



Autoritat de Certificació de la Comunitat Valenciana

Política de Sellado de Tiempo de la ACCV

| | |
|---|-------------------------------|
| Fecha: 23/11/2006 | Versión: 3.4 |
| Estado: APROBADO | Nº de páginas: 21 |
| OID: 1.3.6.1.4.1.8149.1.1.2.6 | Clasificación: PUBLICO |
| Archivo: PoliticaSelladoTiempo.doc | |
| Preparado por: ACCV | |



**Secretaria Autònoma de Telecomunicacions i
Societat de la Informació**

Conselleria d'Infraestructures i Transport

Tabla de Contenido

| | |
|--|-----------|
| 1. INTRODUCCIÓN | 4 |
| 1.1. OBJETO | 4 |
| 2. REFERENCIAS | 5 |
| 3. DEFINICIONES Y ABREVIATURAS | 6 |
| 3.1. DEFINICIONES | 6 |
| 3.2. ABREVIATURAS..... | 6 |
| 4. CONCEPTOS GENERALES | 8 |
| 4.1. SERVICIO DE SELLADO DE TIEMPO (TSS)..... | 8 |
| 4.2. AUTORIDAD DE SELLADO DE TIEMPO (TSA)..... | 8 |
| 4.3. SUBSCRIPTORES | 8 |
| 5. POLÍTICA DE SELLADO DE TIEMPO | 9 |
| 5.1. VISTA GENERAL | 9 |
| 5.2. IDENTIFICACIÓN DE LA POLÍTICA DE SELLADO DE TIEMPO..... | 10 |
| 5.3. APLICACIÓN DEL SELLADO DE TIEMPO | 10 |
| 6. OBLIGACIONES Y RESPONSABILIDADES | 11 |
| 6.1. OBLIGACIONES DE LA TSA..... | 11 |
| 6.1.1. <i>General</i> | 11 |
| 6.1.2. <i>Obligaciones de la Autoridad de Sellado de Tiempo hacia sus subscriptores</i> | 11 |
| 6.2. OBLIGACIONES DE LOS SUBSCRIPTORES | 12 |
| 6.3. OBLIGACIONES DE LAS PARTES CONFIANTES | 12 |
| 6.4. RESPONSABILIDAD FINANCIERA | 13 |
| 7. REQUERIMIENTOS DE LA AUTORIDAD DE SELLADO DE TIEMPO | 14 |
| 7.1. PRÁCTICAS DE SELLADO DE TIEMPO Y DECLARACIÓN DE TÉRMINOS Y CONDICIONES DE USO DE LA AUTORIDAD DE SELLADO DE TIEMPO | 14 |
| 7.1.1. <i>Prácticas de Sellado de Tiempo</i> | 14 |
| 7.1.2. <i>Declaración de Términos y Condiciones de Uso de la Autoridad de Sellado de Tiempo</i> | 15 |
| 7.2. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES..... | 16 |
| 7.2.1. <i>Generación de claves de la TSA</i> | 16 |
| 7.2.2. <i>Protección de la clave privada de la TSA</i> | 16 |
| 7.2.3. <i>Distribución de la clave pública de la TSA</i> | 16 |
| 7.2.4. <i>Regeneración de la clave de la TSA</i> | 16 |
| 7.2.5. <i>Destrucción de la clave privada de la TSA</i> | 17 |
| 7.2.6. <i>Gestión de los HSM</i> | 17 |

| | | |
|----------------------|---------------------------------|--------------|
| Clf.: PUBLICO | Ref.: PolíticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 2 de 21 |

| | | |
|---------|--|----|
| 7.3. | SELLADO DE TIEMPO | 17 |
| 7.3.1. | <i>Token de sello de tiempo</i> | 17 |
| 7.3.2. | <i>Sincronización del reloj con UTC</i> | 18 |
| 7.4. | OPERACIÓN Y GESTIÓN DE LA TSA | 18 |
| 7.4.1. | <i>Gestión de la seguridad</i> | 18 |
| 7.4.2. | <i>Control de riesgos e inventario de activos</i> | 19 |
| 7.4.3. | <i>Seguridad del personal</i> | 19 |
| 7.4.4. | <i>Seguridad física</i> | 19 |
| 7.4.5. | <i>Gestión de las operaciones</i> | 19 |
| 7.4.6. | <i>Gestión de acceso a los sistemas</i> | 19 |
| 7.4.7. | <i>Mantenimiento y despliegue de sistemas de confianza</i> | 19 |
| 7.4.8. | <i>Compromiso de los servicios de sellado de tiempo.</i> | 20 |
| 7.4.9. | <i>Cese de la TSA</i> | 20 |
| 7.4.10. | <i>Cumplimiento de los requisitos legales</i> | 20 |
| 7.4.11. | <i>Registro de información relativa a la operación del servicio de sellado de tiempo</i> | 21 |
| 7.5. | ESQUEMA ORGANIZATIVO | 21 |

1. Introducción

1.1. Objeto

Esta Política establece las reglas generales empleadas por la Autoridad de Sellado de Tiempo de la Autoridad de Certificación de la Comunidad Valenciana (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.

Los sellos de tiempo emitidos bajo esta Política se utilizarán en procesos que tengan a la Administración Pública como una de sus partes.

La presente política es conforme a la norma del ETSI TS 102 023 v1.2.1 “Policy requirements for time-stamping authorities” y a su especificación equivalente RFC-3268 “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 suscriptores de los servicios proporcionados por la ACCV como base para garantizar la confianza de los servicios que se describen en este documento.

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

| | | |
|----------------------|---------------------------------|--------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 4 de 21 |

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 (CSP)
- [2] ETSI TS 102 023 “Policy Requirements for time-stamping authorities”
- [3] RFC-3161 “Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP)”
- [4] ETSI TS 101 861 “Time Stamping Profile”
- [5] ETSI SR 002 176 “Algorithms and Parameters for Secure Electronic Signatures”
- [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

| | | |
|----------------------|---------------------------------|--------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 5 de 21 |

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

Subscriber: 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 CSP [1], Glosario.

3.2. Abreviaturas

TSA: Autoridad de Sellado de Tiempo

TSS: Servicio de sellado de tiempo

TSQ: Solicitud de sello de tiempo

ACCV: Autoridad de Certificación de la Comunidad Valenciana

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

| | | |
|----------------------|---------------------------------|--------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 6 de 21 |

FIPS: Federal Information Processing Standards

HSM: Hardware Security Module

GPS: Global Positioning System

| | | |
|----------------------|---------------------------------|--------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 7 de 21 |

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. Suscriptores

Los suscriptores de este servicio son los organismos de la Generalitat Valenciana, así como cualquier otra administración pública o entidad con la que se haya suscrito el correspondiente convenio de prestación de servicios de firma electrónica.

| | | |
|----------------------|---------------------------------|--------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 8 de 21 |

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. Las normas generales pueden encontrarse en el capítulo 4.4. "Prestaciones generales y política de sellado de tiempo" de este documento.

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 | sha1withRSAEncryption (1.2.840.113549.1.1.5) | |
| Issuer | Common Name(CN) | Root CA Generalitat Valenciana |
| | Organizational Unit Name | PKIGVA |
| | Organization Name | Generalitat Valenciana |
| | Country | ES |
| Not before (Fecha de inicio de la validez del certificado) | Valor UTC (Universal Time Coordinated) Fecha de inicio del periodo de validez del certificado | martes, 21 de noviembre de 2006 18:52:54 |
| Not Alter (Fecha de finalización de la validez del certificado) | Valor UTC (Universal Time Coordinated) Fecha de finalización del periodo de validez del certificado | viernes, 18 de noviembre de 2016 17:52:54 |
| Subject (Distinguished Name) | Common Name (CN) | TSA1 ACCV |
| | Organizational Unit Name | PKIGVA |
| | Organization Name | Generalitat Valenciana |
| | Country | ES |
| Subject Public Key Info | Codificado de acuerdo al RFC 2459, contiene información de la clave publica RSA. Tamaño 2048 bits | |
| Signature | Certificado de firma. Generado y codificado acorde al RFC 2459 | |
| Uso de la clave | Firma digital (80) 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 TS 101 86. 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-Department of Defense(6) Internet(1) Private(4) Enterprises(1) Generalitat Valenciana(8149) CP(3) Politica(20) Version(1) Subversion(0) | Política de Sellado de Tiempo de la ACCV |

El OID de identificación de la política será, por tanto: **1.3.6.1.4.1.8149.3.20.1.0**

El identificador de la política de la Autoridad de Sellado de Tiempo de la ACCV esta 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 e los cuales intervenga la propia Generalitat Valenciana, o cualquier organismo o entidad con los que se haya formalizado un convenio de certificación.

6. Obligaciones y responsabilidades

6.1. Obligaciones de la TSA

6.1.1. General

La Autoridad de Certificación de la Comunidad Valenciana, como Autoridad de Sellado de Tiempo, esta 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, suscriptores y partes confiantes pueden encontrarse en el capítulo 2.1 de la CSP [1].

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

La ACCV garantiza el acceso permanente a los 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 suscriptores del servicio, utilizando los medios de difusión disponibles.

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 11 de 21 |

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], capítulo 2.1.1 “Obligaciones de la CA”.

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/gestcert/rootgva.crl>. 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 CSP [1], capítulo 2.1.3 “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 CSP [1], capítulo 2.1.4, “Obligaciones de las partes confiantes”

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 12 de 21 |

6.4. Responsabilidad financiera

La responsabilidad financiera se encuentra reflejada en la CSP [1], capítulo 2.3, “Responsabilidad financiera”

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 13 de 21 |

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
 - o Documentos que explican como 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.
- La Declaración de Términos y Condiciones de Uso de la Autoridad de Sellado de Tiempo
 - o Resumen de carácter informativo que la Autoridad de Sellado de Tiempo debe divulgar a sus usuarios, con las términos y condiciones de uso de los servicios de sellado de tiempo. Estos documentos se publicarán en la página web de la ACCV.

7.1. Prácticas de Sellado de Tiempo y Declaración de Términos y Condiciones de Uso de la Autoridad 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

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 14 de 21 |

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 1.4 “Datos de contacto”.

7.1.2. Declaración de Términos y Condiciones de Uso de la Autoridad de Sellado de Tiempo

Este documento no reemplaza a la Política de Sellado de Tiempo ni a las Prácticas de Sellado de tiempo, sino que proporciona información suplementaria y simplificada, destinada a los subscriptores del servicio.

Se proporciona así, de forma resumida:

- Personal de contacto
- Ámbito de aplicación
- Algoritmos utilizados
- El tiempo de vida esperado de la firma asociada al sello de tiempo
- La precisión del tiempo del sello con respecto a UTC.
- Las limitaciones de uso
- Las obligaciones de los subscriptores, tal y como se recoge en el apartado 6.2 de la presente política
- Las obligaciones de las partes confiantes, tal y como se describe en el apartado 6.3 de la presente política
- Información de cómo verificar el sello de tiempo y posibles limitaciones del periodo de validez
- El tiempo de retención de los ficheros de eventos asociados al servicio
- La legislación aplicable en la operación del servicio
- Limitaciones de responsabilidad
- Auditorias de conformidad con la presente política

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 15 de 21 |

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, en el apartados 5.2 “Controles Procedimentales” [1].

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 SR 002 176 [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 Backup 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 pública, 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 (ROOTCA de la Generalitat Valenciana). 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.

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 16 de 21 |

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 primaria de tiempo proviene dos receptores de sincronización de tiempos ajustados vía GPS, que consiguen una desviación suficientemente pequeña como para garantizar la precisión de 500ms. del servicio.

La fuente secundaria de tiempo proviene de la red de servidores NTP de la Generalitat Valenciana, de fiabilidad probada y que enlaza, en última instancia, con el organismo encargado 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.

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 17 de 21 |

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 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

La ACCV establece la exactitud del tiempo en los sellos de tiempo tal y como se refleja en el capítulo 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 (capítulo 6.1.2 del presente documento), utilizando como referencia la del Real Instituto y Observatorio de la Armada y la sincronización GPS vía satélite. 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”).

La 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).

7.4. 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], capítulo 5.2 “Controles procedimentales”, siendo acordes a lo establecido en ISO-17799.

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 18 de 21 |

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 la especificación ISO-17799.

La ACCV realizara un análisis de riesgos cada dos años, 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], capítulo 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 la especificación ISO-17799.

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], capítulo 5 “Controles de seguridad física, procedural y de personal”. Estos controles cumplen con los requerimientos normativos del documento ISO-17799.

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 esta 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

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 19 de 21 |

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.

Si este compromiso afecta la claves privadas de la Autoridad de Sellado o a la pérdida de exactitud de los sellos de tiempo, 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 suscriptores 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, 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 994/1999, de 11 de junio) y a la gestión y operación de 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).

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 20 de 21 |

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], capítulo 4.5 “Procedimientos de control de seguridad”.

7.5. Esquema organizativo

La Autoridad de Sellado de Tiempo se encuentra incluido dentro de la Autoridad de Certificación de la Comunidad Valenciana, 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], capítulo 1.4, “Datos de Contacto”.

| | | |
|----------------------|---------------------------------|---------------|
| Clf.: PUBLICO | Ref.: PoliticaSelladoTiempo.doc | Versión: 3.4 |
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.2.6 | Pág. 21 de 21 |