Agencia de Tecnología y Certificación Electrónica

Política de Sellado de Tiempo de la Agencia de Tecnología y Certificación Electrónica

ISTEC
Firmado digitalmente por ISTEC
Fecha: 2020.11.30 09:05:03 +01'00'

Tabla de Contenido

1. Introducción

1.1. Objeto

Esta Política establece las reglas generales empleadas por la Autoridad de Sellado de Tiempo de la Agencia de Tecnología y Certificación Electrónica – Instituto Valenciano de Finanzas (en adelante ACCV), para la emisión de tokens que contienen sellos de tiempo firmados. Se establecen en este documento los participantes de estos procesos, especificando sus responsabilidades, derechos y ámbito de aplicación.

La presente política es conforme a la norma del ETSI EN 319 421 v1.1.1 “Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers issuing Time-Stamps ” y a su especificación equivalente RFC-3628 “Policy Requirements for time-stamping authorities”.

Esta Política asume cierto grado de conocimiento por parte del lector de conceptos relacionados con las infraestructuras de clave pública y los sellos de tiempo. Si este no fuera el caso, se recomienda al lector que se informe sobre los temas anteriores antes de continuar con la lectura del presente documento.

El presente documento puede ser usado por las partes confiantes y los subscriptores de los servicios proporcionados por la ACCV como base para garantizar la confianza de los servicios que se describen en este documento.

Esta política está basada en criptografía de clave pública, fuentes de tiempo fiables y certificados X.509 v3.

2. Referencias

Los documentos que se citan a continuación se mencionan a lo largo del texto:

[1] Declaración de Prácticas de Certificación de la ACCV (CPS)

[2] ETSI EN 319 421 “Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers issuing Time-Stamps ”

[3] RFC-3161 “Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP)”

[4] ETSI EN 319 422 “Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles ”

[5] ETSI TS 119 312 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites ”

[6] Política de Seguridad de la ACCV

[7] Política de Archivo de la ACCV

[8] Política de Auditoria de la ACCV

[9] Política de Copias de la ACCV

[10] Política de Gestión del Cambio de la ACCV

[11] Organigrama y Funciones de la ACCV

[12] Plan de Continuidad del Servicio de la ACCV

3. Definiciones y abreviaturas

3.1. Definiciones

Para los propósitos del presente documento, se aplican los siguientes términos y definiciones:

Autoridad de Sellado de Tiempo: Sistema de emisión y gestión de sellos de tiempo seguros

Subscriptor: Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sellado de Tiempo de la ACCV.

Token de sello de tiempo: Dispositivo de datos empleado en un proceso de creación de firma electrónica, que une la representación de un dato a un tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo.

Usuario: Destinatario de un Token de sello de tiempo y que confía en el mismo.

Declaración de Prácticas de sellado de tiempo: Declaración de las Prácticas que una Autoridad de sellado de tiempo emplea en la emisión. En el caso de la ACCV, todos los puntos que debe tratar esta declaración se encuentra integrada con los documentos operacionales, de procedimiento y técnicos que engloban toda la plataforma.

Otras definiciones aplicables pueden encontrarse en la CPS [1], Glosario.

3.2. Abreviaturas

TSA: Autoridad de Sellado de Tiempo

TSS: Servicio de sellado de tiempo

TSQ: Solicitud de sello de tiempo

ACCV: Agencia de Tecnología y Certificación Electrónica

TST: Token de sello de tiempo

IETF: Internet Engineering Task Force

CEN: Comité Europeo de Normalización

CWA: CEN Workshop Agreement

RFC: Request for comment

UTC: Universal Time Coordinated

CRL: Certificate Revocation List

FIPS: Federal Information Processing Standards

HSM: Hardware Security Module

GPS: Global Positioning System

ETSI: European Telecommunications Standards Institute

4. Conceptos Generales

4.1. Servicio de sellado de tiempo (TSS)

El servicio de sellado de tiempo proporcionado por la ACCV, se divide en este documento a efectos explicativos en dos subsistemas:

- Sistema de generación y emisión de sellos de tiempo
- Sistema de control, monitorización y supervisión de la emisión de sellos de tiempo.

El sistema de control se ocupa de garantizar el acceso a fuentes de tiempo fiables y del control de los programas responsables de la emisión.

Esta división se realiza únicamente a efectos de facilitar la comprensión de estos sistemas y los requisitos de los mismos en el presente documento, y no supone ninguna restricción a la hora de efectuar otras divisiones a nivel de implementación.

4.2. Autoridad de Sellado de Tiempo (TSA)

La autoridad en la que confían los usuarios de los servicios de sellado de tiempo (suscriptores y partes confiantes) para la emisión de los sellos de tiempo. La TSA tiene responsabilidad global en la provisión del servicio de sellado de tiempo que se identifica en la cláusula 4.1.

4.3. Comunidad de usuarios y ámbito de aplicación

4.3.1. Subscriptores

Los subscriptores de este servicio son los organismos y entidades, públicas o privadas, así como las personas físicas, que dispongan de un cliente de sellado de tiempo compatible con el estándar RFC-3161.

4.3.2. Partes confiantes

Se limita el derecho a confiar en los sellos de tiempo emitidos conforme a la presente política a:

Las aplicaciones y servicios pertenecientes a entidades u organizaciones públicas que tengan acceso a los servicios de validación de la ACCV, de la Administración General del Estado o de otras entidades capaces de proporcionar información de validez de certificados expedidos por la ACCV.

Las aplicaciones y servicios que se emplean en relaciones entre ciudadanos, empresas u otras Administraciones Públicas.

4.3.3. Ámbito de aplicación

El ámbito de aplicación de los sellos de tiempo emitidos por la presente política se circunscribe a la comprobación de la existencia de un dato en un tiempo determinado.

5. Política de Sellado de Tiempo

5.1. Vista general

La presente política establece el conjunto de reglas utilizadas durante la emisión y el control de los tokens de sello de tiempo (TST), y regulan además el nivel de seguridad para la TSA.

Los tokens de sellado de tiempo son emitidos con una desviación máxima de 500ms.

El perfil del certificado de la TSA, utilizado en la firma de los TST, se ajusta a lo especificado por el IETF en RFC-3161. En la Tabla 1 se detallan los campos básicos de este perfil.

Tabla 1. Perfil del certificado de la TSA

Nombre del campo	Valor
Version	Version 3
Serial Number	Valor unico para todos los certificados emitidos por la ACCV
Signature Algorithm	sha256withRSAEncryption (1.2.840.113549.1.1.11)
Issuer	Common Name(CN)
	Organizacional Unit Name
	Organization Name
	Country
Not before (Fecha de inicio de la validez del certificado)	Valor UTC (Universal Time Coordinated) Fecha de inicio del periodo de validez del certificado
Not Alter (Fecha de finalización de la validez del certificado)	Valor UTC (Universal Time Coordinated) Fecha de finalización del periodo de validez del certificado
Subject (Distinguished Name)	Common Name (CN)
	Organizacional Unit Name
	Organization Name
	Locality
	State
	Country
Subject Public Key Info	Codificado de acuerdo al RFC 5280, contiene información de la clave publica RSA. Tamaño mínimo 4096 bits
Signature	Certificado de firma. Generado y codificado acorde al RFC 5280
Uso de la clave	Firma digital , Sin repudio (c0) Marcado como crítico
Uso extendido de la clave	Impresión de fecha (1.3.6.1.5.5.7.3.8) Marcado como crítico

La TSA que proporciona sus servicios bajo la estructura de la ACCV, emite los sellos de tiempo acorde a la recomendación ETSI EN 319 422. Cada sello de tiempo incluye el identificador de la política, descrito en el capítulo 5.2 “Identificación de la política de sellado de tiempo”, de la presente política.

El servicio de Sellado de Tiempo es accesible vía http en la dirección tss.accv.es por el puerto 8318. La URL a definir en el cliente es http://tss.accv.es:8318/tsa.

5.2. Identificación de la política de sellado de tiempo

La información de la política, que controla la emisión y el control de los tokens de sellado de tiempo, esta definida en la Tabla 2.

Identificador de la política	Nombre de la política de certificación
iso(1) identified-organization(3) US-Deparment of Defense(6) Internet(1) Private(4) Enterprises(1) Generalitat Valenciana(8149) CP(3) Politica(100) Version(2) Subversion(0)	Política de Sellado de Tiempo de la ACCV

El OID de identificación de la política será, por tanto: **1.3.6.1.4.1.8149.3.100.2.0**

El identificador de la política de la Autoridad de Sellado de Tiempo de la ACCV está incluido en cada sello de tiempo. También aparece en el documento de Declaración de Términos y Condiciones de Uso de la Autoridad de Sellado de Tiempo.

5.3. Aplicación del sellado de tiempo

Los sellos de tiempo emitidos por la Autoridad de Sellado de Tiempo de la ACCV pueden emplearse para garantizar las transacciones y el no repudio en procesos entre ciudadanos, empresas y Administraciones Públicas.

6. Obligaciones y responsabilidades

6.1. Obligaciones de la TSA

6.1.1. General

La Agencia de Tecnología y Certificación Electrónica, como Autoridad de Sellado de Tiempo, está obligada a:

- Realizar sus operaciones en conformidad con esta Política.
- Proteger sus claves privadas
- Emitir sellos de tiempo que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.
- Garantizar que puede determinarse con precisión la fecha y la hora a la que se emitió un sello de tiempo.
- Publicar esta política y los documentos relacionados en el sitio web http://www.accv.es/tss, garantizando el acceso a las versiones actuales y anteriores.
- Garantizar que todos los requerimientos de la TSA, incluidos procedimientos, prácticas relativas a la emisión de tokens y revisión de sistemas están conforme se describe en las documentos operacionales, de procedimiento y técnicos de la ACCV.

La TSA actúa conforme los anteriores procedimientos, no permitiéndose exclusiones a esta regulación. Obligaciones adicionales de la ACCV, subscriptores y partes confiantes pueden encontrarse en los apartados 1.3 y 9 de la CPS [1].

6.1.2. Obligaciones de la Autoridad de Sellado de Tiempo hacia sus subscriptores

La ACCV garantiza el acceso permanente a las servicios de sellado de tiempo que proporciona, excluyendo paradas técnicas de mantenimiento de los mismos, especificadas en documentos

separados, y que hagan referencia a la conservación de sistemas y equipos. Estas paradas técnicas deberán planificarse con la suficiente antelación, tener una duración determinada (no superior a 3 horas) y avisar a los subscriptores del servicio, utilizando los medios de difusión disponibles.

El tiempo UTC, que se incluye en los sellos de tiempo, asegura una desviación máxima de 500ms.

La ACCV garantiza también que:

- Los sistemas utilizados en la provisión de estos servicios se ajusta a lo contemplado en la normativa técnica europea en vigor (CWA-14172).
- No hay ningún procesamiento de datos personales asociado a la operación de la Autoridad de Sellado de Tiempo..
- Se cumplen las normas técnicas mencionadas en el capítulo 5.1 “Vista general”, del presente documento.

Información adicional, definiendo responsabilidades de la ACCV, puede encontrarse en la CSP [1], apartado 9.6.1 “Obligaciones de la Entidad de Certificación”.

6.2. Obligaciones de los subscriptores

En el proceso de obtención de un sello de tiempo, los subscriptores deben verificar la firma electrónica de la ACCV y comprobar en la CRL el estado del certificado de la TSA. La CRL en vigor se encuentra disponible en la dirección http://www.accv.es/ciudadanos/validacion-de-certificados/. La comprobación de la validez puede hacerse, además, utilizando el servicio OCSP proporcionado por la ACCV en http://ocsp.accv.es.

Obligaciones adicionales pueden encontrarse en la CPS [1], apartado 9.6.3 “Obligaciones de los subscriptores”.

6.3. Obligaciones de las partes confiantes

La obligación general de las partes confiantes es la verificación de la firma del sello de tiempo. Deben comprobar el estado del certificado de la ACCV y su periodo de validez.

En el caso de la verificación de un sello de tiempo, después de la expiración del certificado de la TSA, deben:

- Verificar que el número de serie del certificado de la TSA no se encuentra en la CRL, o determinar la validez del certificado de la TSA por otros mecanismos que articule la ACCV.

- Verificar que las funciones y algoritmos criptográficos usados son todavía seguros, y que el tamaño de la clave usada garantiza esta seguridad.

Obligaciones adicionales pueden encontrarse en la CPS [1], apartado 9.6.4, “Obligaciones de las partes confiantes”

6.4. Responsabilidad financiera

La responsabilidad financiera se encuentra reflejada en la CPS [1], apartados 9.2 y 9.8.

7. Requerimientos de la Autoridad de Sellado de Tiempo

La ACCV, como Autoridad de Sellado de Tiempo, completa la información ofrecida en esta política con:

- Prácticas de Sellado de Tiempo
    - Documentos que explican cómo se implementan los controles mencionados en esta política. Todas las políticas y procedimientos operacionales y técnicos se encuentran englobados en las políticas y procedimientos operacionales y técnicos de la ACCV (política de copias, política de archivo, mantenimiento y securización de sistemas, etc.). Estos documentos son de uso interno.

7.1. Prácticas de Sellado de Tiempo

7.1.1. Prácticas de Sellado de Tiempo

Estos documentos detallan la implementación de los controles necesarios para garantizar la fiabilidad y confianza del servicio. Se encuentran integrados en los documentos correspondientes de políticas y procedimientos operacionales y técnicos de la ACCV.

Se detallan los mecanismos y procedimientos establecidos para el cumplimiento de lo establecido en el capítulo 6, “Obligaciones y responsabilidades”, del presente documento, que constituyen las bases del funcionamiento de la TSA.

Estos documentos son:

- Política de Seguridad
- Política de Archivo
- Política de Auditoria
- Política de Copias
- Política de Gestión del Cambio

Otros controles, que afectan a su funcionamiento en base a su relación con la ACCV, se describen en la CPS [1] como de uso interno. Específicamente, y referentes a procedimientos y mecanismos de control, se clasifica de este modo la información relativa a los capítulo 6.5 “Controles de seguridad informática” y 6.6 “Controles de seguridad del ciclo de vida”.

Toda la creación de regulaciones y procedimientos, así como sus modificaciones y planes de mejora, se llevan a cabo por el departamento de documentación de la ACCV, asesorados por los responsables técnicos de la infraestructura, consultores y abogados, miembros todos ellos del equipo de la ACCV. Los elementos para contactar con los responsables, se detallan en la CPS [1], capítulo 1.5 “Política de Administración de la ACCV”.

7.2. Gestión del ciclo de vida de las claves

7.2.1. Generación de claves de la TSA

Las claves de la TSA se generan en módulo de seguridad hardware (en adelante HSM), que cumple con el estándar NIST FIPS 140-1 nivel 4, por personal autorizado de la ACCV. La descripción de los roles y controles del personal puede encontrarse en la CPS [1], en el apartados 5.2 “Controles de Procedimientos”.

El entorno de generación de las claves cumple los requisitos normativos impuestos por la ACCV, de acuerdo con la CPS [1] y cumplen con los requerimientos descritos en ISO 15408 (Information technology. Security techniques. Evaluation criteria for IT security).

El algoritmo y tamaño de claves se describen en el capítulo 5.1 “Vista general” de esta política, cumpliendo lo referenciado por ETSI TS 119 312 “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites ” [5].

7.2.2. Protección de la clave privada de la TSA

Los niveles de seguridad del HSM donde se almacena la clave se describen en el capítulo 7.2.1 “Generación de la clave de la TSA” de esta política.

Esta clave se encuentra bajo control multipersonal. Se encuentra dividida en varios fragmentos y es necesario un mínimo de dos de estos fragmentos para recomponer la clave.

Las copias de respaldo de la clave privada se almacenan cifradas en archivos seguros ignífugos.

7.2.3. Distribución de la clave pública de la TSA

El certificado de la TSA, que incluye su clave publica, se distribuye utilizando los mecanismos facilitados por la ACCV. Puede encontrarse en el directorio LDAP de la ACCV, ldap.accv.es, así como en el sitio Web http://www.accv.es.

El certificado de la TSA se encuentra firmado por la autoridad superior raíz de la ACCV. Información adicional a la publicación de certificados por parte de la ACCV puede encontrarse en la CPS [1], capítulo 6.1.4 “Entrega de la clave pública de la CA a los usuarios”.

7.2.4. Regeneración de la clave de la TSA

El procedimiento de regeneración de la clave de la TSA se lleva a cabo una vez que ha expirado el certificado y claves actuales, o cuando se verifique un compromiso de la misma por debilidades descubiertas en su algoritmo o longitud.

Las claves privadas caducadas se almacenan por un periodo no inferior a 10 años siendo la ACCV la ejecutora del procedimiento y la responsable de esta decisión. Las claves públicas se almacenan por un periodo adicional no inferior a 15 años, para permitir la verificación de sellos de tiempo emitidos con dichas claves.

7.2.5. Destrucción de la clave privada de la TSA

La ACCV garantiza, en base a sus sistemas de emisión y gestión de sellos de tiempo, que no se aceptarán peticiones que involucren a claves caducadas, y que se opera con las claves regeneradas en el instante que esta caducidad ocurre.

Los procedimientos detallados para la destrucción de las claves privadas se consideran de uso interno, siendo revisados por el auditor de forma periódica.

Información adicional puede encontrarse en el capítulo 7.2.4, “Regeneración de las claves de la TSA” de la presente política.

7.2.6. Gestión de los HSM

La ACCV efectúa los análisis recomendados por los fabricantes de los HSM, acordes con la normalización técnica existente, para garantizar que los equipos no han sido manipulados y cumplen con los requisitos.

Los HSM se trasladan por personal interno de la ACCV con roles autorizados para su inicialización y puesta en marcha en las dependencias internas seguras, con los controles de seguridad física adecuados, siendo desde este momento todas las manipulaciones registradas y auditadas.

En caso de cambio de HSM por cualquier motivo, las claves son borradas y destruidas, de acuerdo con los procedimientos que a tal fin suministra el fabricante.

La ACCV dispone de procedimientos asociados para el manejo de los HSM, clasificados de uso interno y revisados de forma periódica por el auditor.

7.3. Sellado de tiempo

7.3.1. Token de sello de tiempo

Cada sello de tiempo emitido por la Autoridad de Sellado de Tiempo de la ACCV incluye un identificador único de política, descrito en el capítulo 5.2 “Identificación de la política de sellado de tiempo” de este documento. Los sellos de tiempo incluyen valores de fecha y hora identificables, mediante los cuales se puede llegar al valor de tiempo UTC.

La fuente de hora fiable que se codifica en los sellos de tiempo proviene de la red de servidores NTP de la ACCV, de fiabilidad probada y que enlaza, en última instancia, con el organismo encargado de forma oficial de mantener la fuente nacional de tiempos, el Real Instituto y Observatorio de la Armada (ROA), de San Fernando (Cádiz). Esta red de tiempos es tolerante a fallos y dispone de caminos alternativos de sincronización. La exactitud del tiempo usado en los sellos se describe en el capítulo 6.1.2 “Obligaciones de la TSA hacia sus subscriptores” de la presente política.

En caso de que sea imposible la obtención de la exactitud requerida por parte de la fuente de tiempos por cualquiera de los caminos establecidos, tal y como se describe en el capítulo 6.1.2, el token de sello de tiempo no será emitido.

Los tokens de sello de tiempo (TST) son emitidos conteniendo los datos recibidos en la petición (TSQ), garantizando así la presencia dato tiempo origen del servicio. Los sellos de tiempo son firmados por la clave privada de la Autoridad de Sellado de Tiempo, cuyo perfil de certificado asociado y extensiones se encuentran descritas en el capítulo 5.1 “Vista general” de la presente política. Estas claves y certificado han sido generados exclusivamente para este propósito por parte de la ACCV.

La Autoridad de Sellado de Tiempo establece todo el procedimiento asociado a la generación de los tokens de sellos de tiempo utilizando el protocolo descrito en RFC-3161 [3].

7.3.2. Sincronización del reloj con UTC

ACCV establece la exactitud del tiempo en los sellos de tiempo tal y como se refleja en el apartado 6.1.2 “Obligaciones de la TSA hacia sus subscriptores” de esta política. Las fuentes de tiempos utilizadas, basadas en el protocolo NTP (Network Time Protocol) se auto calibran por distintos caminos, haciendo que la exactitud no disminuya por debajo de los requerimientos especificados (apartado 6.1.2 del presente documento), utilizando como referencia la del Real Instituto y Observatorio de la Armada. Se disponen de distintos caminos de sincronización de forma que la manipulación de los sistemas no afecta a la exactitud del sello de tiempo.

A nivel interno la ACCV dispone de mecanismos de seguridad que evitan la manipulación física de sus sistemas (información adicional en la CPS, apartado 5.1 “Controles de Seguridad Física”).

ACCV incorpora mecanismos que detectan diferencias entre el tiempo suministrado y el que se incluye en los sellos de tiempo. El cálculo del tiempo se realiza de acuerdo al protocolo NTP y a lo establecido por la “Oficina Internacional de Pesos y Medidas” (BIPM).

7.3.3. Funciones resumen (hash)

El servicio soporta los siguientes algoritmos de resumen (hash) en las peticiones: SHA1, SHA256, SHA384, SHA512.

El algoritmo SHA1 esta en desuso y presenta problemas de seguridad, por lo que se recomienda no utilizarlo.

En las respuestas de los sellos de tiempo se utiliza por defecto el algoritmo SHA256.

7.3.4. Formato de las solicitudes

Las solicitudes de sello de tiempo siguen el esquema definido en el RFC-3161 (TSP via HTTP)

Se define el objeto MIME

Content-Type: application/timestamp-query
<<the ASN.1 DER-encoded Time-Stamp Request message>>

El tratamiento de los campos opcionales es como sigue:

Campo	**Valor**
reqPolicy	Si presente, espera que sea una de las políticas aceptadas. 1.3.6.1.4.1.8149.3.100.2.0
nonce (opcional)	Valor de comprobación. Si esta presente la respuesta lleva el mismo valor
certReq	Si presente incluye el certificado de TSA en la respuesta

7.3.5. Formato de las respuestas

Las respuestas de sello de tiempo siguen el esquema definido en el RFC-3161 (TSA via HTTP)

Se define el objeto MIME

Content-Type: application/timestamp-reply

<<the ASN.1 DER-encoded Time-Stamp Response message>>

El tratamiento de los campos opcionales es como sigue:

Campos	Valor
Política	Por defecto: 1.3.6.1.4.1.8149.3.100.2.0
Ordering	True
nonce	Si presente debe coincidir con el valor enviada en la solicitud
Certificados incluidos	Si se solicita, certificado de la TSA
accuracy	500ms
TSA	GeneralName con los datos del certificado de la TSA
Extensiones	QcStatements esi4-qtstStatement-1 0.4.0.19422.1.1

En caso de no poder procesar la solicitud se devuelve un código de error de los definidos en el RFC-3161

```
PKIFailureInfo ::= BIT STRING {
   badAlg              (0),
     -- unrecognized or unsupported Algorithm Identifier
   badRequest          (2),
     -- transaction not permitted or supported
   badDataFormat       (5),
     -- the data submitted has the wrong format
   unacceptedPolicy    (15),
     -- the requested TSA policy is not supported by the TSA.
   unacceptedExtension (16),
     -- the requested extension is not supported by the TSA.
   systemFailure       (25)
     -- the request cannot be handled due to system failure  }
```

7.4. Operación y gestión de la TSA

7.4.1. Gestión de la seguridad

Todos los elementos relativos al control de la seguridad se describen en la Política de Seguridad de la ACCV de Sellado de Tiempo y en la CPS [1], apartado 5.2 “Controles procedimentales”, siendo acordes a lo establecido en ISO-17799.

7.4.2. Control de riesgos e inventario de activos

Todos los elementos relativos al control de riesgos e inventario de activos se encuentran en documentación de la ACCV clasificada de USO INTERNO, revisada de forma periódica por el auditor. Se sigue lo establecido en el estándar ISO-27001.

ACCV realizara un análisis de riesgos anualmente, usando para ello metodologías y herramientas apropiadas.

7.4.3. Seguridad del personal

Características del personal, así como los roles establecidos e incompatibilidades, se describen en la Política de Seguridad de la ACCV, el documento de Organigrama y Funciones y en la CPS[1], apartado 5.3 “Controles de seguridad de personal” y en varios documentos clasificados de uso interno, solo se proporciona a quien acredite necesidad de conocerla y son revisados de forma periódica por el auditor. Se sigue lo establecido en el estándar ISO-27001.

7.4.4. Seguridad física

La descripción de la seguridad física se detalla en la Política de Seguridad de la ACCV y en la CPS[1], apartado 5 “Controles de seguridad física, de gestión y de operaciones”. Estos controles cumplen con los requerimientos normativos del estándar ISO-27001.

7.4.5. Gestión de las operaciones

La Autoridad de Sellado de Tiempo de la ACCV tiene establecida controles de seguridad procedimental que afectan a todas las operaciones que involucran la emisión y el control de sellos de tiempo, así como en el manejo y control de los sistemas, sistemas de control de incidencias y gestión de copias de seguridad. La parte publica de esta información se encuentra la CPS [1], el resto se ha clasificado de uso interno.

7.4.6. Gestión de acceso a los sistemas

Los sistemas responsables de la emisión y control de los sellos de tiempo se encuentran en las dependencias de la ACCV, compartiendo las medidas de seguridad física de su entorno de confianza. En concreto, el recinto se encuentra protegido por un sistema de alarma contra intrusiones, operadas 24X7 por personal autorizado.

El acceso lógico a los sistemas está limitado a personal autorizado.

7.4.7. Mantenimiento y despliegue de sistemas de confianza

Dentro de la operación de la Autoridad de Sellado de Tiempo, la generación de las claves de la TSA siempre se lleva a cabo dentro del entorno de confianza de la ACCV, por personal interno con roles autorizados, como se describe en el capítulo 7.2.1 “Generación de claves de la TSA” de la presente política. El sistema cumple con los requerimientos EAL411, siendo monitorizado y registrado cada cambio en los sistemas afectados.

Todas las modificaciones que afectan al servicio de sellado de tiempo involucran, aparte de los análisis funcionales y de requerimientos, un análisis de seguridad y una gestión del cambio controlada, tal y como se recoge en la Política de Gestión del Cambio de la ACCV.

7.4.8. Compromiso de los servicios de sellado de tiempo.

En caso de compromiso de los servicios de sellado de tiempo, se harán efectivos los procedimientos descritos en el Plan de Continuidad de Servicio de la ACCV.

ACCV monitoriza la correcta calibración del reloj de la TSA. En caso de detectar una desviación superior a la establecida en la presente política, el servicio de emisión de sellos de tiempo afectado se detendrá automáticamente, y no sera restablecido hasta que se comprueba de forma manual la corrección de la desviación por debajo del umbral establecido.

Si este compromiso afecta la claves privadas de la Autoridad de Sellado la información relevante será comunicada a los suscriptores del servicio y a partes confiantes, y se interrumpirá el servicio.

La información suministrada incluirá la naturaleza del compromiso, y las herramientas o sistemas necesarios para la comprobación de sus sellos de tiempo, garantizando la identificación de los elementos comprometidos.

7.4.9. Cese de la TSA

La Autoridad de Sellado de Tiempo garantiza la minimización del impacto en caso de cese del servicio de sellado de tiempo. En particular, asegura la continuidad de la información requerida para verificar la corrección de los sellos de tiempo.

En caso de cese de actividad voluntaria, la ACCV, como Autoridad de Sellado de Tiempo, realizara con una antelación mínima de dos meses las siguientes acciones:

- Informar a todos los subscriptores y partes confiantes del cese de actividad y los mecanismos habilitados para garantizar la validez de los sellos existentes.
- Comunicar a los organismos de control pertinentes (Ministerio de Industria, Turismo y Comercio) del cese de actividad y los mecanismos habilitados para garantizar la validez de los sellos existentes.

7.4.10. Cumplimiento de los requisitos legales

La ACCV, como Autoridad de Sellado de Tiempo, actúa acorde a los requisitos establecidos por la legislación vigente (apartado 7.6), en lo que hace referencia a la protección de datos (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal), a las medidas de seguridad de los ficheros informatizados que contengan datos de carácter personal (Real Decreto 1720/2007, de 21 de diciembre) y a la gestión y operación se servicios y sistemas informáticos, siguiendo en los casos en que no hay ley aplicable, las directrices técnicas establecidas por los organismos cualificados (ETSI, CEN, etc).

7.4.11. Registro de información relativa a la operación del servicio de sellado de tiempo

La ACCV, como Autoridad de Sellado de Tiempo, incorpora mecanismos para la creación y control de registros de los eventos derivados de su operación. Estos mecanismos se encuentran descritos en la Política de Archivo de la ACCV, en la Política de Seguridad de la ACCV y en la CPS[1], apartado 5.4 “Procedimientos de control de seguridad”.

7.5. Esquema organizativo

La Autoridad de Sellado de Tiempo se encuentra incluido dentro de la Agencia de Tecnología y Certificación Electrónica – Instituto Valenciano de Finanzas, siendo uno de sus servicios adicionales, tal y como se recoge en CWA-14167-1 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements) Los datos del esquema organizativo se encuentran en la CPS [1], apartado 1.5, “Política de Administración de la ACCV”.

7.6. Requisitos comerciales y legales

7.6.1. Tarifas

7.6.1.1. Tarifas de emisión de sellos de tiempo

Los precios para la emisión de los sellos de tiempo a los que se refiere la presente política de certificación se recogen en la Lista de Tarifas de la Agencia de Tecnología y Certificación Electrónica – Instituto Valenciano de Finanzas. Esta Lista se publica en la página web de la ACCV www.accv.es

7.6.1.2. Tarifas de acceso a los sellos de tiempo

El acceso a los sellos de tiempo emitidos bajo esta política, dada su naturaleza pública, es libre y gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

7.6.1.3. Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados que firman los sellos de tiempo es libre y gratuita y por tanto no se aplicará ninguna tarifa.

7.6.1.4. Tarifas de otros servicios como información de políticas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.1.5. Política de reintegros

No se prevén reintegros de las cantidades entregadas para el pago de los sellos de tiempo.

7.6.2. Capacidad financiera

7.6.2.1. Indemnización a los terceros que confían en los sellos de tiempo emitidos por la ACCV

Tal y como se especifica en la Declaración de Prácticas de Certificación (CPS), la ACCV dispone de garantía de cobertura suficiente de responsabilidad civil a través de aval bancario emitido por Bankia S.A., por importe de Tres Millones de Euros (3.000.000 €) que cubre el riesgo de la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos por esta Autoridad de Certificación, cumpliendo así con la obligación establecida en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

7.6.2.2. Relaciones fiduciarias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.2.3. Procesos administrativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.3. Notificaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

Todos los correos que la ACCV envíe a los suscriptores del servicio de sellado de tiempo descrito en esta Política de Certificación, en el ejercicio de la prestación del servicio de certificación, serán firmados digitalmente para garantizar su autenticidad e integridad.

7.6.4. Modificaciones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.4.1. Procedimientos de especificación de cambios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.4.2. Procedimientos de publicación y notificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.4.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.5. Resolución de conflictos

7.6.5.1. Resolución extrajudicial de conflictos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.5.2. Jurisdicción competente

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.5.3. Legislación aplicable

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.5.4. Conformidad con la Ley aplicable

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.

7.6.5.5. Clausulas diversas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACCV.