PRÁCTICAS DE CERTIFICACIÓN SELLADO DE TIEMPO

e-certchile
CAMARA DE COMERCIO DE SANTIAGO

ÍNDICE

1. Introducción.

1.1. Presentación.

Las prácticas de certificación de sellado de tiempo de e-certchile son una descripción detallada de las políticas, procedimientos y mecanismos que nos obligamos a cumplir en la prestación de nuestros servicios de sellado de tiempo, tanto para la emisión como gestión de nuestro rol de autoridad de sellado de tiempo.

En ellas se explican, entre otras cosas:

- Las obligaciones y responsabilidades que tiene la certificadora de firma electrónica de e-certchile, la autoridad de sellado de tiempo, los titulares, las terceras partes que confían en los certificados y la Entidad Acreditadora.
- La forma en que se gestiona el ciclo de vida del sellado de tiempo.
- Los procedimientos para las auditorías, la forma en que protegemos los datos personales que tratamos y la forma en que hacemos frente a la contingencia y recuperación de desastres.
- Las prácticas de seguridad del personal, la seguridad física y ambiental, la gestión de las operaciones.
- La forma en que se administra nuestra Práctica de Certificación, incluyendo la forma en que puede ser modificada.

1.2. Identificación.

El presente documento se individualiza como “Prácticas de Sellado de Tiempo e-certchile” o “CPST e-certchile” y está registrada con el número único (OID) 31725 el que identifica únicamente a e-certchile en un contexto global, según registro en la Internet Assigned Number Authority (IANA).

La “CPST e-certchile” se ha preparado de conformidad con RFC 3628 “Policy Requirements for Time-Stamping Authorities” así como también de las especificaciones técnicas definidas en el documento ETSI TS 102 023 “ElectronicSignatures and infraestructures (ESI) PolicyRequirementsfor Time- StampingAuthorities” y el documento RFC 3161 “Internet X.509 Public Key infraestructura Time- StampingProtocol (TSP)”. De manera complementaria a los documentos indicados, se ha utilizado el documento de nombre “Guías de Evaluación Procedimiento de Acreditación Prestadores de Servicios de Certificación, Servicios de Certificación de Sello de Tiempo”, entregados por el Ministerio de Economía, Fomento y Turismo.

A esta “CPST e-certchile” podrá acceder permanentemente a través de https://www.e-certchile.cl/quienes-somos/politicas-y-practicas-0.

1.3. Comunidad y aplicabilidad.

La "CPST e-certchile" se aplica a todos los sellos de tiempo emitidos por e-certchile.

1.4. Entidades.

1.4.1. Certificador. Son las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorgan certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar. En caso de que deseen acreditarse deberán encontrarse domiciliadas en Chile y seguir el procedimiento de acreditación que señala el Título V de la ley y desarrolla el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.

e-certchile se encuentra acreditado por la Entidad Acreditadora desde el año 2003, mediante la Resolución Exenta Nº 317, de la Subsecretaría de Economía.

1.4.2. Autoridad de Sellado de Tiempo. Es la organización que opera y controla el funcionamiento de la sincronización del tiempo, emisión y otros procesos específicos de sellado de tiempo de un documento o datos, teniendo como principal obligación la provisión de los servicios de sellado de tiempo.

1.4.3. e-certchile se encuentra acreditado por la Entidad Acreditadora desde el año 2016, mediante la Resolución Exenta Nº 3779, de la Subsecretaría de Economía.

1.4.4. Suscriptor. Son entidades que pueden ser individuos, empresas, sistemas y otro tipo, que solicitan la emisión del sello de tiempo.

1.4.5. Tercera Parte que Confía. Son entidades que pueden ser individuos, empresas, sistemas u otro tipo, que son receptores de un sello de tiempo generado por la autoridad de sellado de tiempo.

Una tercera parte que confía no es necesariamente un suscriptor, puede ser cualquier individuo, empresas, sistemas y otro tipo que libre y voluntariamente decide confiar en un sello de tiempo.

Para realizar la verificación de los sellos de tiempo emitidos por la autoridad de sellado de tiempo la parte que confía debe contar con mecanismos que le permitan validar si se trata de un sello de tiempo auténtico.

1.4.6. Entidad Acreditadora: La Subsecretaría de Economía y Empresas de Menor Tamaño en virtud de lo dispuesto en la Ley 19.799.

1.5. Detalles de contacto.

a. Dirección postal: Monjitas 392 Piso 17, comuna y ciudad de Santiago de Chile.
b. Correo electrónico: sclientes@e-certchile.cl
c. Teléfono: (+56 2) 2360 7175
d. Mesa ayuda certificación: (+56 2) 2818 5760
e. Sucursales
   - Enrique Mac-Iver 410, comuna y ciudad de Santiago de Chile:

     Lunes a Jueves: 09:00 – 17:30 hrs.

     Viernes 09:00 – 14:30 hrs.
   - Av. Nueva Providencia 2260, Local 81, comuna de Providencia y ciudad de Santiago de Chile

     Lunes a Jueves: 09:00 – 17:30 hrs.

     Viernes 09:00 – 14:30 hrs.

1.6. Aplicabilidad de los sellos de tiempo.

Los sellos de tiempo emitidos por la autoridad se de sellado de tiempo se utilizarán únicamente conforme a la función y finalidad que están establecidas en esta Práctica de Sellado de Tiempo e-certchile (CPST e-certhile), en concordancia con la normativa vigente para garantizar el no repudio.

a. El uso de los sellos de tiempo está limitado a demostrar que un documento o una serie de datos han existido y no han sido modificados desde un instante de tiempo específico y confiable.

b. Usos prohibidos. Los sellos de tiempo emitidos por autoridad se de sellado de tiempo se utilizarán únicamente conforme a la función y finalidad que se tenga

establecida en la presente Práctica de Sellado e-certchile (CPST e-certchile) de tiempo y de acuerdo con la normativa vigente. Cualquier uso diferente a los indicados está expresamente prohibido.

1.7. Estructuras de los sellos de tiempo.

La estructura de los sellos de tiempo generados por autoridad se de sellado de tiempo se ajustan al documento RFC 3161 “Internet X.509 Public Key Insfraestcruture Time Stamping Protocol (TSP)”.

La certificadora referencia el OID de la Práctica de Sellado de Tiempo e-certchile (CPST e-certchile) en cada uno de los sellos de tiempo.

2. Obligaciones y responsabilidades.

2.1. Obligaciones.

2.1.1. e-certchile.

a. e-certchile en su calidad de autoridad de sellado de tiempo se obliga a:

b. Ofrecer y mantener instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los sellos de tiempo en los términos establecidos en la Ley 19.799 y el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.

c. Cumplir y respetar los procedimientos establecidos en esta “CPST e-certchile”.

d. Cumplir con todas las otras obligaciones establecidas en la Ley 19.799, el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y las normas técnicas dictadas conforme a éste.

e. Garantizar el acceso permanente a los servicios de sellado de tiempo, donde la precisión del tiempo UTC puede tener una desviación máxima de 1 segundo.

f. Mantener su llave privada bajo adecuadas medidas de seguridad, para evitar cualquier mal uso de esta, controlando el ciclo de vida de ella, así como, también del hardware criptográfico.

g. Mantener un identificador único para cada sello de tiempo emitido, así como incluir una referencia a la política bajo la cual fue emitido.

h. Mantener sincronizado el reloj de la unidad de sellado de tiempo con la precisión de la fecha y la hora declarada con respecto al tiempo UTC.

i. Mantener los controles de seguridad física, de procedimiento y personales definidos para el sellado de tiempo.

j. Proporcionar antecedentes e información fidedigna al momento de emitir sellos de tiempo de acuerdo con la información conocida en el momento de su emisión.

k. Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de sellado de tiempo a los que sirven de soporte.

l. Garantizar mediante revisiones y auditorias que todos los requerimientos de la autoridad de sellado de tiempo cumplen con los controles requeridos por la legislación aplicable, la Práctica de Sellado de Tiempo (CPST e-certchile) y los procedimientos internos.

m. Informar:

- El algoritmo de hash utilizado en lo sellos de tiempo.
- La precisión del tiempo utilizado como parte del proceso de certificación de los sellos de tiempo.
- Los mecanismos de verificación de los tokens emitidos por e-certchile.

- El período de permanencia de los logs que maneja la autoridad de sellado de tiempo.

n. Mantener www.e-certchile.cl con información para el público sobre los servicios de e-certchile.

2.1.2. Obligaciones del suscriptor.

a. Las partes que confían deben verificar la firma del sello de tiempo, comprobando el estado del certificado de la autoridad de sellado de tiempo y su periodo de validez.

b. Verificar que la llave de la autoridad de sellado de tiempo no ha sido comprometida hasta el momento de la verificación, utilizando para ello la CRL publicada por e- certchile.

c. En el caso de la verificación de un sello de tiempo, después de la expiración del certificado de la autoridad de sellado de tiempo verificar que el número de serie del certificado no se encuentra en la CRL y que era válido al momento en que se generó el sello de tiempo.

d. Conocer el propósito y alcance de los sellos de tiempo emitidos por e-certchile.

e. Notificar o dar aviso sobre cualquier situación considerada anómala con respecto al servicio de sellado o a los sellos de tiempo emitidos, lo cual debe ser considerado como causa de revocación de éste.

f. Conocer y aceptar los términos, condiciones y límites contenidos en estas “CPST e-certchile”.

2.2. Responsabilidades.

2.2.1. e-certchile.

a. Emitir los certificados de sellado de tiempo cumpliendo todas las exigencias establecidas en estas “CPST e-certchile”.

b. Que la información incluida o incorporada por referencia en el sello de tiempo sea exacta.

c. La aplicación correcta del procedimiento empleado.

e-certchile no será responsable por ningún daño o perjuicio actual o futuro, directo o indirecto, previsto o imprevisto, emergente o lucro cesante, pérdida de datos u otros, debidos, ocasionados o conectados con el uso indebido, no uso, uso tardío de certificados, aun cuando e-certchile hubiera sido advertido de la posibilidad de producción de tales daños.

2.2.2. Limitación de responsabilidad de e-certchile.

Las responsabilidades que afectan la operación de la autoridad de sellado de tiempo se encuentran limitadas a lo establecido en el artículo 14 de la Ley 19.799.

En todo caso, la responsabilidad de autoridad de sellado de tiempo cualquiera sea la naturaleza de la acción o reclamo y salvo que medie dolo o culpa grave atribuible a e-certchile, quedará limitada como máximo al monto correspondiente a UF 5.000 (cinco mil unidades de fomento), monto asegurado de conformidad con lo dispuesto en el artículo 14 de la Ley 19.799 y el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo.

La actividad de la autoridad de sellado de tiempo se encuentra limitada al ciclo de vida del certificado de sellado de tiempo.

2.2.3. Fuerza mayor.

e-certchile no será responsable por daños, pérdidas o perjuicios que provengan de incumplimientos en el desarrollo de la actividad de certificación de firma electrónica y que sean atribuibles a circunstancias constitutivas de caso fortuito o fuerza mayor.

Las obligaciones de e-certchile afectadas por el caso fortuito o la fuerza mayor se suspenderán por el período de tiempo que dure el hecho que lo motivó.

Para los efectos de esta "CPST e-certchile" se entenderá por caso fortuito o fuerza mayor lo dispuesto en el artículo 45 del Código Civil, lo que incluye guerras, desastres naturales, paros, huelgas o suspensión de laborales del personal de e-certchile o de sus contratistas o subcontratistas, sin que esta enumeración sea taxativa.

2.3. Ley aplicable y resolución de controversias.

2.3.1. Ley aplicable.

Esta "CPST e-certchile" se rige por la ley Chilena y se someterán al Tribunal Arbitral que más adelante se expresa.

2.3.2. Procedimiento de resolución de conflictos.

Cualquier diferencia, dificultad, problema o controversia que pueda surgir con motivo de la validez, eficacia, interpretación, nulidad, cumplimiento o incumplimiento de esta "CPST e-certchile y en general la actividad de certificación que realiza e-certchile será resuelto definitivamente por un árbitro mixto, quien tramitará como árbitro arbitrador pero que fallará conforme a derecho. El fallo del árbitro será en única y definitiva instancia, sin que, en contra de sus resoluciones y fallo, ya sean de substanciación o de medidas precautorias o bien el fallo definitivo, proceda ningún recurso. El arbitraje se llevará a cabo en la ciudad de Santiago. El árbitro estará solamente obligado a constituir legalmente el arbitraje, a oír a las Partes en conjunto o separadamente, según él lo decida, a recibir las pruebas que se presenten y a dictar su sentencia oportunamente. Las resoluciones se notificarán por carta certificada dirigidas a las Partes o a sus representantes designados en esta escritura o en el respectivo proceso, a las direcciones que ellos señalen en tales instrumentos, salvo la primera notificación del proceso y la de la sentencia definitiva que deberán notificarse en conformidad a las reglas establecidas para dichas resoluciones en el Título Sexto, del Libro Primero, del Código de Procedimiento Civil. El árbitro designado podrá actuar cuantas veces fuere requerido, por asuntos diferentes, promovidos por cualquiera de las Partes, y en caso de ausencia o impedimento acreditada a juicio del sustituto, éste podrá intervenir de

inmediato, en carácter de subrogante, en el estado en que el asunto se encuentre, sin otro requisito que aceptar el cargo. El respectivo proceso podrá continuarse incluso en una copia autorizada de los autos que cualesquiera de las Partes presentaren ante el sustituto. La evidencia de haberse ausentado del país el árbitro en ejercicio por más de treinta días sin haber regresado, o de impedimento de otra naturaleza acreditado ante el sustituto por medios idóneos y que dure más de treinta días será considerado como ausencia del árbitro.

El árbitro deberá tener el carácter de mixto y su designación será efectuada, a solicitud escrita de cualquiera de las Partes, por la Cámara de Comercio de Santiago A.G. de entre los integrantes de la lista arbitral de su Centro de Arbitraje y Mediación, para lo cual las Partes le otorgan, mediante este instrumento, un mandato especial e irrevocable.

2.3.3. Separación y divisibilidad de cláusulas.

En el evento que alguna disposición contenida en las “CPST e-certchile” sea declarada nula, inoponible o cualquier otra causa de ineficacia jurídica, se deja constancia que dicha declaración sólo afecta la norma en particular, dejando vigente en su integridad el resto del documento.

2.3.4. Conflicto de normas.

En caso de producirse un conflicto de normas, se seguirá el siguiente orden de precedencia:

a. Ley 19.799.

b. Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo que reglamenta la Ley 19.799.

d) “CPST e-certhile” vigente.

f) Otros documentos relacionados con la prestación de servicios de certificación de sellado de tiempo.

2.4. Tarifas.

El solicitante se obliga a pagar a e-certchile las tarifas establecidas para el servicio de sellado de tiempo.

Las tarifas se encuentran permanentemente publicadas y disponibles en www.e-certchile.cl/tarifas.

El pago señalado tiene como causa y fundamento exclusivamente la emisión del certificado de sellado de tiempo.

La no aceptación posterior de un certificado por una causal distinta a errores o inexactitudes en éste o su no uso no autoriza al suscriptor para pedir reembolso alguno.

2.5. Publicaciones y repositorio.

e-certchile mantiene permanentemente a disposición de cualquier interesado esta "CPST e-certchile" en https://www.e-certchile.cl/quienes-somos/politicas-y-practicas-0.

Cualquier modificación a esta "CPST e-certchile" generará una nueva versión, debiendo publicarse dicho cambio y custodiarse la versión anterior.

Cualquier situación ocasionada con relación a la vigencia de un certificado y de las obligaciones contraídas por e-certchile se resolverán de acuerdo con la "CPST e-certchile" vigente al momento de la emisión del sellado de tiempo en cuestión.

2.6. Auditorías.

e-certchile, en su calidad de certificador de sellado de tiempo acreditado, es inspeccionado anualmente por la Entidad Acreditadora para mantener vigente la acreditación obtenida en el año 2016.e-certchile realiza auditorias a su instalaciones y sistemas como parte de sus certificaciones ISO/IEC 19.001 y ISO/IEC 27.001, comprometiéndose a corregir dentro de un plazo razonable, las eventuales deficiencias que se puedan encontrar.

2.7. Protección de datos personales.

El tratamiento de sus datos personales es importante para nosotros y para protegerla de mejor manera hemos diseñado una política de tratamiento de datos.

Esta política explica la forma en que tratmos sus datos personales y las opciones que Ud. tiene respecto a lo que hacemos. En todo caso, tenga presente que todos los tratamientos los hacemos en el marco de la habilitación legal que nos otorga la Ley 19.799 y en los términos establecidos en la Ley 19.628. Nuestra política vigente siempre la encontrará disponible en https://www.e-certchile.cl/quienes-somos/politicas-y-practicas-0.

2.8. Derechos de propiedad intelectual e industrial.

Pertenecerá a e-certchile, en forma total y exclusiva, la propiedad intelectual e industrial de las obras creadas, desarrolladas o modificadas para la prestación de los servicios de certificación. Ningún derecho de propiedad intelectual o industrial preexistente o que se adquiera o licencie a/o por e-certchile se entenderá conferido a cualquiera de las personas individualizadas en el punto 1.4 Entidades.

Los titulares y usuarios no podrán hacer uso del nombre, marca o logo de e-certchile para efectos de publicidad o cualquiera otro, sin perjuicio de poder pactar especialmente, de acuerdo al tipo y alcances de difusión, condiciones diversas con e-certchile, mediante un acuerdo escrito.

3. Gestión del ciclo de vida del certificado.

3.1. Generación de llave de la unidad de sellado de tiempo.

El módulo criptográfico de e-certchile es capaz de generar llaves en base al algoritmo de encriptación de llave publica SHA2RSA con al menos 2048 bits de encriptación tal como se solicita en el criterio común de operación criptográfica CC P2 FCS_COP.1.

Para acceder a funcionalidades del equipo HSM Cryptosec TSA sobre el que se ejecutan las operaciones se utilizan estos medios físicos de protección lógica (ACS y OCS). Ellos controlan el acceso al material criptográfico y además poseen características de protección contra intentos de intrusión física en concordancia con el estándar FIPS140-2 nivel 3, logrando él mismo deshabilitar su contenido en caso de detectar riesgos evidentes.

La encriptación aplicada a la llave privada de la certificadora, bajo las ACS y OCS, permiten minimizar un posible compromiso de esta llave en ausencia de los controles de acceso definidos en el sistema criptográfico, el cual establece un quórum de tarjetas físicas de operación para poder funcionar. Con respecto a este quórum se establece una cantidad de token físicos para poder realizar tareas sobre el material criptográfico en el equipo HSM Cryptosec TSA, y de igual manera existe un quórum para administración del ambiente completo, que es una protección adicional en caso que el o los equipos sean comprometidos por un tercero. El quórum establecido para la administración es 2 de 4 token.

La llave usada por la unidad de sellado de tiempo es generada de acuerdo a la Práctica de Sellado de Tiempo e-certchile (CPST e-certchile) definidas para el proceso de sellado de tiempo, utilizando tanto los algoritmos de encriptación como el largo de llave en estos documentos definidos.

Del mismo modo, la autoridad de sellado de tiempo utiliza para la generación de la llave antes mencionada, un módulo criptográfico HSM que cumple con el estándar FIPS 140-2 nivel 3, el cual sólo puede ser acezado por personal autorizado, altamente confiable y que son parte del quórum de administración definido durante la Ceremonia de Llaves del equipo HSM.

e-certchile declara que satisface los requerimientos identificados en CEN Workshop Agreement 14167-2 [CWA 14167-2] o ISO 15408 al cumplir con la ETSI TS 102 042 que fue la que dio origen al ciclo de vida de la llave aquí descrito.

3.2. Protección de la llave privada de la unidad de sellado de tiempo.

La autoridad de sellado de tiempo lleva a cabo un conjunto de acciones de manera tal de asegurar que la llave privada de la unidad de sellado de tiempo usada para firmar los sellos de tiempo permanezca de manera confidencial y mantenga su integridad. Esto incluye el uso de un HSM; certificado FIPS 140-2 nivel 3. Cuando la llave privada es respaldada, ella es

copiada, almacenada y recuperada sólo por el personal con roles de confianza y bajo un ambiente seguro

La autoridad de sellado de tiempo realiza la protección de las llaves a través de:

- Módulos criptográficos: El HSM "Hardware Security Module" (Módulo de Seguridad Hardware), es un dispositivo hardware de seguridad criptográfica que genera y protege claves privadas. Los HSM de e-certchile cumplen el estándar FIPS 140-2 Nivel 3.
- Control de la llave privada: Las claves privadas utilizadas por la autoridad de sellado de tiempo y sus jerarquías se encuentran bajo control multipersona, es decir, es necesario un mínimo de 2 personas de un total de 6 para modificar el ambiente criptográfico.
- Depósito de la llave privada: La clave privada está cifrada y queda contenida en el repositorio asociado a dispositivo HSM.
- Copia de respaldo de la llave privada: Existe un procedimiento de recuperación de claves de los módulos criptográficos HSM de la AC (raíz o intermedias) que se puede aplicar en caso de contingencia para la certifiacdora. El procedimiento de recuperación de claves de módulos criptográficos corresponde al contexto de procesos certificados que posee el dispositivo HSM.
- Introducción de la clave privada en el módulo criptográfico: Las claves privadas se crean en el módulo criptográfico HSM en el momento de la creación de cada una de las entidades de e-certchile que hacen uso de dichos módulos.
- Método de activación de la clave privada: Las claves privadas de la autoridad de sellado de tiempo y que componen su jerarquías, se activan mediante la inicialización del software de la certificadora y la activación del hardware criptográfico que contiene las claves.

- Método de desactivación de la clave privada: Un Administrador puede proceder a la desactivación de la clave privada de las certificadora o de sus claves intermedias (Clave de la autoridad de sellado de tiempo), mediante la detención del software de la certificadora.
- Método de destrucción de la clave privada: Existe un procedimiento de destrucción de claves de la autoridad de sellado de tiempo, así como de las claves intermedias de la jerarquía.

En lo que respecta a la generación de la llave de la unidad de sellado de tiempo, el módulo criptográfico utilizado mantiene la confidencialidad de la llave en su ciclo de tiempo completo, restringiendo el acceso a éste al personal autorizado solamente. De detectarse un acceso no autorizado, este se registra ya sea de manera física (tampering físico) o a través de log a ser usado durante la auditoria. Este equipo contempla además mecanismos de backup y respaldo de la llave, manteniendo la seguridad de estos respaldos a través de métodos criptográficos. e- certchile declara cumplir con el documento "CEN Workshop Agreement 14167- 2 [CWA 14167- 2]" o ISO 15408 en lo correspondiente al ciclo de vida de su llave criptográfica, realizando la implantación de estos controles de acuerdo a la norma ETSI TS 102 042.

3.3. Distribución de la llave pública.

El certificado digital utilizado por la autoridad de sellado de tiempo es generado por la certificadora de acuerdo a las Prácticas de Certificación de Sellado de Tiempo e-certchile (CPST e-certchile) auditadas por la Entidad Acreditadora.

La forma en que se establece la confianza con una certificadora- descrita para que un tercero que desee confiar - se basa en la instalación del certificado raíz de la unidad de sellado de tiempo respecto a la cual se desea confiar. Es así que e-certchile, como parte de los servicios que provee a sus clientes y terceros, publica en su sitio web los certificados raíces.

Estos certificados, se encuentran disponibles en el sitio web de e-certchile, a través de una conexión segura (https).

Al estar este certificado instalado en el repositorio de confianza del cliente, cualquier sello que haya sido firmado por la certificadora podrá ser validado por el cliente, ya que el certificado raíz de la certificadora contiene la llave pública que permitirá verificar el sello emitido.

A continuación se presenta la secuencia general del modelo de confianza:

- Se descarga certificado raíz de la autoridad de sellado de tiempo que ha emitido el sello a validar. Este certificado debe ser descargado a través de un canal seguro, que debe poseer el sitio de descarga de dicha raíz. Descargado el certificado raíz, este se procede a instalar en el emisoras raíz de confianza del equipo cliente.
- El sistema indicará si la importación e instalación del certificado ha sido correcta. De ser así, cualquier mensaje que sea firmado con un certificado de sello de tiempo, que ha sido emitido y firmado con esta raíz, podrá ser validado automáticamente en el equipo cliente. Una forma de validación adicional a esta instalación, es verificar si el almacén de raíces de confianza incluye a este certificado recién instalado.

Al estar el certificado de la autoridad de sellado de tiempo instalado en el repositorio de confianza del cliente, cualquier sello que haya sido emitido y firmado por esta autoridad de sellado de tiempo podrá ser validado por el cliente, ya que el certificado raíz de la autoridad de sellado de tiempo contiene la llave pública que permitirá verificar el certificado emitido. Una forma de complementar esta cadena de confianza, es instalar además del certificado raíz de la unidad de sello de tiempo (raíz intermedia de la certificadora), el certificado raíz de la certificadora utilizado para firmar el certificado de la unidad de sello de tiempo.

3.4. Remisión de llaves de la unidad de sello de tiempo.

Por motivo de seguridad y evitar el repudio a un certificado, e-certchile como certificador de firma electrónica no procede a realizar la reemisión de llaves una vez generado el certificado de la unidad de sellado de tiempo, esto de acuerdo a Prácticas de Certificación e-certchile (CPS e-certchile) que rigen su operación. Sin embargo, la llave privada de la unidad de sellado de tiempo será reemplazada antes del fin de su periodo de validez, en caso de que el algoritmo o largo de la llave se determine como potencialmente vulnerable.

3.5. Termino del ciclo de vida de la llave de la unidad de sellado de tiempo.

La llave privada de la unidad de sellado de tiempo será reemplazada al momento de su expiración. La unidad de sello de tiempo rechazará cualquier intento de emitir un sello de tiempo cuando esta llave privada haya expirado. Después de expirada, la llave privada es destruida.

e-certchile tiene la capacidad de revocar el certificado raíz activo de la unidad de sello de tiempo, en el momento que estime conveniente, ya sea por un evento de seguridad o bien por cese de actividades.

En el evento que e-certchile vaya a descontinuar sus operaciones como autoridad de sellado de tiempo procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus servicios de sellado de tiempo: titulares, terceros que confían y autoridades de sello de tiempo acreditadas.

e-certchile comunicará a cada uno de sus titulares del cese de sus funciones. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

e-certchile procederá a transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. Esta información incluirá como mínimo la información de los titulares, los certificados de la unidad de sellado de

tiempo revocados, así como la transferencia de las obligaciones para mantener logs, archivos de auditoría, así como acceso a las llaves públicas o certificado usado por los terceros que confían por un periodo de tiempo razonable. La llave privada de la unidad de sello de tiempo, así como sus respaldos son destruidos inmediatamente al momento del cese de la actividad de la autoridad de sellado de tiempo.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, se realizará en conformidad con la ley chilena.

3.6. Renovación de certificados de sellado de tiempo.

No aplica.

3.7. Gestión del ciclo de vida de los módulos criptográficos usados para las firmas de sello de tiempo.

Los equipos HSM con que cuenta e-certchile y que son usados para firmar el certificado utilizado por la unidad de sellado de tiempo para la firma de sus sellos de tiempo; así como para la firma de los mismos sellos de tiempo, cuenta con la detección de intrusión a los equipos, ya sea por sellos holográficos y/o detectores de intrusión. Así mismo, para evitar la intrusión de dispositivos en el hardware del módulo de seguridad, este dispositivo se coloca en la parte posterior a los ventiladores del HSM. El equipo HSM posee varios niveles de detección de intrusión física a la funcionalidad criptográfica, informando estos eventos al administrador y en último caso obligando a reiniciar el equipo a sus condiciones de salida de fábrica. Los eventos antes mencionados son desplegados en la pantalla del equipo.

Ante la detección de los eventos que se indican previamente, no se debe poner en producción dicho equipo, ya sea que los eventos se han producido durante el almacenamiento o transporte del equipo. El administrador de dicho equipo debe proceder a reiniciar el equipo a sus condiciones de salida de fábrica. Posterior a

esto, se debe reconectar el equipo así como recuperar la información clave del equipo, haciendo uso del quórum que otorgan el set de tarjetas de administración definidas.

En particular si se ha detectado apertura de la tapa del equipo, este genera un evento indicando dicha intrusión, lo que implica que la seguridad del equipo se ha comprometido. Bajo este escenario no se debe pasar a producción dicho equipamiento bajo motivo alguno.

Si el evento indicado, se produce durante el transito del equipo desde el fabricante de dicho equipo, el administrador debe contactarse inmediatamente con el fabricante. En cambio de ocurrir este evento posterior a la instalación, adicionalmente se deben revisar las políticas y procedimientos de seguridad que permitieron dicho incidente.

Entre las revisiones que deben realizarse al equipo, tanto posterior a su transporte o durante su almacenamiento es:

- Controlar que los sellos de seguridad no han sido alterados.
- Que las tapas permanecen completamente ajustadas al chasis del equipo.
- Que no se presentan daños aparentes a la estructura general del equipo.
- Que no se detecten daños evidentes en ventilaciones del equipo o que se haya intentado
- introducir algún componente a través de estos espacios.

El equipo HSM utilizado por e-certchile tanto para su certificadora como para su autoridad de sellado de tiempo implementa seguridad de acceso a información criptográfica a través de diferentes niveles.

Para acceder a funcionalidades del equipo HSM, sobre el que se ejecutan las operaciones de instalación, respaldo y recuperación, además poseen características de protección contra intentos de intrusión física en concordancia con el estándar FIPS140-2 nivel 3, logrando él mismo deshabilitar su contenido en caso de detectar riesgos evidentes.

La encriptación aplicada a la llave privada de la certificadora para la generación del certificado de la unidad de sello de tiempo, permiten minimizar un posible compromiso de esta llave en ausencia de los controles de acceso definidos en el sistema criptográfico, el cual establece un quórum de tarjetas físicas de operación para poder funcionar. Con respecto a este quórum se establece una cantidad de tarjetas físicas para poder realizar tareas en el equipo HSM sobre el material criptográfico, y de igual manera existe un quórum para administración del ambiente completo, que es una protección adicional en caso que el o los equipos sean comprometidos por un tercero. El quórum establecido para la administración es 2 de 4 token.

Una vez instalado de manera exitosa el hardware y software asociado al HSM, e-certchile ha definido como criterio de verificación del correcto funcionamiento de los equipos, la emisión de un certificado de prueba, partiendo desde su solicitud hasta su emisión y a continuación la revocación del mismo. Con este ciclo se probará la correcta generación de claves, servicios OCSP y listas de revocación de certificados. Una vez desarrollada esta actividad, se podrá proceder a generar las llaves intermedias utilizadas por los distintos servicios de la PSC, en particular para este caso, la llave de la unidad de sello de tiempo utilizada para la firma de los sellos de tiempo a emitir.

Finalmente, en caso de requerir mover el equipo a otra instalación o el envío del mismo a la fábrica por motivos de garantía, e-certchile ha definido que se debe dejar el equipo a sus condiciones originales que tenía a la salida de fábrica,

borrando con ello todo su contenido de configuraciones interna del equipo HSM. En particular, para el caso de equipos, esto se puede realizar a través del menú de opciones de administración, opción “factory state”. Esto llevará a que el equipo borre todo su contenido. Lo anterior no afectará el “Security Word” data almacenada en el RFS, por tanto en caso de no existir intrusión, el contenido de dicho equipo puede ser restaurado a partir de esta data más las llaves ACS y el quórum definido.

4. Sello de tiempo.

4.1. Token de Sello de Tiempo.

e-certchile garantiza que los token de sellado de tiempo son emitidos en forma segura e incluyen un identificador único de política (OID), valores de fecha y hora proveniente de una fuente confiable de tiempo UTC sincronizado en la precisión definida en esta política.

Para cada sello de tiempo se incluye:

- La representación (Hash) del dato que provee el suscriptor para que sea sellado con el sello de tiempo.
- Un identificador para la política de marca de tiempo
- Un número serial único que será usado para ordenar los TST’s así como para identificar un sello de tiempo específico.
- El Token de Sello de Tiempo calibrado a 1 segundo de la UTC, indicando la fuente de tiempo confiable.
- La firma electrónica que ha sido generada usando una llave que es sólo usada para la firma de los sellos de tiempo.
- La identificación de la autoridad de sellado de tiempo y de la unidad de sellado de tiempo.

- La autoridad de sellado de tiempo establece todo el procedimiento asociado a la generación de los tokens de sello de tiempo, utilizando el protocolo descrito en RFC3161.

4.2. Sincronización de los relojes con UTC

e-certchile declara utilizar una fuente fiable de tiempo, mediante un servidor basado en el protocolo NTP que sincronice con el tiempo UTC a través de una red de satélites GPS o en caso excepcional contra múltiples fuentes que incluyen el "National Measurenment Institute", el cual provee tiempo UTC(k); lo anterior con una desviación máxima de 1 segundo. Esta fuente de tiempo está basada en el protocolo NTP (Network Time Protocol) haciendo que la exactitud no disminuya por debajo de los requerimientos.

De manera más específica:

- La calibración de la unidad de sellado de tiempo es desarrollada de tal manera de que el reloj no escape más allá de la precisión declarada.
- El reloj de la unidad de sellado de tiempo se encuentra protegido contra amenazas ambientales que puedan afectar su precisión fuera del rango declarado.
- En caso de producirse una desviación más allá de la precisión declarada, esto será informado a la comunidad a través del sitio web de la certificadora.
- En caso de detectarse una desviación más allá de la precisión declarada, la unidad de sellado de tiempo no generará nuevos sellados de tiempo hasta que el tiempo correcto es restaurado.
- e-certchile declara que la precisión declarada es mantenida con una desviación de 1 segundo tal como se incluye en el sellados de tiempo.

5. Gestión de la certificadora y operaciones.

5.1. Gestión de la Seguridad.

e-certchile desarrollará una administración activa de la seguridad a través de un Sistema de Gestión de Seguridad de la Información (SGSI), el que considera las siguientes prácticas y estándares de la industria.

- e-certchile declara que su certificadora es responsable por todos los aspectos asociados a la provisión de servicios de sello de tiempo y no subcontrata los servicios de sello de tiempo.
- Todo su personal tienen acceso a sus prácticas y políticas de sello de tiempo.
- Todo el personal es auditado mensualmente a fin de verificar el cumplimiento de la planificación del SGSI.
- e-certchile cuenta con un Comité de Seguridad de la Información, un oficial de seguridad, un oficial adjunto y una oficina técnica, los que en su conjunto velan por el cumplimiento del plan anual definido por el SGSI.
- e-certchile declara que los procedimientos y controles operacionales de la certificadora se encuentran documentados, se mantienen y se implementan.
- e-certchile no subcontrata los servicios de sello de tiempo.

5.2. Gestión y clasificación de activos.

Los activos de e-certchile reciben un apropiado nivel de protección. Para ello la certificadora realiza anualmente un análisis de riesgos. En este análisis se ha levantado el inventario de los activos existentes en el proceso de sello de tiempo, junto con su clasificación de riesgo.

Producto de lo anterior la certificadora generó plan de gestión de seguridad que incluye las mitigaciones a los riesgos detectados previamente.

Para el cumplimiento de este plan, así como su seguimiento, e-certchile cuenta con un Comité de Seguridad de la Información y un oficial de seguridad, los que en su conjunto velan por su cumplimiento; desarrollando las acciones para controlar y mitigar cualquier desviación a dicho plan, o incorporar medidas adicionales con consideradas durante su generación. Tal como se indica anteriormente, todos estos procedimientos y controles operacionales de la autoridad de sellado de tiempo se encuentran documentados, se mantienen y se implementan.

Estos procedimientos son inspeccionados mensualmente a través de auditorías internas y anualmente por la Entidad Acreditadora.

6. Seguridad del personal.

6.1. Requerimiento de antecedentes y experiencia.

e-certchile requiere que todo el personal asociado a la certificadora cuente con una calificación y experiencia acorde a la prestación de servicios de certificación, lo cual incluye:

- Conocimientos y formación sobre entornos de certificación digital y sellos de tiempo.
- Formación básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.
- Título académico o experiencia en la industria equivalente.
- El personal que realiza un rol de confianza no debe tener conflictos de interés que afecten la imparcialidad de las operaciones de la certificadora.

6.2. Comprobación de antecedentes.

e-certchile realiza una comprobación de los antecedentes del personal para asegurar que cumpla con las formación y experiencia necesaria para asumir un rol de confianza en la certificadora.

6.3. Roles de confianza.e-certchile declara que sus roles de confianza al cumplir su función de TSA corresponden a:

- Oficial de seguridad: Responsable de la administración e implementación de las prácticas de seguridad.
- Administrador de Sistemas: Responsable de instalar, configurar y mantener los sistemas de confianza de la certificadora, para la administración de sello de tiempo. Además, es responsable por la operación de los sistemas y autorizado para realizar el respaldo y recuperación.
- Administrador de Seguridad: Responsable de verificar la mantención de los sistemas de confianza de la certificadora.
- Auditor: Responsable de revisar archivos y log de auditoría de la certificadora.

6.4. Requerimientos de formación y reentrenamiento.

Como parte de las recomendaciones en que e-certchile ha trabajado, se considera para el personal asociado a la certificadora, cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de e-certchile para la certificadora de firma electrónica. Este plan incluirá labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

6.5. Sanciones.

El Reglamento Interno de Orden, Higiene y Seguridad considera las sanciones a las que se pueden ver expuestos las personas que laboran en la certificadora.

6.6. Requerimientos de contratación.

Como parte de los requerimientos de contratación, todo trabajador de la certificadora debe firmar un acuerdo de confidencialidad.

6.7. Documentación entregada al personal.

El personal de la certificadora tendrá a su disposición el siguiente material:

- Declaración de Prácticas de Certificación e-certhile (CPS e-certchile).
- Declaración de Prácticas de Certificación Biometría e-certhile (CPSB e-certchile).
- Declaración de Prácticas de Certificación Sellado de Tiempo e-certhile (CPST e-certchile).
- Políticas de Certificación.
- Políticas de Tratamiento de Datos Personales.
- Políticas de Seguridad de la Información.
- Organigrama y funciones del personal

6.8. Control de cumplimiento.

De acuerdo al Plan de Seguridad se mide el control de cumplimiento de las actividades programadas de manera anual.

6.9. Finalización de contratos.

La finalización de contratos cuenta con un procedimiento en el cual se suprimen los privilegios de acceso del individuo a las instalaciones e información de la organización, a excepción de la considerada publica, una vez informado el individuo

de su marcha y de su pérdida de privilegios, se verifica la devolución del material entregado y se le informa al resto de la organización, a los proveedores y entidades externas a e-certchile de que el individuo ya no representa a e- certchile.

7. Seguridad física y ambiental.

La seguridad física y ambiental se detalla en el documento SF01 Seguridad Física.

8. Gestión de las operaciones.

e-certchile establece que su sistema y componentes son fiables, ya que se encuentran operados de manera correcta con un riesgo mínimo de falla en la emisión, el control de sellos de tiempo, el manejo correcto de los medios, el control y planificación de los sistemas, control y reporte de incidentes.

Los componentes del sistema de la certificadora son protegidos de virus, código malicioso e incorporación de código no autorizado. Respecto al manejo de medios y seguridad, e-certchile declara un apropiado tratamiento de sus activos a través de la realización de un análisis anual de riesgo riesgos, el cual genera como parte de su preparación la lista de activos de la certificadora, su nivel de protección así como los procedimientos adicionales a seguir para minimizar su riesgo.

Para el manejo de incidentes y su respuesta, e-certchile cuenta con un sistema de gestión de incidentes que asegura que los eventos y debilidades de la seguridad de la información, asociados con los sistemas de información de los procesos de la certificadora de firma electrónica y su certificadora de sello de tiempo, son comunicados a los roles encargados de la gestión de los incidentes para que realicen correcciones oportunas.

Además considera los siguientes roles de confianza que manejan las operaciones:

- Administrador de Sistemas.
- Oficial de Seguridad.

- Jefe de Seguridad.
- Auditor.
- Responsable de Documentación.

Respecto a los procedimientos operacionales y responsabilidades, e-certchile cuenta con la operación del servicio de Sello de Tiempo de la certificadora, el que opera de manera independiente de otros servicios provistos por la certificadora de firma electrónica; siendo éstas desarrolladas por el personal confiable como se encuentra definido en la estructura de e-certchile y en esta Práctica de Sello de Tiempo e-certchile (CPST e-certchile).

9. Gestión de acceso a los sistemas.

e-certchile, asegura que el acceso a su sistema (hardware, software y datos) se encuentra protegido compartiendo las medidas de seguridad físicas que dan protección al sistema en un entorno de confianza y está limitado al personal autorizado.

Los administradores de e-certchile realizan un monitoreo continuo para detectar intentos o accesos no autorizados a los activos de la certificadora. Es por ello que se cuenta con Cortafuegos, Administración de usuarios, Restricciones de acceso a la información y sistemas, un control apropiado del personal autorizado, Logs de las operaciones. Adicionalmente, los componentes de la red local se mantienen en Data Center bajo ambiente seguro y con una auditoría periódica.

10. Mantenimiento e implementación de sistemas de confianza.

e-certchile se asegura que el sistema y productos están protegidos contra modificaciones no autorizadas, es por ello que se establece monitorear y registrar cada cambio en los sistemas. Para cualquier cambio en los sistemas se lleva a cabo un análisis de requerimientos de seguridad, procedimientos de control de cambio

para nuevas versiones y la generación de las llaves siempre se lleva a cabo dentro del entorno de confianza, por personal critico autorizado.

11. Compromiso de los servicios de la certificadora.

e-certchile declara que ante cualquier compromiso de los servicios de sello de tiempo, se harán efectivos los procedimientos correspondientes al plan de continuidad de e-certchile. Si este compromiso afecta a la llave de firma de la unidad de sello de tiempo o pérdida de precisión de su reloj, se declarará un evento de seguridad y se informará directamente o a través de su sitio web a sus suscriptores y terceros que en ella confía, dicha información del evento. Ante los eventos antes mencionados, la e-certchile no emitirá nuevos sellos de tiempo hasta superar el compromiso declarado.

12. Cese de la certificadora.

En el momento en que e-certchile vaya a descontinuar sus operaciones como certificadora de sello de tiempo, procederá a comunicar del cese de sus funciones

con la debida antelación a todas las partes involucradas con sus servicios de sello de tiempo ya sean suscriptores, terceros de confianza y autoridades de sello de tiempo acreditadas. Además la certificadora procederá revocar los certificados de la unidad de sello de tiempo y transferir los datos de sus sellos de tiempo a otro prestador de servicios, en la fecha en que el cese se produzca. En el caso de las claves y copias de respaldo de e- certchile, estas deben ser borradas y destruidas, de manera que estas no puedan ser recuperadas, de acuerdo a lo especificado en la Práctica de Sello de Tiempo e-certchile (CPST e-certchile).

13. Registro de información relativa a las operaciones del servicio de sello de tiempo.

e-certchile debe mantener registros de la información relevante, concerniente a su operación. Estos registros corresponden a la información personal de los suscriptores que se ha recolectado y se encuentra protegida de acuerdo con la Política de Privacidad de datos personales publicados por e- certchile en su sitio

web, tal como se detalla en la Práctica de Sello de Tiempo de e-certchile (CPST e-certchile).

La integridad de esta información es mantenida por e-certchile por un periodo de 5 años posterior a la expiración de la validez de la llave usada para la firma por parte de la TSU.

Estos registros incluyen:

- Requerimiento de sello de tiempo Sello de tiempo creado.
- Eventos relacionados con la administración de la certificadora, incluyendo:
    - Registros de eventos correspondientes al ciclo de vida de las llaves de la unidad de sello de tiempo.
    - Registros de eventos correspondientes a los certificados de la unidad de sellos de tiempo.
    - Registros relacionados con la sincronización del reloj de usado por la unidad de sello de tiempo contenida en sus sellos de tiempo.
    - Registros asociados a eventos de detección de pérdida de sincronización

Los registros antes mencionados, son almacenados por e-certchile. A estos registros, sólo tiene acceso el personal autorizado por la PSC de e-certchile.

14. Administración de la CPST.

14.1. Procedimiento de Modificación de la CPST.

Las “CPST e-certchile” puede ser modificada cada vez que se estime necesario para asegurar que se mantengan tecnológicamente vigentes, así como, para alterar la forma en que se desarrolla la actividad por la introducción de mejoras en las

instalaciones, sistemas, programas informáticos y los recursos humanos empleados por e-certchile.

Cualquier modificación que se haga a esta "CPST e-certchile" deberá tener una fecha de entrada en vigor no inferior a los 30 días desde la fecha en que se publica en www.e-certchile.cl.

14.2. Políticas de publicación y notificación.

La modificación de esta "CPST e-certchile" será notificada a los Suscriptores de certificados de e-certchile mediante correo electrónico enviado al correo contenido en el certificado de firma electrónico con 30 días de anticipación a la fecha en que entren en vigor las modificaciones introducidas.

El Titular tendrá el plazo indicado para objetar la modificación, en cuyo caso los contratos firmados se entenderán resueltos.

Transcurrido dicho plazo sin que medie comunicación se entenderá que el Suscriptor acepta los cambios introducidos.

14.3. Procedimiento de aprobación de las CPST.

Cualquier nueva versión de la "CPST e-certchile" estará sujeta a un procedimiento de aprobación que considera:

- Elaboración y aprobación interna de la nueva ".
- Presentación de las "CPST e-certchile" al Directorio de e-certchile.
- Una vez pasada las aprobaciones anteriores, se publicarán las nuevas "CPST e-certchile" indicando la fecha de entrada en vigor.

Una vez publicadas las "CPST e-certchile" se informará de éstas a la Entidad Acreditadora.

NORMA(S) QUE APLICA(N)	
Norma	**Referencia Normativa**
ISO 9001:2015	5.2 Política | 8.2.2 Determinación de los requisitos relacionados con los productos y servicios
ISO 27001:2013	5.2 Política
Guía de Acreditación (Minecon) FEA	N/A
Guía de Acreditación (Minecon) BIO	N/A
Guía de Acreditación (Minecon) TSA	PO02 – PO01

CONTROL DE CAMBIOS		
N° DE VERSIÓN	**FECHA**	**DESCRIPCIÓN DE CAMBIOS**
0	Julio/2020	Creación del documento. se recomienda la lectura complete del documento