SERVICIOS DE CONFIANZA DE CERTISUR S.A.

NORMAS PARA EL PROCESO DE CERTIFICACIÓN

SERVICIOS DE SELLADO DE TIEMPO

(TIMESTAMP)

Versión 1.0

Vigencia: 01 de Abril de 2017

Av. Santa Fe 788, 2° Piso (C1059ABO) Buenos Aires, República Argentina

Teléfono (+54 11) 4311 2457

www.certisur.com

Notificación de Derechos de Propiedad Intelectual. Marcas Registradas

CertiSur es marca registrada propiedad de CertiSur S.A. El logotipo de CertiSur es marca registrada de propiedad de CertiSur S.A. Las demás marcas registradas y/o marcas de servicio mencionadas en este documento son propiedad de sus respectivos dueños

Sin limitar los derechos mencionados más arriba y con excepción de los permisos citados en el próximo párrafo, ninguna parte de este documento puede ser reproducida, almacenada o introducida en cualquier sistema desde donde la información pueda ser recuperada o transmitida, de cualquier manera (electrónica, mecánica, fotocopiado, grabación, etc.), sin permiso escrito previo de parte de CertiSur S.A.

Sin perjuicio de lo mencionado, se otorga el permiso de reproducir y distribuir estas Normas para el Proceso de Certificación para los Servicios de Sellado de Tiempo de CertiSur S.A. en forma no exclusiva y sin pago de regalías, siempre que: (i) la notificación de los derechos de Propiedad Intelectual y de marcas registradas y los primeros párrafos de esta página aparezcan de manera destacada al principio de cada copia, y (ii) este documento sea reproducido en forma precisa, por completo, sin modificaciones, atribuyendo su autoría a CertiSur S.A.

Las solicitudes para reproducir estas Normas para el Proceso de Certificación como así también la solicitud de copias, deben dirigirse a CertiSur S.A., Av. Santa Fe 788, 2° Piso, (C1059ABO) Ciudad Autónoma de Buenos Aires, Argentina, Teléfono (54 11) 4311 2457, Fax (54 11) 4311 1450, Correo Electrónico: legal@certisur.com.

Contenido

1 INTRODUCCIÓN

Estas Normas describen las prácticas llevadas a cabo por CertiSur S.A. para operar la Autoridad Certificante que brinda los Servicios de Sellado de Tiempo ("TimeStamp") y que forma parte de los Servicios de Confianza de CertiSur.

Estas Normas suministran información detallada respecto de las prácticas empleadas por la Autoridad Certificante de Sellado de Tiempo relacionadas con el ciclo de vida de los certificados (emisión, administración, revocación, renovación y reemisión de claves) como así también los detalles de asuntos legales, administrativos y técnicos específicos de los Servicios de Sellado de Tiempo.

1.1 Identificación

Las prácticas definidas en las presentes Normas se aplican exclusivamente a los Servicios de Sellado de Tiempo y a la Autoridad Certificante de Sellado de Tiempo bajo los Servicios de Confianza de CertiSur S.A. Estas Normas no incluyen otros servicios que CertiSur S.A. puede brindar dentro del territorio de la República Argentina o de otros países de América del Sur, por ejemplo los Servicios de Certificación bajo la Symantec Trust Network, los cuales están regulados por otras Normas.

Por otra parte, en tanto no esté contemplado específicamente en el presente documento, resultarán de aplicación las Normas para el Proceso de Certificación para los Servicios de Confianza de CertiSur vigentes publicadas en: https://www.certisur.com/legal.

La política de certificación para los servicios de Sellado de Tiempo se encuentra definidas bajo la rama del Identificador (OID) 1.3.6.1.4.1.12456.1.3.

1.2 Alcance y Ámbito de Aplicación

Estas Normas resultan de aplicación para todos los intervinientes en los Servicios de Sellado de Tiempo prestados por CertiSur S.A. Están incluidos aquéllos terceros que aceptan como confiables los Sellos de Tiempo generados por los Servicios y que se denominan Partes Confiadas. Todos estos participantes deben conocer y aceptar las presentes Normas como requisito indispensable para el uso de los Servicios, depositar su confianza en los Sellos de Tiempo generados en base a los mismos y adecuar su comportamiento y responsabilidades a lo previsto en el presente.

Este documento determina las reglas generales de la operación del Servicio de Sellado de Tiempo pero su finalidad no contempla la inclusión de especificaciones técnicas detalladas respecto de la infraestructura física y de procesamiento, los procesos operativos y de control y los aspectos organizativos y comerciales bajo los cuales los Servicios son prestados.

Los sellos de tiempo emitidos en cada momento por la Autoridad Certificante de Sellado de Tiempo están sujetos a las Normas vigentes en cada momento, las cuales son publicadas según lo previsto en el punto 1.1 anterior.

2 DISPOSICIONES GENERALES

2.1 Contacto

La organización específica de Administración de este Documento es al Departamento Legal de CertiSur S.A. Las consultas sobre este documento deben dirigirse a:

CertiSur S.A.
Av. Santa Fe 788 – 2º Piso
(C1059ABO) Ciudad Autónoma de Buenos Aires
República Argentina
Atención: Departamento Legal
Correo electrónico: legal@certisur.com

Las presentes Normas están publicadas en el Repositorio Legal de CertiSur en https://www.certisur.com/legal

2.2 Obligaciones

CertiSur S.A. implementa todos los requerimientos especificados en estas Normas y ejecuta todos los procedimientos de conformidad con las mismas.

CertiSur S.A. brinda acceso en forma continua y permanente a los Servicios de Sellado de Tiempo, con excepción de los intervalos de tiempo destinados a tareas de mantenimiento o donde no resulte posible acceder a una fuente de tiempo confiable.

Los períodos de tiempo destinados a mantenimiento programado serán informados a los suscriptores del servicio, con arreglo a las definiciones contenidas en los contratos de servicio específico suscriptos con los mismos.

CertiSur S.A. implementa y opera una infraestructura de procesamiento de la información para su Autoridad Certificante de Sellado de Tiempo confiable y segura, con arreglo a los estándares mundiales en la materia.

CertiSur S.A. utiliza varias fuentes de tiempo externa, independientes y confiables, siendo al menos una de ellas Stratum 1. La desviación máxima de un sello de tiempo es siempre menor a 1 segundo. La sincronización de sus servidores es realizada por medio del protocolo NTP a través de Internet (RFC 1305 *Network Time Protocol).*

CertiSur S.A. suministra a sus suscriptores y partes confiadas la información suficiente acerca de los términos y condiciones para el uso de los Servicios de Sellado de Tiempo, en un todo de acuerdo con lo establecido en las presentes Normas.

CertiSur S.A. brinda los Servicios de Sellado de Tiempo “tal como son” y no asume responsabilidad alguna antes Suscriptores y Partes Confiadas, salvo que esté explícitamente contemplado en el contrato específico de servicios en particular.

En caso de cualquier reclamo o disputa con referencia a los Servicios de Sellado de Tiempo, se aplicará el mecanismo establecido en el acuerdo específico suscripto con el cliente del servicio.

3 ADMINISTRACIÓN DEL CICLO DE VIDA DE CLAVES

3.1 Generación de Claves de la Autoridad Certificante

Cualquier par de claves utilizado en los Servicios de Sellado de Tiempo es generado en un Hardware Security Module (HSM) que cumple con la especificación FIPS 140-1 Nivel 3 o superior, el cual ha sido evaluado y controlado para asegurar su operación de manera apropiada, antes de comenzar con los procedimientos de generación de claves.

La generación de claves se produce en un ambiente asegurado físicamente y por medio de personal acreditado como Persona Confiable, según lo previsto en las Secciones 5.2 y 5.3 de las Normas para el Proceso de Certificación de los Servicios de Confianza de CertiSur.

En ningún momento durante el proceso de generación, la clave privada es operada fuera del Hardware Security Module y bajo ningún concepto ningún material relacionado con claves privadas es almacenado fuera de dicho Hardware de manera no cifrada.

3.2 Protección de la Clave Privada

Todas las claves privadas empleadas en los Servicios de Sellado de Tiempo son preservadas en un Hardware Security Modules (HSM) que cumplen con la especificación FIPS 140-1 Nivel 3 o superior. Estos dispositivos están conectados a equipos de procesamiento de datos que se encuentran en instalaciones físicas seguras, con arreglo a lo especificado en la Sección 5.1 de las Normas para el Proceso de Certificación de los Servicios de Confianza de CertiSur.

Las claves privadas solamente pueden ser activadas mediante la intervención de dos personas, calificadas como Personas Confiables y la utilización de dispositivos criptográficos previene la posibilidad de que las mismas sean exportadas de manera no cifrada.

Las claves privadas solamente son copiadas, resguardadas y/o recuperadas solamente por Personas Confiables, autorizado específicamente para el desarrollo de esas funciones y siempre con la participación mínima de dos personas. Cualquiera de esas operaciones se lleva a cabo en instalaciones físicas seguras, según lo mencionado en el primer párrafo de esta Sección.

La activación para el uso de las claves privadas se realiza por medio de un mecanismo de división de NofM, requiriéndose siempre al menos 2 personas para esta operación.

3.3 Distribución de la Clave Pública

Los certificados que contienen las claves públicas de los Servicios de Sellado de tiempo son publicadas en el sitio Web de CertiSur https://www.certisur.com. Esto permite que las partes confiadas puedan verificar la integridad y autenticidad de los Sellos de tiempo emitidos por CertiSur.

3.4 Períodos de Uso de Claves

Las claves privadas utilizadas en los Servicios de Sellado de tiempo no son empleadas más allá del plazo de finalización de su ciclo de vida y son destruidas, al igual que cualquier material relacionado con las mismas. Los sistemas de sellado de tiempo rechazan de manera automática cualquier intento de generación de sellado si la clave privada a emplear ha sido marcada como expirada.

Los certificados empleados para los Servicios de Sellado de tiempo no son utilizados más allá del plazo que el algoritmo elegido y el tamaño de claves son considerados como confiables y seguros para el propósito para el cual fueron generados.

El periodo máximo para el uso de una Clave Privada para el sello de tiempo es de 10 años.

Los certificados correspondientes a dichas claves tienen un periodo de validez de hasta 5 años. Durante el periodo de uso de una clave privada se pueden llegar a emitir varios certificados que cubran dicho periodo.

4 SELLADO DE TIEMPO

4.1 Algoritmo de Hash para Sellados de Tiempo

Los algoritmos criptográficos y el tamaño de claves utilizados por los Servicios de Sellado de Tiempo de CertiSur responden a las siguientes características:

- Hash Seguro: Sha-256, Sha-384, Sha-512
- Firma: sha2With RSA Encryption

4.2 Token de Sellado de Tiempo

Los Sellos de Tiempo emitidos por CertiSur incluyen la hora correcta, con el margen de error previsto en estas Normas y un identificador único o número de serie. Cada sellado de tiempo incluye un valor de hash del dato de tiempo que ha sido sellado y es firmado digitalmente utilizando una clave generada exclusivamente con ese propósito.

El certificado de la unidad de sellado de tiempo utilizado en los servicios de sellado incluye:

- Un identificador de la unidad que emitió el sellado de tiempo,
- El nombre de la Autoridad Certificante de Sellado de Tiempo, y
- Un identificador de país en el cual la Autoridad Certificante está establecida.

5. ADMINISTRACIÓN Y OPERACIÓN DE LA AUTORIDAD CERTIFICANTE

5.1. Disponibilidad

Los Servicios de Sellado de Tiempo de CertiSur están disponibles las 24 horas del día, durante todo el año, incluyendo feriados y días no laborables. Las interrupciones generadas por los servicios de mantenimiento de la infraestructura, en donde los cuales el servicio no opera, son comunicados a los suscriptores con arreglo a las características del contrato y el acuerdo del nivel de servicio.

Los servicios se podrán interrumpir por razones de fuerza mayor ajenas a CertiSur o en caso de que no se encuentre disponible una fuente de tiempo confiable.

5.2. Infraestructura Física, Administración y Controles Operativos

Resultan de aplicación, sobre este punto, lo dispuesto en la Sección 5 de las Normas para el Proceso de Certificación de los Servicios de Confianza de CertiSur.

5.3. Registro de Información relacionada con los Servicios de Sellado de Tiempo

CertiSur mantiene los registros de la información relevante de los Servicios de Sellado de Tiempo durante un plazo de 5 años, a contar desde el momento de su generación o hasta un plazo de un año, a contar desde el momento de expiración de las claves de firma empleadas, lo que resulte superior.

CertiSur NO mantiene registros de las solicitudes de sellado de tiempo, de los tokens de sellado de tiempo generados salvo que así sea indicado en el servicio prestado específicamente a un cliente en particular. La validez de un sello de tiempo está derivada del hecho que puede ser validado con el certificado correspondiente a la Autoridad de Sello de Tiempo de CertiSur.

Otros registros, tales como eventos relacionados con la administración de la Autoridad Certificante de Sellado de Tiempo, incluyendo administración de claves y certificados y sincronización de los relojes empleados para brindar el servicio, son registrados para mantener evidencia del correcto funcionamiento del sistema.

Los registros son mantenidos de manera confidencial, excepto que el contrato firmado con un suscriptor especifique la posibilidad de su publicación.

5.4. Finalización de los Servicios de Sellado de Tiempo

En caso que CertiSur decidiera la finalización de la prestación de los Servicios de Sellado de Tiempo, realizará todos los esfuerzos que resulten razonables para mantener los registros archivados de sus actividades y los datos que permitan a suscriptores y partes confiadas verificar la autenticidad e integridad de los sellados de tiempo realizados hasta ese momento.

En caso de finalización de sus servicios, CertiSur revocará los certificados de la Autoridad Certificante de Sellado de Tiempo y destruirá sus claves privadas, incluyendo las copias de respaldo, de tal modo que las mismas no pueden ser utilizadas.

5.5. Auditoría

Los Servicios de Sellado de Tiempo de CertiSur son auditados conforme a lo establecido en la Sección 8 de las Normas para el Proceso de Certificación de los Servicios de Confianza de CertiSur.

6. MISCELANEOS

6.1. Costo de los Servicios

CertiSur podrá fijar un precio por la prestación de los Servicios de Sellado de Tiempo. Dicho precio será establecido específicamente en el contrato a acordar con el suscriptor del servicio.

Podrá, asimismo, brindar servicios de valor agregado relacionados con la Autoridad Certificante de Sellado de Tiempo. Las características de dichos servicios serán definidos en los convenios que se establezcan sobre el particular.

6.2. Derechos de Propiedad Intelectual

Los certificados emitidos por la Autoridad Certificante de Sellado de Tiempo, la información generada por los servicios brindados y las presentes Normas son propiedad intelectual de CertiSur S.A.