ACUERDO DE DIVULGACIÓN DE PKI (PDS)

Nº Versión: v 1.0
Fecha: 29 de mayo de 2017

Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490

ÍNDICE

1 INTRODUCCIÓN

El presente documento ha sido creado de acuerdo con los requisitos técnicos del Anexo B *de ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"*.

Este Acuerdo de Divulgación de PKI no pretende reemplazar a la DPC o a las correspondientes políticas de certificado, en las que se basa *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.* (en adelante, Izenpe) para la gestión de sus certificados.

Ambas están disponibles y pueden consultarse en www.izenpe.eus

2 DATOS DE CONTACTO

Nombre del prestador	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.
Dirección postal	c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz
Dirección e-mail	info@izenpe.com
Teléfono	902 542 542

El formulario y el procedimiento para solicitar una revocación de un certificado se puede obtener en www.izenpe.eus

3 TIPOS DE CERTIFICADO, PROCEDIMIENTO DE VALIDACIÓN Y USO

Las especificidades relativas a cada tipo de certificado emitido por Izenpe están reguladas en la *Política específica para cada certificado* que se adjunta a la *Declaración de Prácticas de Certificación.*

BREVE DESCRIPCIÓN	SOPORTE	IDENTIFICADOR DE POLÍTICA	OID POLÍTICA	Nivel aseguramiento eIDAS
CIUDADANO				
B@K	HSM	NCP	1.3.6.1.4.1.14777.5.2.5	Bajo
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	Sustancial
Certificado Ciudadano	Tarjeta/token USB (Chip criptográfico)	QCP-n-qscd	Perfil eIDAS 1.3.6.1.4.1.14777.2.6	Alto
			Perfil anterior a eIDAS	Alto

			1.3.6.1.4.1.14777.2.18.1	
REPRESENTANTE ENTIDAD				
Representante entidad	HSM	QCP-n	1.3.6.1.4.1.14777.2.14	Sustancial
	Tarjeta/Token USB: chip criptográfico.	QCP-n-qscd	1.3.6.1.4.1.14777.2.12	Alto
	Software: Contenedor de certificados de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.16	Sustancial
REPRESENTANTE ENTIDAD SPJ				
Representante Entidad SPJ	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	Sustancial
	Tarjeta/token USB: chip criptográfico.	QCP-n-qscd	1.3.6.1.4.1.14777.2.13	Alto
	Software: Contenedor de certificados de Izenpe	QCP-n	1.3.6.1.4.1.14777.2.17	Sustancial
PROFESIONAL				
Personal de Entidad Pública	Tarjeta / token USB: chip criptográfico.	QCP-n-qscd	1.3.6.1.4.1.14777.4.14.1	Alto
	Software: contenedor de certificados de Izenpe.	QCP-n	1.3.6.1.4.1.14777.4.14.2	Sustancial
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Sustancial
Personal de Entidad Pública con seudónimo	Tarjeta / token USB: chip criptográfico	QCP-n-qscd	**Firma** 1.3.6.1.4.1.14777.4.13.1.1	Alto
		NCP+	**Autenticación** 1.3.6.1.4.1.14777.4.13.1.2	Alto
		n/a	**Cifrado** 1.3.6.1.4.1.14777.4.13.1.3	Alto
Corporativo cualificado	Tarjeta / token USB: chip criptográfico	QCP-n-qscd	1.3.6.1.4.1.14777.2.19.1	Alto
	Software: contenedor de certificados de Izenpe.	QCP-n	1.3.6.1.4.1.14777.2.19.2	Alto

	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Sustancial
Corporativo no cualificado	Tarjeta / token USB	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a (no cualificado)
Personal de las Entidades públicas (pre-eIDAS)	Tarjeta / token USB	QCP public + SSCD	1.3.6.1.4.1.14777.4.1	n/a
Personal del Gobierno Vasco (pre-eIDAS)	Tarjeta / token USB	QCP public + SSCD	1.3.6.1.4.1.14777.7.1	n/a
Corporativo público reconocido (pre-eIDAS)	Tarjeta / token USB	QCP public + SSCD	1.3.6.1.4.1.14777.4.2	n/a
Corporativo público no reconocido (pre-eIDAS)	Tarjeta / token USB	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a
Corporativo privado reconocido (pre-eIDAS)	Tarjeta / token USB	QCP public + SSCD	1.3.6.1.4.1.14777.2.2	n/a
Corporativo privado no reconocido (pre-eIDAS)	Tarjeta / token USB	NCP+	1.3.6.1.4.1.14777.5.2.2	n/a

SELLO DE ENTIDAD				
Sello de entidad	Contenedor. Contenedor de certificados de Izenpe	QCP-l-qscd	1.3.6.1.4.1.14777.2.11	Sustancial
	HSM	QCP-l	1.3.6.1.4.1.14777.2.20	Sustancial

SELLO DE ADMINISTRACIÓN				
Sello de administración	Software Contenedor de certificados de Izenpe	QCP-l	1.3.6.1.4.1.14777.4.11.2	Sustancial
	HSM	QCP-l	1.3.6.1.4.1.14777.4.11.3	Sustancial

Sello de administración nivel medio (pre-eIDAS)	HSM	NCP+	1.3.6.1.4.1.14777.4.4	n/a

SERVIDOR SEGURO (SSL)				
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.1.2.4	n/a
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.1.2.1	n/a
SSL EV	Software	EVCP	1.3.6.1.4.1.14777.6.1.1	n/a
SEDE	Software	OVCP	1.3.6.1.4.1.14777.1.1.3	n/a
SEDE EV	Software	EVCP	1.3.6.1.4.1.14777.6.1.2	n/a

APLICACIÓN				
Aplicación	Software: contenedor de certificados de Izenpe.	NCP	1.3.6.1.4.1.14777.1.2.2	n/a

FIRMA DE CÓDIGO				
Firma de código	Tarjeta	NCP+	1.3.6.1.4.1.14777.1.3.1	n/a

4 LIMITACIONES EN LA CONFIANZA

Izenpe no aplica limitaciones específicas de confianza de sus certificados en esta política. Se pueden consultar las limitaciones de uso (firma, sello, web) de cada tipo de certificado en el apartado anterior.

Izenpe en su actividad como prestador de servicios de confianza mantiene registros internos o asegura el archivado, de una forma segura, de los siguientes elementos:

- ✓ Todos los certificados cualificados durante 15 años, y los no cualificados durante 7 años
- ✓ Evidencias de auditoría de la emisión de los certificados durante 7 años posterior a la fecha de caducidad
- ✓ Evidencias de auditoría de la revocación de los certificados durante 7 años posterior a la fecha de caducidad

Se almacenan los siguientes logs:

- ✓ Nuevas peticiones de certificado
- ✓ Peticiones de certificado rechazadas
- ✓ Violaciones de acceso a cuentas
- ✓ Firma de certificados
- ✓ Revocación de certificados
- ✓ Logon de cuentas

- ✓ Firma de CRLs
- ✓ Modificaciones en CAs
- ✓ Caducidad de certificados

5 OBLIGACIONES DE LOS SUSCRIPTORES

- ✓ Facilitar a Izenpe información completa y adecuada, conforme a los requerimientos de la Declaración de Prácticas de Certificación en especial en lo relativo al procedimiento de registro.
- ✓ Garantizar la veracidad, totalidad y actualidad de la información que deba constar en los certificados.
- ✓ Conocer y aceptar las condiciones de utilización de los certificados, así como las modificaciones que se realicen sobre las mismas.
- ✓ Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- ✓ Garantizar el buen uso y la conservación de los soportes de los certificados.
- ✓ Emplear adecuadamente el certificado y, en concreto, cumplir con las limitaciones de uso de los certificados.
- ✓ Ser diligente en la custodia de sus credenciales, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en la Declaración de Prácticas de Certificación.
- ✓ Notificar a Izenpe y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
- ✓ La pérdida, el robo o el compromiso potencial de sus credenciales.
- ✓ Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor, instando la revocación del certificado cuando dicha modificación constituya causa de revocación del mismo.
- ✓ Dejar de emplear el medio de identificación transcurrido el periodo de validez.
- ✓ Transferir a los poseedores de claves las obligaciones específicas de los mismos.
- ✓ No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de la Entidad de Certificación.
- ✓ No comprometer intencionadamente la seguridad de los servicios de certificación.
- ✓ No emplear las claves privadas correspondientes a las claves públicas contenidas en los certificados, con el propósito de firmar ningún certificado, como si se tratase de una Entidad de Certificación.

6 OBLIGACIONES DE TERCEROS QUE CONFÍAN

- ✓ Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- ✓ Conocer las condiciones de utilización de los certificados conforme a lo previsto en la Declaración de Prácticas de Certificación.
- ✓ Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- ✓ Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- ✓ Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de verificador.

- ✓ Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- ✓ Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.
- ✓ No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación, sin permiso previo por escrito de Izenpe.
- ✓ No comprometer intencionadamente la seguridad de los servicios de certificación.
- ✓ El usuario de certificados cualificados queda obligado a reconocer, en el debido instrumento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con eIDAS.

7 LIMITACIÓN DE RESPONSABILIDADES

Izenpe responderá,

- ✓ De los daños y perjuicios que cause a cualquier persona o entidad por la falta o retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados o de la extinción de la vigencia de los certificados.
- ✓ De los daños y perjuicios que cause a cualquier persona por la falta o retraso en la inclusión en el servicio de comprobación de la validez del mecanismo de identificación.
- ✓ Asimismo asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que delegue para el ejercicio de las funciones necesarias para la prestación de servicios de certificación. En este sentido se ha constituido un seguro de responsabilidad civil por importe de 3.500.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados.

Izenpe responderá por negligencia o falta de la debida diligencia en los servicios de certificación prestados así como cuando incumpla las obligaciones impuestas en la legislación sobre firma electrónica, excepto en los siguientes de daños causados por:

- ✓ Por las informaciones contenidas en los certificados, siempre que el contenido de los mismos cumpla sustancialmente con la Declaración de Prácticas de Certificación.
- ✓ Por la extinción de la eficacia de los certificados, siempre que cumpla sustancialmente con las obligaciones de publicación previstas en la Declaración de Prácticas de Certificación.
- ✓ Por el uso indebido o posterior a la revocación de los medios de identificación.
- ✓ No será responsable de ningún daño directo e indirecto, especial, incidental, emergente, de cualquier lucro cesante, pérdida de datos, daños punitivos, fuesen o no previsibles, surgidos en relación con el uso, entrega, licencia, funcionamiento o no funcionamiento de los Certificados, las firmas digitales, o cualquier otra transacción o servicio ofrecido o contemplado en la Declaración de Prácticas de Certificación en caso de uso indebido.
- ✓ Por los daños y perjuicios ocasionados al suscriptor o terceros de buena fe, por la inexactitud de los datos que consten en el certificado, si éstos le han sido acreditados mediante documento público notarial, judicial o administrativo, salvo en el caso del documento aportado por la Entidad de Registro.

Los daños y perjuicios ocasionados al suscriptor o a terceros de buena fe, por el incumplimiento de los deberes inherentes a la condición de suscriptor o terceros que confían en los certificados.

Cualquier organización distinta a Izenpe que actúe como Entidad de Registro será responsable frente a Izenpe por los daños causados en el ejercicio de las funciones que asuma, en los términos que se establezcan en el correspondiente instrumento legal.

8 ACUERDOS, DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y POLÍTICAS DE CERTIFICADO APLICABLES

Todos los acuerdos, DPC y Políticas aplicables se encuentran en www.izenpe.eus

9 POLÍTICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Información básica sobre protección de datos	
Responsable	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, SA.
Finalidad	Prestación y gestión de servicios asociados al certificado electrónico.
Derechos	Acceso, rectificación y cancelación a través ., c/ Beato Tomás de Zumárraga 71, 1ª planta 01008 Vitoria-Gasteiz.
Información adicional.	Declaración de Prácticas de Certificación de Izenpe.

Los datos de registro para la emisión o revocación de los certificados se mantienen en Izenpe durante 15 años para los certificados cualificados, o 7 años los no cualificados.

10 POLÍTICA DE REEMBOLSOS

Izenpe no dispone de una política de reintegro, y se acoge a la legislación vigente.

11 LEGISLACIÓN APLICABLE, MECANISMOS DE RESOLUCIÓN DE CONFLICTOS

11.1 Normativa aplicable

La ley española de firma electrónica se aplica en todo lo referente a la ejecución, elaboración, interpretación y validez de esta Declaración de Prácticas de Certificación. La normativa aplicable al presente documento, y a las operaciones que derivan de ellas, es la siguiente:

- ✓ Ley 59/2003, de 19 de diciembre, de firma electrónica.
- ✓ Ley 39-2015 Procedimiento Administrativo Común de las Administraciones Públicas
- ✓ Ley 40-2015 Régimen Jurídico Sector Público
- ✓ Ley 15/99 Orgánica de Protección de Datos (LOPD)
- ✓ Reglamento Europeo 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS)

11.2 Reclamaciones y resolución de disputas

Izenpe está sometida al sistema arbitral de consumo en los términos previstos en la legislación aplicable como medio para atender y resolver con carácter vinculante y ejecutivo para ambas partes, las quejas o reclamaciones de los solicitantes o suscriptores en el caso de los certificados de ciudadanos.

A tales efectos se considerará que el solicitante o suscriptor se acoge a dicho sistema desde el momento de la formalización de la solicitud de arbitraje ante la Junta Arbitral de Consumo que corresponda.

Cualquier otra cuestión litigiosa que pudiera surgir de los solicitantes o suscriptores en el ámbito de los certificados de ciudadanos no sometidos al sistema arbitral de consumo, quedará sometida a la jurisdicción competente.

12 AUDITORÍAS, CERTIFICACIONES Y SELLOS DE CONFIANZA DE LA AC Y LOS REPOSITORIOS

Con el objetivo de desarrollar e implantar eficazmente los servicios, Izenpe ha implementado un sistema de gestión de seguridad de la información para los procesos relacionados con los servicios de confianza, según el estándar ISO 27001.

Izenpe además sigue las indicaciones de los estándares de ETSI (Instituto Europeo de Estándares de Telecomunicaciones) y ha conseguido la certificación bajo las especificaciones técnicas de la norma EN 319 411-2 para la emisión de certificados cualificados, de la norma EN 319 411-1 para la emisión de certificados de clave pública, y de la norma EN ETSI EN 319 422 para la emisión de los sellos de tiempo. Estas normas son las exigidas por el Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS)

Para los certificados de servidor seguro que siguen la política de certificados de validación extendida (EVCP), para los certificados de servidor seguro que siguen la política de validación de la organización (OVCP) y para los certificados de servidor seguro que siguen la política de validación del dominio (DVCP) se siguen además las guías aprobadas por el CA/Browser Forum, disponibles en www.cabforum.org.

Todas las acreditaciones están disponibles para su consulta en www.izenpe.eus

13 CONTROL DE VERSIONES

Versión inicial.

IZENPE S.A.

Digitally signed by IZENPE S.A.
DN: cn=IZENPE S.A., c=ES, o=IZENPE S.A.
Date: 2017.06.02 08:56:28 +02'00'