados que contiene un certificado del firmante o creador de sello y certificados de la AC, que termina en un certificado raíz. El emisor del certificado del firmante o creador de sello es el titular del certificado del PCSC y a su vez, el emisor del certificado del PCSC es el titular del certificado de AC Raíz-Py. El

firmante, creador de sello o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.

7. Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley N° 6822/2021.

8. **Certificado cualificado de sello electrónico**: un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley N° 6822/2021.

9. **Cifrado**: es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que sólo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.

10. **Claves criptográficas**: valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

11. **Clave pública** y **privada**: la criptografía en la que se basa la ICPP, es la criptografía asimétrica. En ella, se emplean un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública

y está incorporada en el certificado electrónico, mientras que a la otra se le denomina privada y está bajo exclusivo control del titular o responsable del certificado.

12. Compromiso: violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.

13. Contrato de prestación de servicios de sello cualificado de tiempo electrónico:

Acuerdo entre el PCSC y el suscriptor del servicio que contiene información relativa al solicitante del servicio y además establece los

derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio. Este contrato,
requiere la aceptación explícita de las partes intervinientes.

14. Datos de activación: valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.

15. **Declaración de Prácticas de Certificación**: documento en el cual se determina la declaración de las prácticas que emplea una AC al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la AC para satisfacer los
requisitos especificados en la PC vigente.

16. **Dossier del Suscriptor**: deberá estar conformado por el Contrato de prestación de servicios de sello cualificado de tiempo electrónico y las documentaciones utilizadas para la solicitud o cancelación del servicio.

17. **Firma electrónica cualificada**: una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, 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 estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

18. **Firmante**: una persona física que crea una firma electrónica.

19. Habilitación: autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.

20. **Identificador de Objeto**: sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de

identificación. El árbol de OID se define plenamente en las Recomendaciones UIT-T y las normas internacionales ISO.

21. Infraestructura de Claves Públicas del Paraguay: conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal
para actos electrónicos firmados o cifrados con certificados electrónicos cualificados y claves criptográficas emitidas por esta infraestructura.

22. **Integridad**: característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

23. Lista de Certificados Revocados: lista emitida por una AC, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.

24. Módulo criptográfico: software o hardware criptográfico que genera y almacenas claves criptográficas.

25. **Módulo de Seguridad Criptográfico**: dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.

26. **Normas Internacionales**: requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.

27. **Organismo de Evaluación de Conformidad**: organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los
servicios de confianza que este presta conforme a la Ley N° 6822/2021.

28. **Organismo de Supervisión**: organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios

de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley N° 6822/2021.

29. Parte usuaria: persona física o jurídica que confía en el servicio de confianza.

30. **Perfil del certificado**: especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

31. **Política de Certificación**: documento en el cual la AC define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.

32. **Prestador Cualificado de Servicios de Confianza**: prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.

33. Política de Seguridad: es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, gerenciamiento de riesgos, plan de continuidad de negocio y análisis de registros de eventos de una AC.

34. Prestador de Servicios de Soporte: entidad externa vinculada a un PCSC mediante un acuerdo operacional a la que recurre la AC o la AR y autorizada por la AC Raíz-Py para desempeñar actividades descritas en la DPC o en una PC.

35. **Registro de Auditoría**: registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.

36. **Repositorio**: sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública

Sello cualificado de tiempo electrónico: sello cualificado de tiempo electrónico que debe vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte, basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado y haber sido firmada mediante el uso de una firma electrónica o sellada con un sello electrónico del prestador cualificado de servicios de confianza o por cualquier método equivalente.

38. **Solicitud**: formulario utilizado para la suscripción o cancelación del servicio de sello cualificado de tiempo.

39. **Suscriptor**: persona física o jurídica que adquiere el servicio de sello cualificado de tiempo.

40. Verificación y **validación de firma** o **sello**: determinación y validación de que la firma o sello electrónico fue creado durante el periodo operacional de un certificado válido, por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su creación.

41. X.509: estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2. SIGLAS Y ACRÓNIMOS

-AC: Autoridad de Certificación (AC por sus siglas en inglés, Certificate Authority)

-AC Raíz-Py: Autoridad Certificadora Raíz del Paraguay

-CCTV: Circuito cerrado de TV

-**DP**-**SCTE**: Declaración de prácticas de sello cualificado de tiempo electrónico

-**DGCE**: Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.

-**FCT**: Fuente confiable de tiempo

-**ISO**: Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).

-**LRC**: Lista de certificados revocados (LCR por sus siglas en inglés, CertificateRevocation List)

-**MIC**: Ministerio de Industria y Comercio

-**MSC**: Módulo de seguridad criptográfico

-**OID**: Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)

-**OU**: Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)

-**PKI**: Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).

-**ICPP**: Infraestructura de Claves Públicas del Paraguay

-**OEC**: Organismo de Evaluación de la Conformidad

-**OS**: Organismo de Supervisión

-**PCSC**: Prestador cualificado de Servicios de confianza

-**PCN**: Plan de Continuidad del negocio

-**PC-SCTE**: Política de certificación de sello cualificado de tiempo electrónico

-**PS**: Política de Seguridad

-**PSS**: Prestador de Servicios de Soporte

-**RFC**: Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)

-**SCTE**: Sello cualificado de tiempo electrónico

-**SSTE**: Servidor de Sello de tiempo electrónico

-**UPS**: Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)

-**URL**: Localizador uniforme de recursos (URL por sus siglas en inglés, UniformResource Locator).

-**ETSI**: European Telecommunication Standard Institute

-**ITSEC**: European Information Technology Security Evaluation Criteria

-**ITU**: International Telecommunications Union

-**SNMP**: Simple Network Management Protocol

-**TSP**: Protocolo de Sello de Tiempo (TSP por sus siglas en inglés, Time Stamp Protocol)

-**TSQ**: Solicitud de Sello de Tiempo (TSQ Por sus suglas en inglés, Time Stamp Request)

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

En los apartados siguientes, son referidos en los ítems correspondientes a la DPC de CONFIRMA S.A

2.1. PUBLICACIÓN DE INFORMACIÓN DEL PCSC
2.2. TIEMPO O FRECUENCIA DE PUBLICACIÓN
2.3. CONTROLES DE ACCESO A LOS REPOSITORIOS

3. IDENTIFICACION Y AUTENTICACION

En los apartados siguientes, son referidos en los ítems correspondientes a la DPC de CONFIRMA S.A

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

En el primer paso de este proceso, el suscriptor solicita un SCTE enviando una solicitud (que es o incluye una TSQ) al PCSC CONFIRMA S.A. Luego, en el segundo paso, PCSC CONFIRMA S.A. responde enviando una respuesta (que es o incluye un sello de tiempo) al suscriptor.

4.1. SOLICITUD DE SCTE

Para solicitar un SCTE en un documento electrónico, el suscriptor debe enviar un TSQ que contenga el hash a ser firmado o sellado. A continuación, se detallan los requisitos y procedimientos que deben cumplir y ejecutar los suscriptores:

a) el protocolo de solicitud de sello de tiempo (http, correo electrónico, etc.);

b) los algoritmos hash que pueden utilizar los suscriptores para solicitud de sello de tiempo.

c) solicitud formal de suscripción del servicio.

d) contrato de prestación de servicios de sello cualificado de tiempo electrónico firmado con firma electrónica cualificada del suscriptor del servicio. En caso de imposibilidad técnica de firmar electrónicamente el contrato de prestación de servicio de confianza será aceptada la firma manuscrita del contrato por parte del suscriptor del servicio, en este caso será necesaria la verificación de la firma contra el documento de identificación y se adjuntará al dossier de titular del certificado, el documento manuscrito digitalizado y firmado con firma electrónica cualificada por el AGR, conforme al DOC-ICPP-05.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE SCTE

Como establezca la DPC del PCSC CONFIRMA S.A.

4.1.2. PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Como establezca la DPC del PCSC CONFIRMA S.A.

4.2. EMISIÓN DEL SCTE

Como establezca la DPC del PCSC CONFIRMA S.A.

4.3. ACEPTACIÓN DEL SCTE

A continuación, se detallan los requisitos y procedimientos operativos relacionados con la aceptación de un SCTE recibido por el suscriptor.

Los requisitos y procedimientos son:

Algoritmo del hash insertado.

Procedimiento de verificación del sello cualificado de tiempo electrónico por parte del suscriptor.

Después de recibir la respuesta (que normalmente contiene un sello de tiempo electrónico en un TimeStampResp), el suscriptor debe verificar si hay errores en la respuesta. Si no hay errores, debe verificar los campos del SCTE y la validez de la firma electrónica cualificada del mismo. Es crucial verificar que lo que se selló coincide con lo recibido para sellar. Además, se debe verificar que el SCTE fue emitido por CONFIRMA S.A., y que el hash de los datos y el OID del algoritmo hash son correctos. Luego, se debe verificar el tiempo de la respuesta comparándolo con una fuente de tiempo local confiable o el número de control incluido en la solicitud. Si alguna de estas verificaciones falla, el SCTE debe ser rechazado.

Además, se debe verificar el estado del certificado del SSTE, por ejemplo, consultando la Lista de Certificados Revocados (LCR), para asegurarse de que el certificado sigue siendo válido. El suscriptor también debe analizar el campo "política" para determinar si la política bajo la cual se emitió el sello es aceptable para la solicitud.

4.4. CARACTERÍSTICAS DEL SCTE

Las características de los sellos de tiempo que serán emitidos según PC-SCTE, contienen:

a) la exactitud o precisión mínima de la hora registrada en el sello;

b) la unidad utilizada en el campo genTime del SCTE (segundos, milisegundos o microsegundos).

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

Como establezca la DPC del PCSC CONFIRMA S.A.

Como establezca la DPC del PCSC CONFIRMA S.A.

Como establezca la DPC del PCSC CONFIRMA S.A

Como establezca la DPC del PCSC CONFIRMA S.A

9. OTROS ASUNTOS LEGALES Y COMERCIALES

Como establezca la DPC del PCSC CONFIRMA S.A

9.6.1. REPRESENTACIONES Y GARANTÍAS DE TERCERAS PARTES
9.6.2. CONSENTIMIENTO DE LOS SUSCRIPTORES
9.7. EXENCIÓN DE GARANTÍA
9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL
9.9. INDEMNIZACIONES
9.10. PLAZO Y FINALIZACIÓN
9.10.1. PLAZO
9.10.2. FINALIZACIÓN
9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA
9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES
9.12. ENMIENDAS
9.12.1. PROCEDIMIENTOS PARA ENMIENDAS
Como establezca la DPC del PCSC CONFIRMA S.A
9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN
Como establezca la DPC del PCSC CONFIRMA S.A
9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS
9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS
9.14. NORMATIVA APLICABLE
9.15. ADECUACIÓN A LA LEY APLICABLE
9.16. DISPOSICIONES VARIAS
9.16.1. ACUERDO COMPLETO

Esta PC - SCTE representa las obligaciones y deberes aplicables a CONFIRMA S.A. y autoridades vinculadas.

En caso de conflicto entre esta PC- SCTE y otras resoluciones de la AC Raíz-Py, prevalecerá siempre la última editada

9.16.2. ASIGNACIÓN
9.16.3. INDEPENDENCIA DE LAS DISPOSICIONES

La nulidad o ineficacia de cualquiera de las disposiciones de esta PC – SCTE no afectará a las demás disposiciones, las cuales permanecerán plenamente válidas y eficaces. En este caso, la disposición inválida, nula o ineficaz se tendrá por no escrita, por lo que la presente DPC se

interpretará como si no la contuviera y, en lo posible, manteniendo la intención original de las restantes disposiciones.

10. DOCUMENTOS DE REFERENCIA

10.1. REFERENCIAS EXTERNAS

Ley Nº 6822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos."

● RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.

● RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, november 2003.

● RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.

● ETSI TS 101.861 - v 1.2.1 Technical Specification / Time Stamping Profile, marzo de 2002.

10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

REFERENCIA	NOMBRE DEL DOCUMENTO	CODIGO
[1]	Directivas obligatorias para la formulación de la Declaración de Prácticas de Certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP.	DOC-ICPP-03
[2]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[3]	Guía para la acreditación de los organismos de evaluación de la conformidad.	DOC-ICPP-11
[4]	Requisitos Mínimos para Políticas de Sello Cualificado de Tiempo Electrónico de los PCSC de la ICPP	DOC-ICPP-26