PDS

Declaración de Divulgación PKI

CÓDIGO DEL DOCUMENTO	**ICERT-INDI-PDS**
VERSIÓN	**3.3**

INFOCERT
TINEXTA GROUP

1. ÍNDICE

2. Introducción

Esta Declaración de divulgación de Infraestructura de Clave Pública - PKI (PDS, por sus siglas en inglés) cumple el requisito de publicación dispuesto en la norma europea ETSI EN 319 411-1, relativa al servicio de certificación ofrecido por el Prestador de Servicios de Confianza Cualificado InfoCert SpA, (en adelante, «**InfoCert»,** «**QTSP**» o «**CA**»), y tiene por objeto facilitar al solicitante del servicio la información técnica necesaria para su utilización.

El 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 el que se deroga la Directiva 1999/93/CE se denomina en adelante «**Reglamento eIDAS**».

Este documento se suma a los Términos y Condiciones del Servicio como parte integral de la documentación contractual de InfoCert.

La publicación de este PDS no reemplaza la publicación de la Declaración de Prácticas de Certificación (CPS, por sus siglas en inglés), en la que se detalla la información, que puede consultarse en el sitio web de InfoCert, en la dirección:
https://www.firma.infocert.it/documentazione/.

3. Contactos

InfoCert S.p.A. – Núm. de IVA 07945211006
Prestador de Servicios de Confianza Cualificado
Piazza Sallustio, 9
00187 - Roma, Italia

Oficina comercial
Piazza Luigi da Porto, 3
35131 Padua, Italia

Teléfono: +39 06 836691 - Fax: +39 06 23328861
Número de teléfono de atención al cliente Firma Digital: ver enlace https://help.infocert.it/contatti/
Web: http://www.firma.infocert.it/
e-mail: firma.digitale@legalmail.it
Es posible solicitar la **revocación** del certificado de firma digital utilizando el formulario apropiado publicado en el sitio web de InfoCert y enviándolo por email certificado, correo postal certificado o fax, acompañado de una fotocopia de un documento de identidad válido. También es posible solicitar la revocación en la oficina de registro pertinente, de conformidad con los Términos y Condiciones del Servicio.. InfoCert se reserva el derecho de realizar otras verificaciones sobre la identidad del solicitante.

Es posible solicitar la **suspensión** del certificado de firma digital directamente online en el sitio web de InfoCert, utilizando el código secreto asignado durante el registro.

4. Tipos de certificados, validación y uso

InfoCert expide certificados cualificados conformes a la norma europea **ETSI EN 319 411** y otras normas conexas, los certificados se ofrecen al público (empresas privadas, organismos públicos, profesionales, particulares, etc.), según las condiciones publicadas en el sitio web del QTSP o de las Autoridades de Registro (RA, por sus siglas en inglés).

El algoritmo utilizado para firmar los certificados puede elegirse de entre los siguientes:

• sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]

• ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]

• ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]

• ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)].

Las firmas y certificados se pueden verificar mediante la App **GoSign**, que es posible descargar de forma gratuita del sitio web de InfoCert.

5. Límites de responsabilidad

InfoCert emite:

- **certificados cualificados a personas físicas** para firma electrónica avanzada o cualificada;
- **certificados cualificados a personas jurídicas para sello electrónico**, incluso para cumplimiento PSD2

Asimismo, InfoCert presta servicios de firma a distancia en los Dispositivos de Creación de Firma Electrónica Cualificada (QSCD, por sus siglas en inglés), generando y gestionando claves y certificados para el firmante.

Los detalles y políticas se pueden encontrar en las Declaraciones de Prácticas de Certificación disponibles en *https://www.firma.infocert.it/documentazione*.

El período de validez de cada certificado figura en el mismo y puede variar entre un mínimo de una hora y un máximo de tres años y tres meses.

Está prohibido emplear el certificado fuera de los límites y finalidades establecidos en el CPS y en los contratos, como así también infringiendo los límites de uso y de valor (*key usage*, *extended key usage*, *user notice*) indicados en el certificado.

Los registros de eventos relacionados con la emisión de certificados se almacenan en el sistema de almacenamiento de InfoCert durante al menos

20 (veinte) años a partir de la fecha de expiración del certificado hasta un máximo de 23 (veintitrés) años a partir de la fecha de expedición.

6. Obligaciones del Suscriptor

El **Suscriptor** deberá cumplir con las cláusulas contenidas en el CPS y en los Términos y Condiciones del Servicio, a saber:

- leer y comprender la documentación contractual y cualquier documentación de información adicional;
- efectuar los procedimientos de identificación adoptados por la Autoridad de Certificación como se describe en el CPS;
- proporcionar toda la información necesaria para la identificación, acompañada, en su caso, de la documentación adecuada;
- utilizar el par de claves solo para los fines y en la forma permitida por el CPS;
- al firmar la solicitud de registro y certificación, aceptar las condiciones contractuales que rigen la prestación del servicio, tal como indicado en los formularios analógicos o electrónicos puestos a disposición por la CA;
- informar rápidamente a la CA o la RA, hasta la fecha de expiración del certificado, de los siguientes hechos:
    - si el dispositivo de firma del Suscriptor ha sido extraviado, robado o dañado;
    - la pérdida del control exclusivo de la clave privada, por ejemplo, debido a que se encuentran comprometidos los datos de activación (por ejemplo, el PIN) del dispositivo de firma;
    - algunos de los datos del certificado del Suscriptor son incorrectos o ya no son válidos;
- proteger la confidencialidad de las credenciales necesarias para utilizar los dispositivos o servicios de firma, no comunicándolas o revelándolas a terceros y manteniéndolas bajo su control exclusivo;
- dejar de usar de forma inmediata y permanente la clave que ha sido comprometida, excepto para desencriptar la misma clave;

- asegurarse de que la clave privada ya no sea utilizada por el suscriptor si se le informa al solicitante que el certificado del Suscriptor ha sido revocado, o que la CA ha sido comprometida.

El solicitante es responsable de proporcionar y utilizar una conexión a Internet y todos los instrumentos necesarios (equipo y programas informáticos).

7. Obligaciones del Solicitante si no fuera el Suscriptor

De no ser el Suscriptor, el **Solicitante** deberá atenerse a las cláusulas contenidas en el CPS y en los Términos y Condiciones del Servicio, a saber:

- leer y comprender la documentación contractual y cualquier documentación de información adicional;
- respetar los procedimientos de identificación adoptados por el QTSP;
- proporcionar toda la información necesaria para la identificación, acompañada, en su caso, de la documentación adecuada;
- al firmar la solicitud de registro y certificación, aceptar las condiciones contractuales que rigen la prestación del servicio, tal como indicado en los formularios analógicos o electrónicos puestos a disposición por la CA;
- identificar y comunicar al TSP el procedimiento informático a través del cual se enviarán los documentos que se someterán al procedimiento de firma a distancia y la activación de las claves de firma por parte del Suscriptor;
- correr con los gastos del servicio de firma a distancia e indicar, mediante actos y procedimientos específicos, los Suscriptores a los que se deberán expedir los certificados;
- indicar el tipo de sistema de autenticación elegido para activar el procedimiento de firma a distancia;
- si tiene la intención de solicitar la revocación o suspensión del certificado del Suscriptor, deberá firmar el correspondiente formulario

de solicitud de revocación o suspensión puesto a disposición por el QTSP;

- informar al Suscriptor de las obligaciones que se derivan del certificado, proporcionar la información correcta y veraz sobre la identidad del Suscriptor, y respetar los procesos e instrucciones del QTSP y/o de la RA;
- si el Suscriptor es una persona jurídica, proporcionar la siguiente información al QTSP:
    - Apellido y nombre del Solicitante;
    - Código TIN o código de identificación similar del Solicitante (código fiscal en Italia);
    - Detalles del documento de identificación presentado para la identificación del Solicitante, tales como tipo, número, organismo emisor y fecha de emisión del mismo;
    - Correo electrónico para enviar comunicaciones del QTSP al Solicitante;
    - Nombre del titular o persona jurídica;
    - VAT code o bien NTR (número de IVA o número de Registro Mercantil para los Suscriptores italianos);
- cuando las claves se generan en el dispositivo del Suscriptor, el Solicitante también debe enviar la solicitud en formato PKCS#10 firmada por el mismo Solicitante. Si el QTSP no pone a disposición el dispositivo de firma, el Solicitante deberá garantizar que el dispositivo respeta la normativa vigente presentando la documentación correspondiente y sometiéndose a auditorías periódicas del QTSP.

8. Estado de validez de los certificados

Todos aquellos que se basan en la información contenida en los certificados deben verificar que los certificados no estén suspendidos ni revocados.

La información sobre el estado de los certificados se obtiene consultando la lista de certificados revocados (CRL) publicada por la CA en la URL indicada en el certificado o a través del servicio OCSP. La validez del certificado se puede

verificar mediante el producto Dike GoSign, que es posible descargar de forma gratuita del sitio web de InfoCert.

9. Garantía limitada y ausencia/limitación de responsabilidad

Los certificados cualificados se proporcionan de acuerdo con este documento y los Términos y Condiciones del Servicio. Todos los detalles técnicos necesarios están explicados en el CPS.

InfoCert es responsable de eventuales daños determinados directamente, por mala fe o negligencia, a cualquier persona física o jurídica, como resultado del incumplimiento de las obligaciones establecidas en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de fecha del 23 de julio de 2014 y el hecho de que InfoCert no haya implementado todas las medidas adecuadas para evitar el daño.

En el caso mencionado en el apartado anterior, el Solicitante o el Suscriptor tendrá derecho a obtener, a título de indemnización por los daños sufridos directamente como resultado del comportamiento al que se hace referencia en el apartado anterior, una cantidad que en ningún caso podrá exceder los valores máximos dispuestos, por cada reclamación y por año, en el art. 3, apdo. 7, del Reglamento adjunto a la Determinación AgID 185/2017.

El reintegro no se puede solicitar si la imposibilidad de uso depende de la utilización inapropiada del servicio de certificación o por causa imputable al operador de la red de telecomunicaciones o si se deriva de circunstancias fortuitas, fuerza mayor o causas no atribuibles a InfoCert.

10. Acuerdos aplicables, políticas y Declaraciones de Prácticas de Certificación

Los acuerdos y condiciones aplicables al servicio del QTSP y los CPS están publicados en el sitio web de InfoCert en la dirección https://firma.infocert.it/documentazione.

11. Política de privacidad

La información relacionada con el Suscriptor/Titular y el Solicitante que la CA haya recabado en el ejercicio de sus actividades típicas debe considerarse, a menos de consentimiento expreso, confidencial y no publicable, con la excepción de aquellas explícitamente destinadas al uso público: *clave pública, certificado (si lo solicita el Suscriptor), fechas de revocación y suspensión del certificado*.

En particular, los datos personales son tratados por InfoCert de acuerdo con las disposiciones del Decreto Legislativo (Italia) 196, de 30 de junio de 2003, y del 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, aplicable a partir del 25 de mayo de 2018.

12. Política de reintegro

El Suscriptor/Titular deberá comunicar al QTSP su decisión de desistimiento del contrato mediante una declaración explícita enviada, antes de expirar el periodo de desistimiento, mediante email certificado a la dirección *richieste.rimborso@legalmail.it* o mediante carta certificada con acuse de recibo enviada a InfoCert S.p.A.. - Direzione Generale e Amministrativa - Via Marco e Marcelliano, 45 00147 Roma. A tal fin, para mayor comodidad, el Suscriptor/Titular podrá utilizar el formulario de desistimiento estándar

disponible en el sitio web de InfoCert, accediendo desde el siguiente enlace: *https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf*.

Los gastos de devolución del dispositivo de firma, en su caso, correrán por cuenta del Suscriptor/Titular y/o del Solicitante, mientras que el QTSP reintegrará los pagos ya realizados. Tales reintegros se efectuarán en la cuenta corriente bancaria utilizada para la transacción inicial, a menos que el Suscriptor/Titular haya indicado expresamente datos bancarios diferentes; en cualquier caso, el Suscriptor/Titular no incurrirá en ningún gasto como resultado de ese reintegro.

13. Ley aplicable a las reclamaciones y a la solución de controversias

La prestación del servicio de certificación y sello de tiempo está regulada por las leyes vigentes en Italia. Para todo aquello que no esté expresamente previsto en el presente documento, remítase al Código Civil italiano y a otras normas legales aplicables.
Para la resolución de cualquier conflicto que pudiere surgir de la interpretación y ejecución del presente contrato, o en relación con el mismo, se someterán a la jurisdicción exclusiva de los tribunales competentes de Roma, a menos que se especifique lo contrario en los Términos y Condiciones del Servicio.

Si el cliente es un consumidor, las posibles controversias relacionadas con el contrato celebrado por el consumidor estarán sujetas a la competencia territorial obligatoria de los tribunales del lugar de residencia o domicilio del consumidor.

14. Archivos, licencias y marcas, auditorías

La CA no verifica el uso de marcas comerciales pero puede negarse a generar o solicitar la revocación de un certificado involucrado en un conflicto.

La verificación de conformidad con el Reglamento (UE) 910/201, de 23/07/2014, conforme a las normas ETSI EN 319 401, ETSI EN 319 411-1; ETSI EN 319 411-2, ha sido realizada por CSQA Certificazioni S.r.l, según el esquema de evaluación eIDAS definido por ACCREDIA para las normas ETSI EN 319 403 y ISO/IEC 17065:2012.

InfoCert ha presentado el informe de conformidad a "Agenzia per l'Italia Digitale – AgID" che ha confirmado la presencia de InfoCert en la Lista de Confianza de Prestadores cualificados de servicios de confianza de acuerdo con el reglamento (UE) 910/2014, de 23/07/2014.

La Lista de confianza (Trusted List) de las Autoridades de Certificación (CA) en Italia se puede consultar en el sitio web *https://eidas.agid.gov.it/TL/TSL-IT.xml*