



Política de Certificados de Viafirma TSU

Policy OID 1.3.6.1.4.1.34253.7.3

Viafirma Prestador de Servicios de Confianza

ÍNDICE

1. INTRODUCCIÓN	11
1.1. Resumen	11
1.2. Identificación del Documento	11
1.3. Participantes.....	11
1.3.1. Autoridad de Certificación.....	12
1.3.2. Autoridades de Registro	12
1.3.3. Suscriptores	12
1.3.4. Terceros que confían	13
1.4. Uso del Certificado	13
1.4.1. Usos apropiados del certificado	13
1.4.2. Usos prohibidos del certificado	13
1.5. Administración de Políticas	13
1.5.1. Autoridad de políticas	13
1.5.2. Contacto de la autoridad de políticas	13
1.5.3. Persona que determina la idoneidad de las políticas.....	14
1.5.4. Procedimiento de aprobación de las políticas.....	14
1.6. Definiciones y Acrónimos.....	14
2. PUBLICACIÓN Y REPOSITORIO DE CERTIFICADOS	16
2.1. Repositorios.....	16
2.2. Publicación de la información de certificación	16
2.3. Frecuencia de publicación.....	16
2.4. Control de acceso a los repositorios.....	17
3. IDENTIFICACION Y AUTENTICACIÓN	18
3.1. Uso de nombres	18
3.1.1. Tipo de Nombres	18
3.1.2. Significado de los nombres.....	18
3.1.3. Seudónimos	18
3.1.4. Reglas para interpretar varios formatos de nombre	18
3.1.5. Unicidad de nombres.....	18
3.1.6. Reconocimiento, autenticación y función de las marcas registradas	19
3.2. Validación de identidad inicial	19
3.2.1. Métodos de prueba de la posesión de la clave privada	19
3.2.2. Autenticación de la identidad de una organización	20
3.2.3. Autenticación de la identidad de un individuo	20

3.2.4. Información no verificada del suscriptor	20
3.2.5. Validación de la autoridad	20
3.2.6. Criterios de interoperabilidad	20
3.3. Identificación y autenticación para la renovación de certificados	20
3.3.1. Identificación y autenticación para la renovación de certificado vigente	20
3.3.2. Identificación y autenticación para la renovación un certificado caducado.....	20
3.4. Identificación y autenticación para solicitudes de revocación	21

4. CICLO DE VIDA DEL CERTIFICADO Y REQUISITOS OPERACIONALES..... 22

4.1. Solicitud de Certificados	22
4.1.1. Quién puede solicitar un certificado	22
4.1.2. Proceso de registro	22
4.2. Proceso de solicitud de un certificado	22
4.2.1. Funciones de identificación y autenticación	22
4.2.2. Aprobación o rechazo de solicitudes.....	22
4.2.3. Plazos del proceso de solicitud.....	22
4.3. Emisión de certificados.....	23
4.3.1. Acciones de la CA durante la emisión de certificados	23
4.3.2. Notificaciones a suscriptores por parte de la CA durante la emisión de certificados..	23
4.4. Aceptación del certificado	23
4.4.1. Hechos que constituyen la aceptación del certificado	23
4.4.2. Publicación del certificado por parte de la CA	23
4.4.3. Notificación de la emisión a otras entidades.....	23
4.5. Uso del certificado.....	23
4.5.1. Uso de clave privada del suscriptor	23
4.5.2. Confianza y uso de la clave pública.....	24
4.6. Renovación de certificados.....	24
4.6.1. Situaciones para la renovación de certificados	24
4.6.2. Quién puede solicitar la renovación	24
4.6.3. Proceso de solicitudes de renovación	24
4.6.4. Notificación de la renovación del certificado al suscriptor.....	24
4.6.5. Hechos que constituyen la aceptación del certificado renovado.....	24
4.6.6. Publicación del certificado renovado	25
4.6.7. Notificación de la renovación a otras entidades.....	25
4.7. Reemisión del Certificado	25
4.7.1. Circunstancias para la reemisión del certificado.....	25
4.7.2. Quién puede solicitar la reemisión del certificado	25
4.7.3. Procedimiento para las solicitudes de reemisión del certificado.....	25
4.7.4. Notificación al suscriptor del nuevo certificado reemitido	25
4.7.5. Hechos que constituyen la aceptación del certificado reemitido	26
4.7.6. Publicación por parte de la CA del certificado reemitido	26

4.7.7. Publicación por parte de la CA del certificado reemitido a otras entidades.....	26
4.8. Modificación del certificado	26
4.8.1. Circunstancias para la modificación del certificado	26
4.8.2. Quién puede solicitar la modificación del certificado	26
4.8.3. Proceso de solicitud de modificación del certificado	26
4.8.4. Notificación de la modificación del certificado	26
4.8.5. Hechos que constituyen la aceptación del certificado modificado	27
4.8.6. Publicación por parte de la CA de la modificación del certificado	27
4.8.7. Notificación de la modificación del certificado por parte de la CA a otras entidades..	27
4.9. Revocación y suspensión de certificados.....	27
4.9.1. Situaciones para la revocación.....	27
4.9.2. Quién puede solicitar la revocación.....	27
4.9.3. Proceso para la revocación del certificado	27
4.9.4. Período de gracia de la solicitud de revocación	27
4.9.5. Período en el que la CA debe procesar la solicitud de revocación.....	28
4.9.6. Requisitos de verificación de la revocación por las partes que confían.....	28
4.9.7. Frecuencia de emisión de la CRL	28
4.9.8. Latencia máxima de la CRL	28
4.9.9. Comprobación online del estado de la revocación.....	28
4.9.10. Requisitos para la comprobación online del estado de revocación	28
4.9.11. Otras formas de comprobación del estado de revocación	28
4.9.12. Requisitos especiales para la reemisión de certificados por compromiso de claves .	29
4.9.13. Circunstancias para la suspensión	29
4.9.14. Quién puede solicitar la suspensión	29
4.9.15. Procedimiento para la solicitud de suspensión.....	29
4.9.16. Límites del período de suspensión	29
4.10. Servicios para el estado del certificado.....	29
4.10.1. Características operacionales	29
4.10.2. Servicios disponibles	29
4.10.3. Características opcionales	29
4.11. Fin de la suscripción.....	30
4.12. Depósito de claves y recuperación.....	30
4.12.1. Prácticas para el depósito y recuperación de claves	30
4.12.2. Prácticas de encapsulado y recuperación de recuperación de claves	30

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERACIONALES 31

5.1. Controles físicos.....	31
5.1.1. Localización y construcción	31
5.1.2. Acceso físico	31
5.1.3. Alimentación eléctrica y aire acondicionado	31
5.1.4. Exposición al agua	31
5.1.5. Protección y prevención de incendios.....	31

5.1.6.Sistema de almacenamiento	31
5.1.7.Eliminación de residuos.....	31
5.1.8.Backup remoto.....	31
5.2. Controles procedimentales	32
5.2.1.Roles de confianza	32
5.2.2.Número de personas requeridas por tarea	32
5.2.3.Identificación y autenticación para cada rol	32
5.2.4.Roles que requieren separación de funciones	33
5.3. Controles personales	33
5.3.1.Requisitos de calificación, experiencia y autorización.....	33
5.3.2.Procedimientos de verificación de antecedentes	33
5.3.3.Requisitos de formación	33
5.3.4.Requisitos y frecuencia de formación	33
5.3.5.Frecuencia y secuencia de rotación de tareas	33
5.3.6.Sanciones por acciones no autorizadas.....	33
5.3.7.Requisitos para personal independiente.....	33
5.3.8.Documentación entregada al personal.....	33
5.4. Procedimientos para el registro de auditoría	34
5.4.1.Tipo de eventos registrados.....	34
5.4.2.Frecuencia del procesamiento de registros.....	34
5.4.3.Período de retención del registro de auditoría.....	34
5.4.4.Protección del registro de auditoría.....	34
5.4.5.Procedimiento del backup del registro de auditoría	34
5.4.6.Sistema de recolección de auditoría.....	34
5.4.7.Notificación de eventos	34
5.4.8.Evaluación de vulnerabilidades	34
5.5. Archivo de registros	34
5.5.1.Tipos de archivo de registros	34
5.5.2.Período de retención del archivo	35
5.5.3.Protección del archivo	35
5.5.4.Procedimientos para el backup del archivo	35
5.5.5.Requisitos para el sellado de tiempo del registro	35
5.5.6.Sistema de recolección del archivo.....	35
5.5.7.Procedimientos para obtener y verificar la información del archivo.....	35
5.6. Cambio clave.....	35
5.7. Recuperación en caso de compromiso de la clave o desastre.....	35
5.7.1.Procedimientos para la gestión de incidentes	35
5.7.2.Obsolescencia y deterioro.....	36
5.7.3.Procedimientos ante compromiso de clave de una entidad	36
5.7.4.Plan de continuidad de negocio ante desastres	36
5.8. Cese de la CA o RA.....	36

6. CONTROLES TÉCNICOS DE SEGURIDAD	37
6.1. Generación del par de claves y su instalación	37
6.1.1. Generación del par de claves	37
6.1.2. Entrega de la clave privada al suscriptor	37
6.1.3. Entrega de la clave pública al suscriptor	37
6.1.4. Entrega de la clave pública de la CA a los terceros que confían.....	37
6.1.5. Tamaño de las claves	37
6.1.6. Control de calidad de los parámetros de generación de la clave pública.....	37
6.1.7. Propósito de uso de la clave.....	38
6.2. Protección de clave privada y controles del módulo criptográfico	38
6.2.1. Controles y estándares del módulo criptográfico	38
6.2.2. Control dual n de m para el uso de la clave privada	38
6.2.3. Depósito de la clave privada	38
6.2.4. Backup de la clave privada.....	38
6.2.5. Archivo de la clave privada	38
6.2.6. Importación de la clave privada al módulo criptográfico.....	38
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico	39
6.2.8. Método de activación de la clave privada	39
6.2.9. Método de desactivación de la clave privada.....	39
6.2.10. Método de destrucción de la clave privada.....	39
6.2.11. Clasificación del módulo criptográfico.....	39
6.3. Otros aspectos sobre la gestión de par de claves.....	39
6.3.1. Archivo de la clave pública.....	39
6.3.2. Periodos operativos de certificado y periodos de uso del par de claves.....	39
6.4. Datos de activación	40
6.4.1. Generación e instalación de datos de activación	40
6.4.2. Protección de los datos de activación.....	40
6.4.3. Otros aspectos de los datos de activación.....	40
6.5. Controles de seguridad informática	40
6.5.1. Requisitos técnicos de los controles de seguridad	40
6.5.2. Clasificación de la seguridad	40
6.6. Ciclo de vida de los controles técnicos.....	40
6.7. Controles de seguridad de red.....	41
6.8. Sello de tiempo	41
6.8.1. Tipos y usos de los sellos de tiempo electrónico	42
6.8.1.1. Formato de la Request	43
6.8.1.2. Formato de la Response.....	43
7. CERTIFICADOS, CRL, OCSP Y PERFILES	45
7.1. Perfil de certificado.....	45
7.1.1. Número de versión.....	45

7.1.2. Extensiones del certificado	45
7.1.3. Identificador (OID) del algoritmo de firma	47
7.1.4. Uso de nombres	47
7.1.5. Restricciones de nombres.....	47
7.1.6. Identificador de política de certificado.....	47
7.1.7. Uso de la extensión de política de restricciones.....	47
7.1.8. Sintaxis y semántica de la política de calificadoros	48
7.1.9. Semántica del procedimiento para las extensiones críticas del certificado	48
7.2. Perfil de la CRL	48
7.2.1. Número de versión.....	48
7.2.2. CRL y extensiones.....	48
7.3. Certificado OCSP.....	49
7.3.1. Certificado utilizado para firma el OCSP que valida el certificado de TSA SUB CA	49
7.3.2. Certificado utilizado para firma el OCSP que valida el certificado de TSU.....	51
8. AUDITORÍAS.....	54
8.1. Frecuencia o circunstancias de la auditoría	54
8.2. Identidad y cualificación del auditor	54
8.3. Relación del auditor con el prestador	54
8.4. Temas tratados en la auditoría	54
8.5. Acciones a realizar como resultado de una deficiencia	54
8.6. Comunicación de resultados	54
9. OTROS ASUNTOS LEGALES.....	55
9.1. Tarifas.....	55
9.1.1. Tarifa para la emisión y renovación de certificados	55
9.1.2. Tarifa de acceso al certificado	55
9.1.3. Tarifa de acceso a OCSP o CRL	55
9.1.4. Tarifa para otros servicios.....	55
9.1.5. Política de reembolsos	55
9.2. Responsabilidad financiera.....	55
9.3. Confidencialidad de la información comercial.....	56
9.3.1. Alcance de la información confidencial	56
9.3.2. Alcance excluido de la información confidencial.....	56
9.3.3. Responsabilidad para la protección de la información confidencial	56
9.4. Privacidad de la información personal	56
9.4.1. Plan de privacidad	56
9.4.2. Información con tratamiento privado	56
9.4.3. Información no considerada con tratamiento privado	56
9.4.4. Responsabilidad para la protección de la información privada	56
9.4.5. Consentimiento de uso de la información privada	56

9.4.6. Divulgación de conformidad con procesos judiciales o administrativos	57
9.4.7. Otras casos para la divulgación de información.....	57
9.5. Derechos de propiedad intelectual.....	57
9.6. Obligaciones y Responsabilidad	57
9.6.1. Obligaciones de la CA	57
9.6.2. Obligaciones de la RA	57
9.6.3. Obligaciones del suscriptor	57
9.6.4. Obligaciones de los terceros que confían	57
9.6.5. Obligaciones de otras entidades.....	58
9.7. Renuncias de la garantía.....	58
9.8. Límites de responsabilidad	58
9.9. Indemnizaciones	59
9.10. Términos de uso y duración	59
9.10.1. Términos de uso.....	59
9.10.2. Duración	59
9.10.3. Supervivencia tras fin de la duración.....	59
9.11. Avisos y comunicaciones individuales a los participantes.....	59
9.12. Resolución de Conflictos	60
9.12.1. Procedimiento de conflictos	60
9.12.2. Mecanismo y período de notificación.....	60
9.12.3. Circunstancias por las que un OID puede ser modificado.....	60
9.13. Disposiciones para la resolución de disputas.....	60
9.14. Normativa aplicable.....	60
9.15. Cumplimiento de la normativa aplicable	61
9.16. Otras disposiciones	61
9.17. Otras provisiones	62

CONTROL DE DOCUMENTO

Título:	Política de Certificados de Viafirma TSU - Policy OID 1.3.6.1.4.1.34253.7.3		
Autor:	Viafirma Prestador de Servicios de Confianza		
Estado:	Aprobado		
Versión:	1.3		
Código:	QTSP-CP-TSU-VIAFIRMA	Fecha:	22-01-2021
Idioma:	Castellano	Revisión anterior:	12-01-2021
		Núm. Páginas:	62

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	Versión	Motivo del Cambio
12-11-2019	1.0	Primera versión.
16-06-2020	1.1	Revisión Capítulo 1.2 "Identificación del Documento". Revisión Capítulo 2.2 "Publicación de la Información". Revisión Capítulo 7.3 "Certificado OCSP".
12-01-2021	1.2	Eliminación de las referencias a la Ley 59/2003 (derogada por la Ley 6/2020). Ajustes en apartado 2.3.
22-01-2021	1.3	Nuevo capítulo 6.8.1 "Tipos de usos de los sellos de tiempo electrónico". Nuevo capítulo 6.8.1.1 "Formato de la Request" Nuevo capítulo 6.8.1.2 "Formato de la Response"

ACERCA DEL DOCUMENTO

Este documento, con nivel de seguridad público, es propiedad de **Viafirma, S.L.** Para más información contacte con:

Viafirma, S.L. (Viafirma)

Antonio Cabrera Jiménez (Consejero Delegado)

Glorieta Fernando Quiñones, s/n. Planta Baja, M8

Edificio CENTRIS | 41940 Tomares (Sevilla – España)

CIF B91052142 | Telf. : +34 954 15 52 44 | psc@viafirma.com

1. INTRODUCCIÓN

1.1. Resumen

Viafirma S.L. es una compañía española especializada en el desarrollo de sistemas de información de firma electrónica, con CIF B91052142, ubicada en España, en la ciudad de Tomares (Sevilla), Edificio CENTRIS, Glorieta Fernando Quiñones s/n, Planta Baja, Módulo 8 (código postal 41940).

El sellado de tiempo, o timestamping, es un protocolo online que permite probar que un conjunto de datos han existido, y no han sido modificados, desde un instante específico en el tiempo. Está descrito en RFC 3161.

Viafirma se constituye en Autoridad de Sellado de Tiempo: TSA - TimeStamp Authority. Este documento recoge la política del certificado TSU utilizado para la expedición de sellos electrónicos cualificados de tiempo, así como los aspectos más relevantes y procedimientos definidos para la gestión del servicio.

1.2. Identificación del Documento

Este documento está estructurado acorde al RFC3647, con el nombre Viafirma_QTSP_CP_TSU, codificado con el código VF-QTSP-CP-TSU, y disponible en su última versión en la siguiente URL de acceso público: <https://qtsp.viafirma.com/docs/QTSP-CP-TSU-VIAFIRMA.pdf>

Las presentes políticas de certificado están identificadas con el OID número **1.3.6.1.4.1.34253.7.3**.

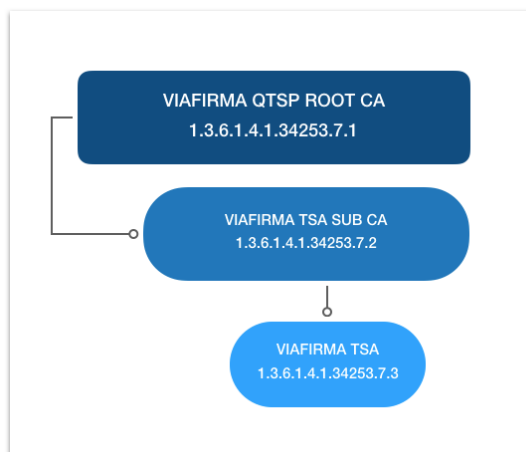
1.3. Participantes

Se consideran las siguientes partes intervinientes:

- **Viafirma**, Prestador de Servicios de Confianza, que emite el certificado de TSA y actúa como Autoridad de Sellado de Tiempo (Viafirma TSA) emitiendo sellos de tiempo o TST(s).
- **Suscriptor**: tercero (persona física o jurídica) que consume los servicios de sellado de tiempo proporcionados por Viafirma TSA, mediante un acuerdo comercial.
- **Terceras partes** que confían en los sellos de tiempo (TSTs) emitidos por Viafirma TSA.

1.3.1. Autoridad de Certificación

La TSA de Viafirma QTSP queda definida y regulada en la presente política de certificados por su Autoridad de Certificación raíz **VIAFIRMA QTSP ROOT CA**.



1.3.2. Autoridades de Registro

El servicio ofrecido por la TSA de Viafirma no contempla la gestión de Autoridades de Registros para la emisión de certificado de sellos de tiempo (TSU). La generación del único Certificado de TSU se realiza mediante procedimiento único y no delegado en Autoridades de Registro. No obstante, en cada una de las Políticas de Certificados disponibles se definirá y regularán las Autoridades de Registro autorizadas.

1.3.3. Suscriptores

Será considerado suscriptor de un certificado TSU emitido por Viafirma TSA el titular del certificado para el que es emitido, constatado en el DN y Common Name del mismo.

Será obligación de los suscriptores los siguientes términos y condiciones:

- Deben respetar y cumplir lo plasmado en el presente documento y en los documentos que regulan la relación comercial con Viafirma, incluyendo al menos el contrato de servicio y los términos y condiciones.
- Deben comprobar el estado de revocación del certificado utilizado para emitir el sello de tiempo.

- Deben disponer de sistemas de generación de sellos de tiempo adecuados a los estándares técnicos.
- Deben utilizar los sellos para los usos permitidos por la política.

1.3.4. Terceros que confían

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

- a) Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
- b) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confían, y aceptar sujetarse a las mismas.
- c) No aceptar certificados digitales para fines no contemplados en la presente Política de Certificación.

1.4. Uso del Certificado

1.4.1. Usos apropiados del certificado

El uso de un certificado de TSU para la firma de sellos de tiempo.

1.4.2. Usos prohibidos del certificado

No se podrá usar un certificado de TSU para autenticar o cifrar.

1.5. Administración de Políticas

1.5.1. Autoridad de políticas

La autoridad de políticas de Viafirma QTSP está compuesta por los roles de confianza incluidos en el comité de seguridad, definido en el procedimiento específico "PE-02 - Comité de Seguridad" de la compañía.

1.5.2. Contacto de la autoridad de políticas

Viafirma, S.L. (Viafirma)

Antonio Cabrera Jiménez (Consejero Delegado)
Glorieta Fernando Quiñones, s/n. Planta Baja, M8
Edificio CENTRIS | 41940 Tomares (Sevilla – España)
VATES B91052142 | Telf. : +34 954 15 52 44 | psc@viafirma.com

1.5.3. Persona que determina la idoneidad de las políticas

Los cambios y actualizaciones de las presentes Políticas de Certificado serán revisadas y aprobadas por la Autoridad de Políticas.

1.5.4. Procedimiento de aprobación de las políticas

Cualquier elemento de esta política es susceptible de ser modificada. Todos los cambios autorizados serán inmediatamente publicados en la web pública junto al histórico de versiones anteriores. Los terceros que confían afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la autoridad de políticas.

La probación de políticas o cualquier cambios que afecten a éstas serán debidamente notificadas tal y como se recoge en el capítulo 2.3 de las presentes políticas.

1.6. Definiciones y Acrónimos

- **TSA:** TimeStamp Authority, Autoridad de Sellado de Tiempo.
- **TSU:** TimeStamping Unit, Unidad de Sellado de Tiempo.
- **PSC:** Prestador de Servicios de Confianza.
- **TSP:** Trust Services Provider, correspondencia en inglés a PSC.
- **QTSP:** Qualified Trust Services Provider (PSC cualificado).
- **HSM:** Hardware Security Module, módulo de seguridad hardware.
- **NTP:** Network Time Protocol.
- **ROA:** Real Instituto y Observatorio de la Armada.

-
- **OID:** Object identifier, identificador de objeto único.
 - **PKI:** Public Key Infrastructure, infraestructura de clave pública.
 - **UTC:** Coordinated Universal Time.
 - **TSP:** TimeStamping Protocol, protocolo de sellado de tiempo.
 - **TST:** TimeStamping Token, token de sellado de tiempo.
 - **eIDAS :** electronic IDentification, Authentication and trust Services (Reglamento UE 910/2014).
 - **SGSI:** Sistema de Gestión de la Seguridad de la Información.

2. PUBLICACIÓN Y REPOSITORIO DE CERTIFICADOS

2.1. Repositorios

Viafirma QTSP publicará las claves públicas de toda su cadena de confianza en el sitio web <https://qtsp.viafirma.com>. Y de forma explícita en las siguientes direcciones:

<http://qtsp.viafirma.com/tsp/rootca.crt>

<http://qtsp.viafirma.com/tsp/subca.crt>

Y de forma específica para esta Política de Certificado, la clave pública del Certificado de TSU de Viafirma QTSP en la siguiente dirección:

https://qtsp.viafirma.com/docs/viafirma_tsu_publickey.cer

Las fuentes de verificación de certificados revocados para esta política serán las siguientes:

http://qtsp.viafirma.com/tsp/tsa_subca.crl

http://qtsp1.viafirma.com/tsp/tsa_subca.crl

<http://qtsp.viafirma.com/ocsp>

2.2. Publicación de la información de certificación

La presente política de certificado estará publicada en el sitio web <https://qtsp.viafirma.com>. Y de forma explícita en la siguiente dirección:

<https://qtsp.viafirma.com/docs/QTSP-CP-TSU-VIAFIRMA.pdf>

2.3. Frecuencia de publicación

Cualquier versión que actualice la presente política de certificados será publicada en el sitio web <https://qtsp.viafirma.com> manteniendo el histórico de versiones anteriores. El intervalo máximo establecido por la revisión de las presentes políticas es de seis meses a contar desde la fecha de su última publicación.

Al mismo tiempo, cuando sea necesario por implicar cambios en los servicios prestados, los cambios en la presente política de certificado serán notificados acorde al procedimiento establecido por el correspondiente órgano regulador, a través de la Sede Electrónica de la Secretaría de Estado para el Avance Digital, y su procedimiento definido para las Notificaciones de los art. 19.2, 21.1 y 24.2 del Reglamento (UE) N° 910/ 2014 relativo a la identificación electrónica y los servicios de confianza y comunicaciones del artículo 30.2 de la Ley 59/2003 de firma electrónica, o las actualizaciones que el regulador realice en base a la Ley 6/2020, de 11 de noviembre, que deroga a la anterior.

En cuanto a la frecuencia de publicación de las CRLs de la presente Política de Certificados será de 12 horas.

Al mismo tiempo, se expone un servicio de validación online, basado en el protocolo OCSP (RFC6960), que ofrece el estado en tiempo real.

2.4. Control de acceso a los repositorios

El acceso a la información será gratuito y estará a disposición de los Firmantes/Suscriptores y terceros que confían. El acceso se hará mediante protocolo HTTP, tanto para el acceso a las CRLs como al servicio OCSP.

3. IDENTIFICACION Y AUTENTICACIÓN

3.1. Uso de nombres

3.1.1. Tipo de Nombres

Todos los suscriptores de certificados requieren un nombre distintivo (distinguished name) conforme con el estándar X.509.

El distinguished name se incluye en el campo Common Name (CN) y se corresponde con el nombre de la Unidad de la Autoridad de Sello de tiempo autorizada por Viafirma QTSP, por ejemplo, VIAFIRMA TSA. No tendrá que coincidir con un identificador único tipo CIF o similar.

3.1.2. Significado de los nombres

El nombre utilizado para identificar al certificado tendrá que ser semántico.

3.1.3. Seudónimos

Viafirma QTSP no permite el uso de seudónimos en los certificados que emite.

3.1.4. Reglas para interpretar varios formatos de nombre

El nombre elegido para identificar a la TSA, y a que aparecerá en el Common Name del certificado de TSU, tendrá que ser semántico y estar asociado a la Organización a la que representa. En el contexto de la presente política de certificado el nombre utilizado para la identificación de la TSA será "VIAFIRMA TSA".

3.1.5. Unicidad de nombres

En el propósito y alcance de la presente política no contempla emisiones masivas de certificados de TSU, por lo que el cumplimiento de unicidades de nombre no implicará mayores esfuerzos durante la fase de revisión previa a la emisión. Al mismo tiempo, la configuración del perfil de certificado incluye entre sus reglas la prohibición de emitir dos certificados con el mismo DN.

3.1.6. Reconocimiento, autenticación y función de las marcas registradas

Todas las marcas, nombres comerciales o signos distintivos de cualquier clase que aparecen en las páginas de Viafirma QTSP, y en especial los escritos doctrinales o publicaciones de la misma son propiedad de Viafirma o, en su caso, de terceros que han autorizado su uso, sin que pueda entenderse que el uso o acceso a dichos Contenidos atribuya al Usuario derecho alguno sobre las citadas marcas, nombres comerciales y/o signos distintivos, y sin que puedan entenderse cedidos al Usuario, ninguno de los derechos de explotación que existen o puedan existir sobre dichos Contenidos.

La utilización no autorizada de dichos contenidos, así como la lesión de los derechos de Propiedad Intelectual o Industrial de Viafirma o de terceros incluidos en la Página que hayan cedido contenidos dará lugar a las responsabilidades legalmente establecidas.

La marca VIAFIRMA cuenta con los correspondientes registros europeos y españoles con los siguientes números de depósito:

EUIPO - European Union Intellectual Property Office

EUTM File Info [011204617](#)

<https://euipo.europa.eu/eSearch/#details/trademarks/011204617>

OEPM – Oficina Española de Patentes y Marcas:

Exp **M4026263**

<http://consultas2.oepm.es/ceo/jsp/busqueda/consultaExterna.xhtml?numExp=M4026263>

3.2. Validación de identidad inicial

3.2.1. Métodos de prueba de la posesión de la clave privada

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.2. Autenticación de la identidad de una organización

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.3. Autenticación de la identidad de un individuo

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.4. Información no verificada del suscriptor

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.5. Validación de la autoridad

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.2.6. Criterios de interoperabilidad

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.3. Identificación y autenticación para la renovación de certificados

3.3.1. Identificación y autenticación para la renovación de certificado vigente

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.3.2. Identificación y autenticación para la renovación un certificado caducado

No se contempla este procedimiento en la presente política. La emisión de un certificado de TSU se realizará mediante procedimientos internos.

3.4. Identificación y autenticación para solicitudes de revocación

El certificado de TSU regulado en la presente política es emitido a nombre de VIAFIRMA, por lo que no se contemplan solicitudes externas para la revocación del mismo. Se cuenta por tanto con un procedimiento interno, que prevé los distintos casos autorizados para poder revocar el certificado, y que serán llevados a cabo por miembros y roles de confianza de Viafirma QTSP.

4. CICLO DE VIDA DEL CERTIFICADO Y REQUISITOS OPERACIONALES

4.1. Solicitud de Certificados

Viafirma QTSP no contempla la solicitud externa de certificados de TSU. La solicitud, emisión y gestión del mismo está destinada a uso interno acorde a los procedimientos internos de gestión del servicio cualificado de sello de tiempo.

4.1.1. Quién puede solicitar un certificado

No aplica.

4.1.2. Proceso de registro

No aplica.

4.2. Proceso de solicitud de un certificado

Viafirma QTSP no contempla la solicitud externa de certificados de TSU. La solicitud, emisión y gestión del mismo está destinada a uso interno acorde a los procedimientos internos de gestión del servicio cualificado de sello de tiempo.

4.2.1. Funciones de identificación y autenticación

No aplica.

4.2.2. Aprobación o rechazo de solicitudes

No aplica.

4.2.3. Plazos del proceso de solicitud

No aplica.

4.3. Emisión de certificados

4.3.1. Acciones de la CA durante la emisión de certificados

Viafirma QTSP se reserva las acciones necesarias derivadas de los eventos generados durante cualquier fase del ciclo de vida de una emisión de certificado.

4.3.2. Notificaciones a suscriptores por parte de la CA durante la emisión de certificados

A partir de los datos facilitados y autorizados a Viafirma QTSP, el suscriptor podrá ser notificado a lo largo del ciclo de vida del proceso de emisión del certificado.

4.4. Aceptación del certificado

4.4.1. Hechos que constituyen la aceptación del certificado

La emisión del certificado de TSU regulado en la presente política se entenderá por aceptado tras la formalización de la ceremonia de creación de claves del certificado de TSA, en presencia de distintos roles de confianza autorizados por la Autoridad de Políticas.

4.4.2. Publicación del certificado por parte de la CA

La clave pública del certificado de TSU emitido por Viafirma QTSP quedará publicada en el sitio web <https://qtsp.viafirma.com>, y en concreto en la siguiente dirección:

https://qtsp.viafirma.com/docs/viafirma_tsu_publickey.cer

4.4.3. Notificación de la emisión a otras entidades

Viafirma QTSP no establece entre sus procedimientos la notificación a otras entidades de la emisión de un nuevo certificado.

4.5. Uso del certificado

4.5.1. Uso de clave privada del suscriptor

La clave privada de los certificados emitidos por Viafirma QTSP podrá ser usada acorde al alcance y limitaciones para el que fueron emitidos, tal y como se recoge en los términos y uso del servicio de sello de tiempo.

El suscriptor deberá proteger el uso de la clave privada ante usos no autorizados, y deberá dejar de hacer uso de clave privada cuando ésta haya expirado o haya sido revocada.

4.5.2. Confianza y uso de la clave pública

Será obligación de los terceros que confían en las claves públicas de Viafirma QTSP cumplir con lo dispuesto en la normativa. También será obligación de éstos la verificación de la validez de los certificados en el momento de realizar cualquier operación basada en el uso de los mismos. De igual forma deberán conocer y sujetarse a las garantías, límites y responsabilidades aplicables en cada caso.

4.6. Renovación de certificados

4.6.1. Situaciones para la renovación de certificados

Al tratarse de un certificado de TSU, no sujeto al público en general, la renovación del certificado de TSU podrá iniciarse según lo previsto en los procedimientos internos de Viafirma QTSP para la gestión de los servicios de confianza.

4.6.2. Quién puede solicitar la renovación

No se contempla la solicitud externa de certificados de TSU de Viafirma QTSP.

4.6.3. Proceso de solicitudes de renovación

No se contempla la solicitud externa de certificados de TSU de Viafirma QTSP.

4.6.4. Notificación de la renovación del certificado al suscriptor

No se contempla la solicitud externa de certificados de TSU de Viafirma QTSP.

4.6.5. Hechos que constituyen la aceptación del certificado renovado

No se contempla la solicitud externa de certificados de TSU de Viafirma QTSP.

4.6.6. Publicación del certificado renovado

La clave pública del certificado de TSU renovado por Viafirma QTSP quedará publicada en el sitio web <https://qtsp.viafirma.com>, y en concreto en la siguiente dirección:

https://qtsp.viafirma.com/docs/viafirma_tsu_publickey.cer

Del mismo modo se mantendrá un histórico de las claves públicas caducadas.

4.6.7. Notificación de la renovación a otras entidades

Viafirma QTSP no establece entre sus procedimientos la notificación a otras entidades de la renovación de un certificado.

4.7. Reemisión del Certificado

4.7.1. Circunstancias para la reemisión del certificado

Viafirma QTSP no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.2. Quién puede solicitar la reemisión del certificado

Viafirma QTSP no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.3. Procedimiento para las solicitudes de reemisión del certificado

Viafirma QTSP no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.4. Notificación al suscriptor del nuevo certificado reemitido

Viafirma QTSP no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.5. Hechos que constituyen la aceptación del certificado reemitido

Viafirma QTSP no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.6. Publicación por parte de la CA del certificado reemitido

Viafirma QTSP no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.7.7. Publicación por parte de la CA del certificado reemitido a otras entidades

Viafirma QTSP no permite la reemisión entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8. Modificación del certificado

4.8.1. Circunstancias para la modificación del certificado

Viafirma QTSP no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.2. Quién puede solicitar la modificación del certificado

Viafirma QTSP no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.3. Proceso de solicitud de modificación del certificado

Viafirma QTSP no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.4. Notificación de la modificación del certificado

Viafirma QTSP no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.5. Hechos que constituyen la aceptación del certificado modificado

Viafirma QTSP no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.6. Publicación por parte de la CA de la modificación del certificado

Viafirma QTSP no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.8.7. Notificación de la modificación del certificado por parte de la CA a otras entidades

Viafirma QTSP no permite la modificación de los datos de un certificado ya emitido entre los procedimientos previstos en el ciclo de vida de sus certificados.

4.9. Revocación y suspensión de certificados

4.9.1. Situaciones para la revocación

Viafirma QTSP activará los procedimientos establecidos para la revocación de su certificado de TSU en caso de compromiso de claves, cambios significativos en los datos contenidos en el certificado, por ejemplo cambio de razón social o CIF, o bien, o ante un compromiso de algunos de los algoritmos utilizados para su generación.

4.9.2. Quién puede solicitar la revocación

No se contemplan solicitudes externas a Viafirma QTSP.

4.9.3. Proceso para la revocación del certificado

La renovación del certificado de TSU podrá iniciarse según lo previsto en los procedimientos internos de Viafirma QTSP para la gestión de los servicios de confianza.

4.9.4. Período de gracia de la solicitud de revocación

Viafirma QTSP no contempla período de gracia durante el proceso de revocación. Una vez completado el proceso de revocación tendrá efecto inmediato.

4.9.5. Período en el que la CA debe procesar la solicitud de revocación

Al tratarse de un procedimiento interno de Viafirma QTSP, no sujeto a solicitudes externas, el proceso de revocación tendrá efecto inmediato.

4.9.6. Requisitos de verificación de la revocación por las partes que confían

Las distintas fuentes de verificación de certificados publicadas por Viafirma QTSP podrán ser consultadas gratuitamente por los terceros que confían, siendo éstos responsables de verificar la autenticidad de la fuente.

4.9.7. Frecuencia de emisión de la CRL

Las CRLs sujetas a la presente política cuentan con una frecuencia de emisión y publicación de 12 horas.

4.9.8. Latencia máxima de la CRL

Las CRLs sujetas a la presente política cuentan con una carencia máxima de 4 días.

4.9.9. Comprobación online del estado de la revocación

Viafirma QTSP publica un servicio de validación online de sus certificados a través del protocolo OCSP y disponible en <http://qtsp.viafirma.com/ocsp>.

4.9.10. Requisitos para la comprobación online del estado de revocación

Viafirma QTSP no define requisitos particulares para el uso de este servicio más allá de las recomendaciones citadas en la RFC6960 .

4.9.11. Otras formas de comprobación del estado de revocación

Además del servicio OCSP los certificados emitidos por Viafirma QTSP podrán ser verificados a través de las distintas CRLs publicadas e informadas en sus respectivos certificados.

4.9.12. Requisitos especiales para la reemisión de certificados por compromiso de claves

Viafirma QTSP no permite entre sus procedimientos la reemisión de certificados. En caso de compromiso de claves éstos deberán ser revocados, y el suscriptor tendrá que completar un proceso de nueva emisión.

4.9.13. Circunstancias para la suspensión

Viafirma QTSP no permite entre sus procedimientos la suspensión de certificados.

4.9.14. Quién puede solicitar la suspensión

Viafirma QTSP no permite entre sus procedimientos la suspensión de certificados.

4.9.15. Procedimiento para la solicitud de suspensión

Viafirma QTSP no permite entre sus procedimientos la suspensión de certificados.

4.9.16. Límites del período de suspensión

Viafirma QTSP no permite entre sus procedimientos la suspensión de certificados.

4.10. Servicios para el estado del certificado

4.10.1. Características operacionales

Viafirma QTSP no ofrece servicios adicionales para la comprobación del estado del certificado distintos a la comprobación de la CRL y/o OCSP descritos en capítulos anteriores.

4.10.2. Servicios disponibles

Viafirma QTSP no ofrece servicios adicionales para la comprobación del estado del certificado distintos a la comprobación de la CRL y/o OCSP descritos en capítulos anteriores.

4.10.3. Características opcionales

Viafirma QTSP no ofrece servicios adicionales para la comprobación del estado del certificado distintos a la comprobación de la CRL y/o OCSP descritos en capítulos anteriores.

4.11. Fin de la suscripción

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

4.12. Depósito de claves y recuperación

4.12.1. Prácticas para el depósito y recuperación de claves

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

4.12.2. Prácticas de encapsulado y recuperación de recuperación de claves

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5. INSTALACIÓN, GESTIÓN Y CONTROLES OPERACIONALES

5.1. Controles físicos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.1.1. Localización y construcción

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.1.2. Acceso físico

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.1.3. Alimentación eléctrica y aire acondicionado

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.1.4. Exposición al agua

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.1.5. Protección y prevención de incendios

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.1.6. Sistema de almacenamiento

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.1.7. Eliminación de residuos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.1.8. Backup remoto

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.2. Controles procedimentales

5.2.1. Roles de confianza

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP, y de forma específica para la gestión del Servicio Cualificado de Sello de Tiempo ofrecido por Viafirma TSA, se cuentan con los siguientes roles de confianza:

Se dispone de un número de personal suficiente con conocimiento experto en la gestión de Certificados Digitales, Sellos de Tiempo y toda la gestión relacionada con el ciclo de vida de los servicios asociados por una Autoridad de Certificación y Autoridad de Sellado de Tiempo.

Para ello se definen una serie de roles y responsabilidades encajadas en el organigrama organizacional de la compañía e identificados en el equipo designado para la gestión de la Seguridad de la TSA de Viafirma. En algún caso, se amplían las responsabilidades de roles existentes en el apartado anterior, y en otro, se crean nuevos roles. Los roles no implican unívocamente cargos: una persona puede ostentar más de un rol, si bien se han tenido en cuenta las incompatibilidades y restricciones recogidas en las buenas prácticas y estándares como RFC3647.

La norma especifica cuatro nuevos roles:

- Security Officer
- System Administrator
- System Operator
- System Auditor

5.2.2. Número de personas requeridas por tarea

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.2.3. Identificación y autenticación para cada rol

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.2.4. Roles que requieren separación de funciones

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.3. Controles personales

5.3.1. Requisitos de calificación, experiencia y autorización

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.3.2. Procedimientos de verificación de antecedentes

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.3.3. Requisitos de formación

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.3.4. Requisitos y frecuencia de formación

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.3.5. Frecuencia y secuencia de rotación de tareas

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.3.6. Sanciones por acciones no autorizadas

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.3.7. Requisitos para personal independiente

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.3.8. Documentación entregada al personal

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.4. Procedimientos para el registro de auditoría

5.4.1. Tipo de eventos registrados

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.4.2. Frecuencia del procesamiento de registros

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.4.3. Período de retención del registro de auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.4.4. Protección del registro de auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.4.5. Procedimiento del backup del registro de auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.4.6. Sistema de recolección de auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.4.7. Notificación de eventos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.4.8. Evaluación de vulnerabilidades

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.5. Archivo de registros

5.5.1. Tipos de archivo de registros

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.5.2. Período de retención del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.5.3. Protección del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.5.4. Procedimientos para el backup del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.5.5. Requisitos para el sellado de tiempo del registro

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.5.6. Sistema de recolección del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.5.7. Procedimientos para obtener y verificar la información del archivo

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.6. Cambio clave

No se contempla el cambio de claves para la presente política de certificados.

5.7. Recuperación en caso de compromiso de la clave o desastre

5.7.1. Procedimientos para la gestión de incidentes

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.7.2. Obsolescencia y deterioro

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.7.3. Procedimientos ante compromiso de clave de una entidad

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.7.4. Plan de continuidad de negocio ante desastres

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

5.8. Cese de la CA o RA

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. Generación del par de claves y su instalación

6.1.1. Generación del par de claves

La generación del par de claves de un certificado de TSU, acorde a las presentes políticas, es llevada a cabo bajo un procedimiento denominado “Ceremonia de Claves”, incluido entre los procedimientos internos de Viafirma QTSP.

6.1.2. Entrega de la clave privada al suscriptor

La clave privada del certificado de TSU es generada y almacenada en un módulo criptográfico (HSM) FIPS 140-2 Level 3 EAL4+ gestionado por Viafirma QTSP que actúa en este escenario como suscriptor.

6.1.3. Entrega de la clave pública al suscriptor

La clave pública del certificado de TSU emitido será publicada en el sitio web de Viafirma QTSP tal y como se define en el capítulo 2.2 de la presente política de certificados.

6.1.4. Entrega de la clave pública de la CA a los terceros que confían

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.1.5. Tamaño de las claves

Con carácter general, el tamaño de las claves generadas por Viafirma QTSP serán de 2048 para los certificados finales, y de 4096 para los certificados de entidades intermedias y raíz de su jerarquía. En el caso del certificado de TSU regulado en la presente política de certificados, el tamaño será de 2048.

6.1.6. Control de calidad de los parámetros de generación de la clave pública

Los parámetros utilizados para la generación del certificado de TSU regulado en la presente política serán definidos como parte del procedimiento de ceremonia de claves y aprobados por Viafirma QTSP.

6.1.7. Propósito de uso de la clave

Las directrices para el uso de clave en los certificados de las entidades intermedias y raíz de su jerarquía serán Key Cert Sign y CRL Sign. Para el caso de los certificados finales, como el certificado de TSU sujeto a la presente política, será Digital Signature y Non-Repudiation, además de la extensión "Time Stamping" (1.3.6.1.5.5.7.3.8).

6.2. Protección de clave privada y controles del módulo criptográfico

6.2.1. Controles y estándares del módulo criptográfico

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.2. Control dual n de m para el uso de la clave privada

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.3. Depósito de la clave privada

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.4. Backup de la clave privada

El backup de la clave privada del certificado de TSU coincide con lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.5. Archivo de la clave privada

El archivo de la clave privada del certificado de TSU coincide con lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.6. Importación de la clave privada al módulo criptográfico

La importación de la clave privada del certificado de TSU coincide con lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

El almacenamiento de la clave privada del certificado de TSU coincide con lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.8. Método de activación de la clave privada

La activación de la clave privada del certificado de TSU coincide con lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.9. Método de desactivación de la clave privada

No se contemplan procedimientos de desactivación de claves.

6.2.10. Método de destrucción de la clave privada

El backup de las clave privada del certificado de TSU coincide con lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.2.11. Clasificación del módulo criptográfico

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.3. Otros aspectos sobre la gestión de par de claves

6.3.1. Archivo de la clave pública

No se contempla procedimiento para la publicación de claves públicas de la raíz, sus subordinadas o del certificado de TSU cuando éstas han caducado. No obstante esta información está disponible en el sistema que gestiona la PKI a partir del histórico de claves públicas registradas por el sistema, incluyendo claves que hayan sido renovadas o revocadas.

6.3.2. Periodos operativos de certificado y periodos de uso del par de claves

La validez de la clave pública del certificado de TSU será de 5 años, mientras que el valor operativo de su clave privada será de 3 años.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los procedimientos de generación de datos para la activación de la clave privada del certificado de TSU se lleva a cabo acorde a los procedimientos definidos en sus respectivas ceremonias de clave y conforme con las normas ETSI EN 319 421.

Parte de estos datos de activación son generados individualmente por los distintos roles de confianza que participan en las ceremonias de creación y activación de claves.

6.4.2. Protección de los datos de activación

Los roles de confianza involucrados en la generación de datos para la activación de claves siguen un procedimiento interno de Viafirma QTSP por el que se registra y audita el proceso de creación, almacenamiento y uso de los soportes que contienen los datos utilizados para la activación de claves.

Además, se cuenta con un depósito por duplicado, a cargo de más de un rol de confianza por si fuese necesaria su uso en caso de fuerza mayor o indisponibilidad del custodio principal del dato.

6.4.3. Otros aspectos de los datos de activación

No se han definido otros aspectos relevantes para este punto.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos de los controles de seguridad

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.5.2. Clasificación de la seguridad

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.6. Ciclo de vida de los controles técnicos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.7. Controles de seguridad de red

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

6.8. Sello de tiempo

Viafirma QTSP presta el servicio cualificado de sello de tiempo a través de su TSA y sus correspondientes certificados TSU emitidos bajo la presente política de certificado.

El servicio de sellado de tiempo se emite acorde a lo establecido en la norma ETSI EN 319 421 Anexo B, incorporando entre sus mecanismos de seguridad el control de desfase horario para asegurar que la desviación no supere los umbrales establecidos en la correspondiente políticas de sello de tiempo.

La validación de los sellos de tiempo firmados por certificados de la presente política pueden ser validados en las siguientes fuentes de validación:

- **CRL:** https://qtsp.viafirma.com/tsp/tsa_subca.crl
- **CRL:** https://qtsp1.viafirma.com/tsp/tsa_subca.crl
- **OCSP:** <https://qtsp.viafirma.com/ocsp/>

También se cuenta con mecanismos de seguridad para el control y monitorización del consumo del servicio a través de credenciales seguras y bajo controles para evitar ataques de fuerza bruta.

La política de emisión del sellos cualificado de tiempo emitido por Viafirma QTSP queda identificada en el OID 0.4.0.2023.1.1 del sello.

La emisión de los sellos de tiempo cuenta con un desfase inferior a un segundo contemplado en ETSI EN 319 421. Para ello se utilizan fuentes de tiempo *stratum 1*, concretamente UTC(ROA), mediante protocolo NTP.

Todas las características técnicas del sellado de tiempo quedan definidas y publicadas en los **Términos y Condiciones TSA Viafirma** disponible en el sitio <https://qtsp.viafirma.com> y en concreto en la siguiente dirección: <https://qtsp.viafirma.com/docs/TERMS-QTSA-VIAFIRMA.pdf>.

6.8.1. Tipos y usos de los sellos de tiempo electrónico

El servicio cualificado de Sellado de Tiempo es ofrecido por Viafirma como Prestador de Servicios de Confianza y de conformidad con el Reglamento eIDAS y de acuerdo a las especificaciones recogidas en los siguientes estándares y normas:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers.
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- RFC-3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).
- El sello de tiempo tendrá presente el OID de política de firma 0.4.0.2023.1.1.

El servicio de sellado de tiempo es un servicio comercial que requiere la suscripción de un acuerdo con Viafirma. Los suscriptores deberán:

- Cumplir lo especificado en la declaración de prácticas y políticas del servicio y los términos y condiciones contractuales.
- Verificar el sello de tiempo.
- Validar el certificado de la TSA.
- Verificar que no se ha alterado el hash enviado al servicio de sello de tiempo.

Para validar los certificados de sello de tiempo se dispone de CRLs y OCSP, disponibles en:

CRLs:

- https://qtsp.viafirma.com/tsp/tsa_subca.crl
- https://qtsp1.viafirma.com/tsp/tsa_subca.crl

OCSP:

- <https://qtsp.viafirma.com/ocsp/>

6.8.1.1. Formato de la Request

Los sellos de tiempo emitidos por Viafirma TSA siguen el estándar RFC 3161 y están conformes con la especificación ETSI EN 319 422, y tendrán el siguiente formato en la llamada (request):

```
TimeStampReq ::= SEQUENCE {  
    version INTEGER {v1(1)},  
    messageImprint MessageImprint,  
    reqPolicy TSAPolicyId OPTIONAL,  
    nonce INTEGER OPTIONAL,  
    certReq BOOLEAN DEFAULT FALSE,  
    extensions [0] IMPLICIT Extensions OPTIONAL}
```

Donde messageImprint sigue la siguiente estructura:

```
MessageImprint ::= SEQUENCE {  
    hashAlgorithm AlgorithmIdentifier,  
    hashedMessage OCTET STRING}
```

Y reqPolicy se define de la siguiente forma:

```
TSAPolicyId ::= OBJECT IDENTIFIER
```

De acuerdo al apartado 5 de ETSI EN 319 422, los campos opcionales reqPolicy, nonce y certReq deben ser soportados. Se aceptan algoritmos SHA1, SHA256, SHA384 y SHA512 de acuerdo a las recomendaciones de la Guía de Seguridad de las TIC CCN-STIC 807.

6.8.1.2. Formato de la Response

El formato de la response generada por Viafirma TSA cumple el estándar RFC3161:

```
TimeStampResp ::= SEQUENCE {  
    status PKIStatusInfo,  
    timeStampToken TimeStampToken OPTIONAL}
```

Destacando el desglose de TimeStampToken:

```
TSTInfo ::= SEQUENCE {  
    version INTEGER {v1(1)},  
    policy TSAPolicyId,  
    messageImprint MessageImprint,  
    timeStampReq serialNumber INTEGER,  
    genTime GeneralizedTime,  
    accuracy Accuracy OPTIONAL,  
    ordering BOOLEAN DEFAULT FALSE,  
    nonce INTEGER OPTIONAL,  
    tsa [0] GeneralName OPTIONAL,  
    extensions [1] IMPLICIT Extensions OPTIONAL}
```

GeneralizedTime sigue la estructura *YYYYMMDDhhmmss[.s...]Z*. Mientras tanto, *Accuracy* refleja la desviación respecto a UTC de la fecha/hora recogida en *genTime*:

```
Accuracy ::= SEQUENCE {  
    seconds INTEGER OPTIONAL,  
    millis [0] INTEGER (1..999) OPTIONAL,  
    micros [1] INTEGER (1..999) OPTIONAL}
```

La respuesta sigue las restricciones específicas recogidas en el apartado 5 de ETSI EN 319 422, que indica que:

- El campo *policy* debe estar presente.
- El campo *genTime* debe tener la precisión exigida.
- El campo *accuracy* debe estar presente, con un valor inferior a 1 segundo, en concreto 0.8 segundos.
- El campo *ordering* no debe estar presente o estar a *false*.
- Ningún campo *extension* debe estar marcado como crítico.

7. CERTIFICADOS, CRL, OCSP Y PERFILES

7.1. Perfil de certificado

7.1.1. Número de versión

Perfil asociado a la versión 3 del estándar X.509.

7.1.2. Extensiones del certificado

El perfil asociado al certificado de TSU regulado en la presente política cuenta con las siguientes extensiones:

Subject Name

<i>Country</i>	<ES>
<i>Organization</i>	<ORGANIZATION NAME>
<i>Organizational Unit</i>	<OU NAME>
<i>Common Name</i>	<TSA NAME>
<i>Other Name</i>	<VATES>

Issuer Name

<i>Country</i>	ES
<i>Organization</i>	VIAFIRMA SOCIEDAD LIMITADA
<i>Organizational Unit</i>	VIAFIRMA QTSP
<i>Serial Number</i>	VATES-B91052142
<i>Common Name</i>	VIAFIRMA TSA SUB CA

<i>Serial Number</i>	<SERIALNUMBER>
<i>Version</i>	3
<i>Signature Algorithm</i>	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
<i>Parameters</i>	none

<i>Not Valid Before</i>	<BEGIN>
<i>Not Valid After</i>	<until 5 YEARS>

Public Key Info

<i>Algorithm</i>	RSA Encryption (1.2.840.113549.1.1.1)
<i>Parameters</i>	none

Public Key 256 bytes : <PUBLICKEY>

Exponent <3>
Key Size 2048 bits
Key Usage Verify

Signature 512 bytes : <publickeysignature>

Extension Key Usage (2.5.29.15)
Critical YES
Usage Digital Signature, Non-Repudiation

Extension Basic Constraints (2.5.29.19)
Critical YES
Certificate Authority NO

Extension Extended Key Usage (2.5.29.37)
Critical YES
Purpose #1 Time Stamping (1.3.6.1.5.5.7.3.8)

Extension Subject Key Identifier (2.5.29.14)
Critical NO
Key ID 4A 55 48 CA 14 B0 D4 A4 39 84 6F D3 AA 6B C6 45 B1 ED 1F C0

Extension Authority Key Identifier (2.5.29.35)
Critical NO
Key ID 4A C8 02 04 18 43 C2 BD 7F 03 90 B8 8F F7 13 C8 DC BE BE 26

Extension Certificate Policies (2.5.29.32)
Critical NO
Policy ID #1 (1.3.6.1.4.1.34253.7.3)
Qualifier ID #1 Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI <http://qtsp.viafirma.com/cps>

Extension CRL Distribution Points (2.5.29.31)
Critical NO
URI http://qtsp.viafirma.com/tsp/tsa_subca.crl

URI *http://qtsp1.viafirma.com/tsp/tsa_subca.crl*

Extension *Private Key Usage Period (2.5.29.16)*

Critical *NO*

Not Valid Before *<BEGIN>*

Not Valid After *<UNTIL 3 YEARS>*

Extension *Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)*

Critical *NO*

Method #1 *CA Issuers (1.3.6.1.5.5.7.48.2)*

URI *http://qtsp.viafirma.com/tsp/subca.crt*

Method #2 *Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)*

URI *http://qtsp.viafirma.com/ocsp*

Fingerprints

SHA-256 *<digest>*

SHA-1 *<digest>*

7.1.3. Identificador (OID) del algoritmo de firma

SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

7.1.4. Uso de nombres

Lo establecido en el capítulo 3.1.

7.1.5. Restricciones de nombres

No se permiten DN duplicados.

7.1.6. Identificador de política de certificado

La política de certificado recogida en el OID 2.5.29.32 "Certificate Policies" llevará informado para la presente política el valor 1.3.6.1.4.1.34253.7.3.

7.1.7. Uso de la extensión de política de restricciones

No se hacen uso de Políticas Constraints.

7.1.8. Sintaxis y semántica de la política de calificadores

No se contempla.

7.1.9. Semántica del procedimiento para las extensiones críticas del certificado

Lo establecido en la correspondiente Política de Certificado.

7.2. Perfil de la CRL

7.2.1. Número de versión

Número secuencial de cada CRL emitida y publicada por Viafirma QTSP, y debidamente informada en el OID 2.5.29.20 "CRL Number" de la estructura de la CRL.

7.2.2. CRL y extensiones

Extensiones disponibles acorde al estándar X.509 CRL Number (2.5.29.20) y Authority Key Identifier (2.5.29.32).

7.3. Certificado OCSP

Se cuenta con dos servicios OCSP, uno para validar el certificado de la TSU emitido por la SUBCA y otro servicio OCSP para validar el certificado de la SUBCA. Ambos servicios OCSP están firmado por los siguientes Certificados.

7.3.1. Certificado utilizado para firma el OCSP que valida el certificado de TSA SUB CA

VIAFIRMA TSA SUB CA

Subject Name

Country ES
Organization VIAFIRMA SOCIEDAD LIMITADA
Organizational Unit VIAFIRMA QTSP
Serial Number VATES-B91052142
Common Name VIAFIRMA TSA SUB CA

Issuer Name

Country ES
Organization VIAFIRMA SOCIEDAD LIMITADA
Organizational Unit VIAFIRMA QTSP
Serial Number VATES-B91052142
Common Name VIAFIRMA QTSP ROOT CA

Serial Number 42 D7 40 76 6F AB 99 18 26 D4 9B 0B 3A 23 84 3C 2B 02 69 92

Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

Parameters none

Not Valid Before Thursday, 17 October 2019 at 14:25:49 Central European Summer Time

Not Valid After Monday, 17 October 2039 at 14:25:49 Central European Summer Time

Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1.1)

Parameters none

Public Key 512 bytes : CD 52 FF 1F 3B E5 3D 39

BE DC 2A E8 2B C7 17 81 AF 00 57 49 A1 91 77 C5 9A C4 00 95 BD B8 4E 7B D5 97 70 B6 5F 6F F7
62 66 A5 1E 1B 18 7F 4A 5D 7B D2 76 95 83 CC ED 67 BD 51 40 47 9C 1F 7E 8E 81 8B 22 62 FB EC
FF EF 92 BC D9 AF 7C 8D 8A 83 25 36 29 18 FB 1C 44 F1 90 AD 74 EB C1 30 92 EF 5C 0D 37 8A 56
A7 FD CF 65 81 35 BD DE 95 E7 06 D0 61 3B E6 19 D5 48 2A 6A D5 A5 F6 F7 63 BA 5A 4E 6E AF 33

85 CA 98 71 42 56 C0 CE 45 25 28 A3 4E 8E E0 90 77 E7 CC 45 E2 CD 53 E4 7E 5E DF 07 79 C4 26
 39 EF 7A DE 78 21 54 84 5A FB 4C 03 60 DB C1 A7 BC BC 09 CC CD 5C 83 90 37 42 A1 70 EE 27 F6
 7B 13 4E 5A 6C DE 9F DF F1 0E 3B 61 1B 99 77 CC 70 A9 70 2F 16 B0 A0 20 26 56 DD 68 38 8C 69
 E2 26 D8 DE AF 88 4E 54 3E 4E 56 4F 00 19 B0 DC 28 AF A0 95 6C 65 B4 2B 11 DD 8E FB 85 E2 B4
 33 B8 32 D2 7D 0B 08 71 F7 BE 53 29 49 1C 49 FE 59 71 A0 1B 04 32 3C 90 2C 2E 3A BD F1 24 9C
 F4 34 FF 0B 32 3D 14 4B 00 6D 6A 9B 99 5E 78 A7 05 65 C5 1D AB 73 9C 48 D6 03 1C 8D 94 8F A0
 97 61 E4 EF 9B 4F 6F 24 CD B0 F5 36 03 37 ED E4 BA B7 27 D7 93 35 23 F3 AE D8 F5 7A 6F D9 AD
 5F 94 80 2D AA 5C 33 B3 79 8F 47 0A 0B A6 64 D5 4D 59 2C C2 0C 82 F2 B1 A6 D0 BA F5 FD 80
 4D FB 58 19 45 5A 1A 5F BC B4 B3 7C AC BE 4B 8A E0 30 79 DC 94 B7 3D AB 8A A6 C0 E8 97 FF
 03 D1 47 04 06 9D 8A DF 10 C9 33 FC B6 E7 1D DA B5 46 65 E8 D4 27 A6 52 C5 4D 72 FA AF F1
 9D 60 F9 BF A3 C7 91 3B 96 C7 5A 96 2E 2F 2B 7A 3C 9A 18 A6 86 FA B4 06 E5 8B 4E 61 D4 CE BE
 96 23 F9 00 32 19 BB 9E A2 89 E8 75 64 0C D7 63 49 8F 50 D4 96 A4 F9 F7 FA 45 D4 C9 F7 B6 55
 A6 1A CB 93 6A CD E6 74 30 3A BF

Exponent 65537
 Key Size 4096 bits
 Key Usage Verify

Signature 512 bytes : 9A 17 F7 DE 5A 05 E2 55

94 BF 31 E3 98 01 39 BD D3 60 05 C9 0C 69 BB 8A F3 5A E7 A9 97 26 11 4D E0 A0 0E 7A 21 BB D9
 F8 F8 34 0F 20 37 9F 66 78 8D A2 91 1F 41 6A 38 39 9B 7B 9A 4B 4C 73 9A 95 D4 A7 5E 1E AC 98
 6E C7 61 07 5F C3 1E 85 1F 22 2A 0D CF 08 15 0F 48 47 5B 65 CA FF 28 3A A0 22 70 C6 78 A8 F2
 BF 29 FA E9 69 B9 F4 37 18 9F FE AA 0F 3C B5 A4 8F B0 5B 48 7B 52 CA 73 91 3C 21 96 AA 4B 65
 BE D4 F7 11 D8 6C E5 9B F8 30 39 86 4E DF 2F 19 B3 2F 78 6C 68 0A 8B 9B C4 6C 6C F0 D8 2B 5B
 FD 89 E2 7F 42 42 C3 A9 82 DF E3 AD 64 71 F2 28 E5 21 8A 06 AD 1E 0B 24 3D 18 28 23 2E 80 C5
 DE 2C 2C 50 1D FE CE B3 B2 14 61 A8 84 08 32 BB 7B 4D 9D D0 30 9A 53 21 89 B0 97 66 26 E8 ED
 EC 70 60 2A 42 61 DF 90 1E E7 21 CE 49 E1 09 94 FE 6E CC A9 96 DC 50 8A 31 DE FF 06 33 F7 4A
 B5 54 34 3D B9 A2 26 8F F5 A5 69 32 18 C2 B4 F8 A8 6E 6A 5B 93 C0 0D E9 06 B0 3D D6 1C 05 52
 A4 C2 27 03 68 A5 35 5D B2 F5 45 A6 84 FA 8A 6A 65 3C 7D 90 B1 13 3E 32 BA C7 08 6F 45 70 C8
 F6 23 73 12 D9 63 C9 CE DC 7E 45 0F C3 15 2E 6C 64 47 78 9E A3 1E 32 AB 4D 39 85 7A C1 4F 7D
 8A 5B FC F4 DB 94 C6 02 01 DE 64 62 3B 44 6F 20 22 13 39 26 86 2C 45 EC 85 82 E9 E1 E5 8F EA
 C8 C8 94 8D 7A 80 EC 84 5C E0 FB 09 F7 39 6D 49 6E 83 16 AC 32 93 C6 ED FC 27 E4 A9 07 47 8F
 EF 47 7F 28 F2 99 92 63 9D 7E 6B AC E7 CA 69 C2 CF 4F DC 4E 16 4A 47 B1 13 81 A8 68 E8 49 85
 D2 64 20 31 89 26 97 89 00 94 F5 6A 72 E6 24 E0 71 98 52 32 53 06 A1 9F 13 9E D5 B2 71 B8 C8
 8D D2 9E B7 30 F1 D5 71 34 F9 CE FF 26 7C 05 F0 B0 80 97 DA 79 F7 D7 59 F6 3B 66 5A 31 A8 C0
 47 93 70 7D E0 1A FC 5D

Extension Key Usage (2.5.29.15)
 Critical YES
 Usage Key Cert Sign, CRL Sign

Extension Basic Constraints (2.5.29.19)
 Critical YES
 Certificate Authority YES
 Path Length Constraint 0

Extension Subject Key Identifier (2.5.29.14)
 Critical NO
 Key ID 4A C8 02 04 18 43 C2 BD 7F 03 90 B8 8F F7 13 C8 DC BE BE 26

Extension Authority Key Identifier (2.5.29.35)
 Critical NO

Key ID 73 A0 A2 20 9D 0C C2 10 56 6D 9A 7D 17 F7 F5 63 61 12 67 11

Extension Certificate Policies (2.5.29.32)
Critical NO
Policy ID #1 (1.3.6.1.4.1.34253.7.2)
Qualifier ID #1 Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI <http://qtsp.viafirma.com/cps>

Extension CRL Distribution Points (2.5.29.31)
Critical NO
URI http://qtsp.viafirma.com/tsp/root_ca.crl
URI http://qtsp1.viafirma.com/tsp/root_ca.crl

Extension Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical NO
Method #1 CA Issuers (1.3.6.1.5.5.7.48.2)
URI <http://qtsp.viafirma.com/tsp/rootca.crt>
Method #2 Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI <http://qtsp.viafirma.com/ocsp>

Fingerprints

SHA-256 45 13 96 84 F6 2A 6D 70 A5 B8 B2 45 6B 9F 1D 63 CF 5A 57 20 12 3F 48 FA C1
C1 6B EB BE 3E 4E 24

SHA-1 58 A2 40 64 73 EB C0 B2 29 4D 8B 64 50 02 EA 87 98 58 3C 29

7.3.2. Certificado utilizado para firma el OCSP que valida el certificado de TSU

VIAFIRMA TSA OCSP

Subject Name

Country ES
Organization VIAFIRMA SOCIEDAD LIMITADA
Organizational Unit VIAFIRMA QTSP
Serial Number VATES-B91052142
Common Name VIAFIRMA TSA OCSP

Issuer Name

Country ES

Organization VIAFIRMA SOCIEDAD LIMITADA
Organizational Unit VIAFIRMA QTSP
Serial Number VATES-B91052142
Common Name VIAFIRMA TSA SUB CA

Serial Number 23 D8 01 8D C2 FC 87 52 37 D3 75 F0 96 9F 70 3B C6 68 BD A7
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none

Not Valid Before Friday, 18 October 2019 at 09:42:49 Central European Summer Time
Not Valid After Sunday, 16 October 2039 at 00:00:00 Central European Summer Time

Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 256 bytes : DB 56 47 FE 87 0D 03 61

68 C9 C2 A6 87 8A 1E 81 0A 61 32 5A 33 F4 57 5F 52 E8 27 59 3D DF 1F 1A 95 59 D2 50 22 A7 51
E6 26 6A 87 DC C0 D4 D2 A2 7D 62 50 A0 A5 A5 6B AD 2F 43 9B 7E 54 C0 55 52 D3 18 44 88 DA
4C 37 15 34 27 99 38 14 30 DF D3 24 38 24 3C 8B 44 6C 40 EF 17 5B C2 BF F7 4B E8 5F 2E CA 68
1D CF 68 BE 23 45 AC CD 87 20 15 92 32 D0 80 61 29 60 A1 70 EF 03 55 ED DA BB F7 09 51 07 44
55 0B DB 97 5A A8 D7 6A 08 7A 7A 89 2D DE 6E DD 48 04 AB 26 6B 32 0F 2C 8E 2C 5F 39 CC 63
67 2E D8 FC 58 6A F9 EB 4E A7 F5 B1 39 7B A2 2C 4B 10 F7 C9 A9 1C 8B D0 99 F8 93 0A E7 4C 26
0C AD 72 96 9F FE B3 A7 C4 C1 98 09 F8 72 37 0A CD 77 D8 3F 00 65 85 AD 49 76 6E CD 54 B1 58
CD 41 BF 11 1F E3 A2 F9 FE 19 F7 32 C2 57 75 A8 69 27 A9 14 A8 DD AF C3 0B 71 B0 55 5C 69 F1
3A 53

Exponent 65537
Key Size 2048 bits
Key Usage Verify

Signature 512 bytes : 19 39 4F A5 7C 7A B4 96

A7 81 98 57 CB 01 D1 15 06 7A 9D 80 1F 19 92 4F CE FE 2C BA D7 14 17 EC 53 9F 30 B4 52 12 7B
93 81 81 49 69 90 63 BB D4 33 44 D0 5D 25 5E 76 4F DF 0E DD 2E 1C B0 22 0E 3F 29 19 55 D1 BC
A0 2D 88 E4 53 20 5E 17 70 63 63 F0 C2 D5 0D 37 7A B8 84 41 61 ED 05 EC 6C F2 3F FA 79 2E E6
11 F7 69 1B 49 38 8A 7D C9 41 3C B5 8D 6C 66 2A F7 01 05 0F B8 3D FD 35 EE B1 14 48 0C F6 7F
1F 9B B9 A3 C0 DA FF 15 79 73 80 4B 92 41 85 9C 16 69 C8 58 BB EE 85 10 6F 5E 48 1D 3C DB FA
F7 DB F4 F4 F1 02 39 74 2C DE BA 07 36 46 03 C6 68 5F DB C3 5F 4A 8C E2 39 A2 1A EC E8 7F 03
01 8C F0 DE F6 A4 DE 0E FE AC 73 AC 0F A7 36 AD 40 EE E3 B9 2E 95 3D 58 08 13 FD 87 D2 20 CB
24 9B 63 EF EE DB FC 58 86 8C 95 05 A5 E2 4F CF 4C D8 D1 A0 F3 E2 C3 71 96 64 F3 FF 7E 44 59
0B 27 29 2A FA 83 4D 30 9C AA F0 9D DF B8 65 AA 99 60 38 B3 4C 3A B6 C7 80 2B E0 4D E4 5B
A2 A0 2D 91 BE D9 01 41 38 57 70 0B 00 2B 88 A1 C1 3A B9 8D E2 C0 96 5A 89 31 E3 B6 E2 9D A5
3D 5A 75 70 85 41 10 DF 97 6B A3 98 AB D9 CA E3 AB 53 C2 4D 5A 00 CF C5 04 12 A3 11 40 DF 95
A9 A5 1A 9D 76 01 0E CF F3 31 C1 AF 8D 60 A5 8D B5 3E 7E 7A B8 BF B6 34 44 3D F7 8D 92 73 3B
7D 68 CF 90 BC E1 9D 1C 92 41 0E 26 3E 32 1B 76 A1 C9 0E C2 42 75 79 D2 40 89 0D CC 88 55 26
0D BC 5C B1 31 A7 99 B0 33 4B B0 1C 39 73 E1 03 E9 00 6B BC 9B AD E4 E9 84 D1 76 80 93 7E 57
FE D9 31 34 5A 20 0A 89 14 B2 EB 5C 19 EE A6 9F 58 CB 80 A3 AF 18 8C E2 31 EC FF 1C 93 9C 1C
CE 84 CF CB 30 B4 AC C2 0D 4D 53 F4 00 13 2F AE 01 5D 61 76 7F 47 49 86 F4 EF BF CF B3 2E 72
76 C4 FB 09 91 6B 1D 8A 27

Extension Key Usage (2.5.29.15)

Critical YES
Usage Digital Signature, Non-Repudiation

Extension Basic Constraints (2.5.29.19)
Critical YES
Certificate Authority NO

Extension Extended Key Usage (2.5.29.37)
Critical YES
Purpose #1 OCSP Signing (1.3.6.1.5.5.7.3.9)

Extension Subject Key Identifier (2.5.29.14)
Critical NO
Key ID 51 E1 B5 CF 26 9C 75 9D 18 71 06 0B FE AE 59 88 A3 79 DC 1E

Extension Authority Key Identifier (2.5.29.35)
Critical NO
Key ID 4A C8 02 04 18 43 C2 BD 7F 03 90 B8 8F F7 13 C8 DC BE BE 26

Extension Certificate Policies (2.5.29.32)
Critical NO
Policy ID #1 (1.3.6.1.4.1.34253.7.4)
Qualifier ID #1 Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI <http://qtsp.viafirma.com/cps>

Extension CRL Distribution Points (2.5.29.31)
Critical NO
URI http://qtsp.viafirma.com/tsp/tsa_subca.crl,http://qtsp1.viafirma.com/tsp/tsa_subca.crl

Extension Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical NO
Method #1 CA Issuers (1.3.6.1.5.5.7.48.2)
URI <http://qtsp.viafirma.com/tsp/subca.crt>

Fingerprints

SHA-256 25 DD A3 25 6A D7 F4 CC 87 BE 6B 80 83 1F 31 EA 34 1F 22 3A 1C 31 11 20 A0
E7 E6 4D B2 26 8C C3
SHA-1 ED F4 5D DF E3 72 5A C5 3A FA 3C 12 77 19 B5 18 EF 3A 31 BE

8. AUDITORÍAS

8.1. Frecuencia o circunstancias de la auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

8.2. Identidad y cualificación del auditor

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

8.3. Relación del auditor con el prestador

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

8.4. Temas tratados en la auditoría

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

8.5. Acciones a realizar como resultado de una deficiencia

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

8.6. Comunicación de resultados

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9. OTROS ASUNTOS LEGALES

9.1. Tarifas

9.1.1. Tarifa para la emisión y renovación de certificados

Viafirma QTSP establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial <https://qtsp.viafirma.com>.

9.1.2. Tarifa de acceso al certificado

Viafirma QTSP establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial <https://qtsp.viafirma.com>.

9.1.3. Tarifa de acceso a OCSP o CRL

No se establecen tarifas o costes adicionales para el acceso a las fuentes de verificación OCSP o CRL publicadas por Viafirma QTSP. Su uso gratuito.

9.1.4. Tarifa para otros servicios

Viafirma QTSP establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial <https://qtsp.viafirma.com>.

9.1.5. Política de reembolsos

Viafirma QTSP establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial <https://qtsp.viafirma.com>.

9.2. Responsabilidad financiera

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.3. Confidencialidad de la información comercial

9.3.1. Alcance de la información confidencial

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.3.2. Alcance excluido de la información confidencial

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.3.3. Responsabilidad para la protección de la información confidencial

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.4. Privacidad de la información personal

9.4.1. Plan de privacidad

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.4.2. Información con tratamiento privado

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.4.3. Información no considerada con tratamiento privado

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.4.4. Responsabilidad para la protección de la información privada

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.4.5. Consentimiento de uso de la información privada

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.4.6. Divulgación de conformidad con procesos judiciales o administrativos

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.4.7. Otras casos para la divulgación de información

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.5. Derechos de propiedad intelectual

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.6. Obligaciones y Responsabilidad

9.6.1. Obligaciones de la CA

Lo establecido en las Declaración de Prácticas de Certificación de Viafirma QTSP.

9.6.2. Obligaciones de la RA

Bajo la presente política de certificados no se contempla el uso de autoridades de registro.

9.6.3. Obligaciones del suscriptor

- Hacer uso del certificado acorde a los límites y condiciones regulados en la presente política de certificados.
- Poner todos los medios a su alcance para la protección y uso adecuado de la clave privada del certificado.
- Solicitar inmediatamente la revocación del certificado ante la sospecha de un compromiso de clave.
- No hacer uso del certificado cuando éste ha caducado o ha sido revocado.

9.6.4. Obligaciones de los terceros que confían

Es obligación de los terceros que confían en los certificados y servicios prestados por Viafirma QTSP:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y su correspondiente política de certificado.
- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
- Asumir su responsabilidad en la correcta verificación de las firmas digitales
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

9.6.5. Obligaciones de otras entidades

Viafirma QTSP no establece obligaciones a otras entidades participantes.

9.7. Renuncias de la garantía

Viafirma QTSP podrá renunciar aquellas garantías de los servicios que estuvieran asociados a las obligaciones definidas en el marco regulatorio vigente para los prestadores de confianza, en concreto aquellas que pudieran estar adaptadas a un propósito particular o mercantil.

9.8. Límites de responsabilidad

- Daños y perjuicios en los usos que puedan realizarse de los certificados o sellos de tiempo de Viafirma QTSP, ya sean estos por culpa de los interesados o por defectos de origen de los elementos.
- Hechos acontecidos por usos no acordes con las presentes CPS, en casos de desastres naturales, atentado terrorista, huelga, fuerza mayor (incidencias en servicios eléctricos o redes telemáticas o de comunicaciones), así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad.
- Usos indebidos, fraudulentos, en ausencia de convenio o contrato suscrito con Viafirma QTSP, en caso de extralimitación del uso o de omisiones del suscriptor.
- Los algoritmos criptográficos ni de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si se ha procedido con la diligencia debida de acuerdo al estado actual de la técnica, y conforme a los documentos publicados y la normativa vigente.

- Problemáticas asociadas al incumplimiento por parte de los suscriptores de las condiciones de contratación (por ejemplo, impagos).

9.9. Indemnizaciones

Las cuantías que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial Viafirma QTSP a los suscriptores en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de TRES MIL EUROS (3.000€).

9.10. Términos de uso y duración

9.10.1. Términos de uso

Viafirma QTSP establece en sus límites de uso las condiciones de uso de los distintos servicios de confianza prestados. Todos ellos serán informados en el Texto Divulgativo asociado a cada servicio y publicado en la página oficial <https://qtsp.viafirma.com>.

9.10.2. Duración

La duración estará sujeta al tipo de servicio contratado en cada caso, y definido por tanto en los términos y condiciones de cada uno de ellos.

9.10.3. Supervivencia tras fin de la duración

Viafirma QTSP establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, cláusulas de supervivencia, en virtud de la que ciertas reglas continúan vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

9.11. Avisos y comunicaciones individuales a los participantes

Viafirma QTSP podrá hacer uso de notificaciones y comunicaciones realizadas de forma individual a las partes involucradas en el servicio prestado, en especial a los suscriptores, donde podrán ser notificados de forma automática ante eventos asociados a caducidades, renovaciones, etc..

9.12. Resolución de Conflictos

9.12.1. Procedimiento de conflictos

Viafirma QTSP tiene previsto el uso de mecanismos jurídicos mediante los que se articule su relación con los suscriptores del servicio, los procedimientos de mediación, arbitraje y resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de la legislación de procedimiento administrativo aplicable.

9.12.2. Mecanismo y período de notificación

Se mantendrán de forma preferente los mismos canales elegidos por las partes afectadas en el conflicto.

9.12.3. Circunstancias por las que un OID puede ser modificado.

No se contempla.

9.13. Disposiciones para la resolución de disputas

Las relaciones entre los suscriptores y Viafirma QTSP se rigen por la normativa española y europea vigente, así como la legislación específica civil, mercantil y de protección de datos que sea aplicable.

En el caso de conflictos surgidos en relación con los servicios de prestador de confianza, las partes tratarán una resolución amistosa. En el caso de no ser posible, las partes se someten a la jurisdicción exclusiva de los tribunales de España en la ciudad de Sevilla.

De igual forma, en los Términos y condiciones del servicio de confianza expresamente contratado o consumido estarán publicados en el sitio web <http://qtsp.viafirma.com>.

9.14. Normativa aplicable

El presente documento se ha realizado considerando, al menos, la siguiente normativa aplicable:

- Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS).

- Ley 59/2003, de 19 de diciembre, de firma electrónica, derogada por la Ley 6/2020, de 11 de noviembre.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Del mismo modo, se han considerando los siguientes estándares tecnológicos:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers.
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).

9.15. Cumplimiento de la normativa aplicable

Viafirma QTSP declara que las presentes CPS y sus correspondientes políticas de certificados cumplen con lo dispuesto en la normativa aplicable y en concreto a lo dispuesto en el Reglamento (UE) 910/2014.

9.16. Otras disposiciones

No se definen otras disposiciones adicionales.

9.17. Otras provisiones

Dando cobertura a cualquier eventualidad que haga colisionar algunas de las disposiciones definidas en la documentación reguladas por las presentes CPS, se tendrá en consideración como criterio de prioridad el siguiente orden de documentos.

- a) La PC (política de certificado o servicio explícita)
- b) La DPC
- c) Límites de uso y condiciones del servicio explícitamente contratado