Sistemas Informáticos Abiertos, S.A.
Avenida de Europa, 2
Alcor Plaza Edificio B
Parque Oeste, Alcorcón 28922
Alcorcón - Madrid (España)
Telf: (34) 902 480 580 Fax: (34) 91 641 95 13

www.sia.es

PDS – SIA TSP

Texto divulgativo del Prestador de Servicios de Confianza SIA

Servicio de expedición de certificados electrónicos de autenticación de sitios web

Fecha: 17/11/2020

INDICE

RELACION DE TABLAS

1. INFORMACIÓN DEL TSP

El presente documento recoge la información relativa al Servicio de expedición de certificados electrónicos cualificados del Proveedor de Servicios de Confianza SIA a un alto nivel. Para la definición de este texto divulgativo, se han seguido las indicaciones de la norma ETSI 319 411 - anexo A.

Este documento, no reemplaza ni las Políticas del Servicios de expedición de certificados electrónicos cualificados (PC) ni la Declaración de Practicas de certificación (DPC) de SIA, las cuales se encuentran accesibles en la propia WEB del Proveedor de Servicios de Confianza (TSP).

1.1 Organización responsable del TSP

Nombre	SIA
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580

Tabla 1 – Organización responsable

1.2 Datos de contacto del TSP

Contacto	psc@sia.es
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2

	Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580
Web	https://psc.sia.es

Tabla 2 – Persona de contacto

Los suscriptores, los terceros que confían, los proveedores de software de aplicación y otros terceros pueden ponerse en contacto con AC SIA mediante soc@sia.es para denunciar incidentes de seguridad relacionados con los certificados proporcionados por el TSP, un supuesto compromiso de la clave privada, un uso incorrecto de certificados, otros tipos de fraude, compromiso, uso indebido o conducta inapropiada relacionada con los certificados o PKI de SIA AC

2. TIPOS DE SERVICIOS

2.1 Tipos de certificados emitidos

El proveedor de servicios de confianza emite los siguientes tipos de certificados de autenticación de sitio web

- Certificados cualificados de Autenticación de Sitio Web – Nivel medio.
- Certificados cualificados de Autenticación de Sitio Web PSD2 – Nivel medio
- Certificados cualificados de Sede Electrónica – Nivel medio
- Certificados cualificados de Sede Electrónica – Nivel alto

Los certificados electrónicos cualificados, son cualificados en cumplimiento con los requisitos del Reglamento (UE) Nº 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 (eIDAS).

Estos certificados se expiden conforme al Reglamento (UE) Nº 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 (eIDAS)

2.2 Procedimientos de Validación

Las terceras partes que confíen en los certificados de autenticación de sitio web de SIA, tendrán lo obligación de conocer los detalles de la DPC y política que aplica a cada tipo de certificado. Pudiendo verificar por medios de validación de OCSP y descarga de CRLs indicados, la validez del estado de los certificados.

Los Certificados SIA para autenticación de sitio web y sede electrónica se encuentran dentro de la jerarquía “SIA Root 2020”.

Se podrá ampliar la información respecto a este apartado en las PC y DPC ubicadas en la Web del TSP y detalladas en el siguiente apartado.

2.3 Usos de los certificados

Los certificados del Proveedor de Servicios de Confianza SIA, se emitirán bajo los términos de uso establecidos en sus correspondientes políticas:

Nombre identificativo de la Política	OID de la Política
Política de certificación de Certificados de autenticación de sitio web y Sede Electrónica **1.3.6.1.4.1.39131.10.1.21**	1.3.6.1.4.1.39131.10.1.21.1 (QWAC, QWAC PSD2, Sede Nivel alto y Sede Nivel alto)

Tabla 3 – OID políticas de certificación

3. LIMITES DE CONFIANZA

Un certificado emitido por la AC de SIA sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en la Declaración de Practicas de Certificación y en su correspondiente Política de Certificación, por lo que existen ciertas limitaciones en el uso de los certificados de SIA.

Los certificados deben emplearse únicamente de conformidad con la legislación que les sea aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación en materia criptográfica existentes en cada momento.

Los certificados deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades de las descritas para cada uno de ellos.

Ha de considerarse, que se tendrán en cuenta los requisitos relativos al archivo de registros y logs de eventos / auditoria de la especificación ETSI 319 411-1, apartados 6.4.5 y 6.4.6. Al igual que las obligaciones indicadas por la normativa vigente.

La AC y la AR no serán responsables de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del solicitante, de la entidad y/o Terceros usuarios, ni de la incorrecta utilización de los Certificados y las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información suministrada por la AC, en particular, el lucro cesante, la pérdida de ingresos o pedidos o pérdida de datos, no dando lugar a ningún tipo de derecho indemnizatorio.

La AC y la AR no será responsable en ningún caso cuando se encuentre ante cualquiera de las circunstancias establecidas en la delimitación de responsabilidades de la DPC

Si cualquier parte usuaria o tercero, confía en un Certificado de autenticación de sitio web sin realizar la comprobación del estado del Certificado, no se obtendrá cobertura de la Declaración de Prácticas de Certificación aplicable a este tipo de certificados y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra SIA por daños, perjuicios o conflictos provenientes del uso o confianza en un Certificado de autenticación de sitio web.

4. OBLIGACIONES DE LOS SUSCRIPTORES

Las obligaciones de los suscriptores serán las estipuladas en los convenios o contratos firmados por parte del proveedor de servicios de confianza y las personas o entidades que solicitan los servicios de emisión de los certificados .

Se podrá ampliar la información respecto a este apartado en las PC y DPC ubicadas en la Web del TSP.

5. OBLIGACIONES DE VALIDACIÓN DE LAS PARTES DE CONFIANZA

Para la validación del estado de los certificados emitidos por el TSP SIA, los usuarios o terceras partes aceptantes, podrán emplear los mecanismos dispuestos en el apartado 2.2 Procedimientos de Validación del presente documento.

Ha de considerarse, que se tendrán en cuenta los requisitos especificados en ETSI 319 411-1, apartado 6.3.5 h) hasta j). y 6.3.5-03 a).

Será de obligación de los terceros aceptantes:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en el momento de realizar cualquier operación basada en ellos, en conformidad con lo expresado en las extensiones de los certificados y en la DPC, PC y términos y condiciones.
- Asumir su responsabilidad en la comprobación de la validez y del estado de revocación de los certificados en que confían.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confían y asumir sus obligaciones.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

6. LIMITACIONES DE RESPONSABILIDAD

Las limitaciones de responsabilidad de los suscriptores serán las estipuladas en los convenios o contratos firmados por parte del proveedor de servicios de confianza y las personas o entidades que solicitan los servicios proporcionados por la Autoridad de emisión de certificados.

Se podrá ampliar la información respecto a este apartado en las PC y DPC ubicadas en la Web del TSP.

7. ACUERDOS APLICABLES, DPC Y PC

Las PCs y DPC ya indicadas detallaran los acuerdos aplicables, al igual que en los convenios o contratos firmados por parte del proveedor de servicios de confianza y las personas o entidades que solicitan los servicios proporcionados por la Autoridad de emisión de certificados.

Se podrá ampliar la información respecto a este apartado en las PC y DPC ubicadas en la Web del TSP.

8. POLÍTICA DE PRIVACIDAD

El proveedor de servicios de confianza SIA, aplica la política de protección de datos personales vigente en España. Incorporando a un fichero registrado en la Agencia de Protección de Datos especifico del TSP.

Toda la información recabada será almacenada por el TSP según lo estipulado por la legislación vigente aplicable.

9. POLÍTICA DE DEVOLUCIÓN

La política de reembolso será la estipulada en los convenios o contratos firmados por parte del proveedor de servicios de confianza y las personas o entidades que solicitan los servicios proporcionados por la Autoridad de emisión de certificados.

Se podrá ampliar la información respecto a este apartado en las PC y DPC ubicadas en la Web del TSP.

10. LEGISLACIÓN APLICABLE Y RESOLUCIÓN DE CONFLICTOS

10.1 Legislación aplicable

La normativa aplicable al presente documento, así como a las distintas PC, y a las operaciones que derivan de ellas, es la siguiente:

- Reglamento (UE) Nº 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 (en adelante eIDAS) y por el que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

10.2 Resolución de conflictos

Para la resolución de cualquier conflicto que pudiera surgir en relación con este documento, las PC o el instrumento Jurídico vinculante, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles a los Tribunales de Justicia de Madrid.

11. ACREDITACIONES DE CONFIANZA Y AUDITORIAS DE CONFORMIDAD

Conforme a lo establecido en el Reglamento eIDAS y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, el Proveedor de Servicios de Confianza SIA se encuentra incluido en:

- TSL; Lista de Proveedores de Confianza Española
- Portal de Proveedores de Servicios de Confianza del Organismo Supervisor.

Así mismo, el TSP SIA cuenta con el Informe de evaluación de la conformidad en el marco del reglamento (UE) nº 910/2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior (reglamento eIDAS).