Subsecretaría de Economía y Empresas de Menor Tamaño

Gobierno de Chile

160014318
1106777186
División Jurídica - DJVP

ORD. N°: 5007 27 JUN 2018

MAT.: Emite pronunciamiento a solicitud de BPO-Advisors SpA.

ANT: Carta de 15 de mayo de 2018, de don Marcelo Mora Saa, Gerente General BPO-Advisors.

ADJ.: Informe Custodia de Certificado Privado en HSM.

Santiago,

DE: IGNACIO GUERRERO TORO
SUBSECRETARIO DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO

A: MARCELO MORA SAA
GERENTE GENERAL
BPO – ADVISORS SPA

Por medio de la presente, me permito dar respuesta al pronunciamiento solicitado por usted mediante carta de 15 de mayo de 2018.

En dicha comunicación solicitó un pronunciamiento de esta Subsecretaría, respecto a la implementación de un procedimiento de emisión de firma electrónica avanzada de los usuarios utilizando la tecnología de HSM, con uso de PIN bajo exclusivo control del suscriptor de los certificados electrónicos.

Sobre el particular, puedo informar a usted que dicha solicitud ha sido analizada por el Encargado de la Entidad Acreditadora, emitiendo un Informe de "Custodia de Certificado Privado en HSM", que adjunto a la presente comunicación.

En dicho informe, se analiza la solicitud de la empresa BPO – Advisors, concluyendo que la firma electrónica avanzada custodiada en un HSM cumple con las normas técnicas requeridas, siempre que se observen las siguientes recomendaciones:

1. Esta modalidad debe incluirse de manera explícita en la Política de Certificación (CP – requisito PO01).
2. Esta modalidad debe incluirse de manera explícita en la Declaración de Prácticas de Certificación (CPS – requisito PO02).
3. En el contrato que se suscriba con el firmante, debe incluirse una cláusula de custodia de la clave privada. Se requiere un PIN de acceso y un PIN para firmar, este último es similar al que se le solicita al firmante cuando hace uso de un eToken.

4. El enrolamiento debe ser presencial o con prueba de vida y lo debe realizar un enrolador capacitado por el PSCA.
5. El enlace entre el cliente intermedio (empresa u organismo estatal) que facilita la plataforma y/o aplicación al firmante (cliente final), debe contar con cifrado (tipo VPN).
6. Los flujos de información entre el cliente intermedio (empresa u organismo estatal) y el PSCA deben estar cifrados (HTTPS).
7. La comunicación y flujo de información entre el cliente intermedio (empresa u organismo estatal) y el cliente final (firmante) deben estar cifrados.
8. La capacitación de los enroladores debe realizarla el PSCA, debiendo actualizarla anualmente o en caso de actualización de la plataforma tecnológica. Debe realizar una auditoría anual del proceso de enrolamiento, guardando los medios de prueba para presentarlos en la Inspección Anual Ordinaria.

Sin otro particular, saluda atentamente a usted,

REPUBLICA DE CHILE
SUBSECRETARIA DE ECONOMIA Y EMPRESAS DE MENOR TAMAÑO
SUBSECRETARIO

IGNACIO GUERRERO TORO
SUBSECRETARIO DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO

GABINETE SUBSECRETARIO ECONOMIA Y E.M.T.
JEFE DE GABINETE

DISTRIBUCIÓN:
- Destinatario (Kennedy N° 7100, oficina 610, Vitacura, Santiago)
- Gabinete Subsecretario
- Entidad Acreditadora
- División Jurídica
- Oficina de Partes

SUBSECRETARIA DE ECONOMIA CHILE
ENCARGADA ADMINISTRACION

REF: Solicita pronunciamiento a nuevo procedimiento para otorgar firma electrónica avanzada como servicio a los usuarios de la empresa BPO-Advisors SpA como Prestadora de servicios de certificación de firma electrónica.

Santiago, 15 de Mayo de 2018.

A: IGNACIO GUERRERO TORO,

SUBSECRETARIA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO

DE: MARCELO MORA SAA,

GERENTE GENERAL BPO-ADVISORS

Por medio de la presente, y de acuerdo a lo establecido en el artículo 18 de la ley 19.799, y en el artículo 18 del Decreto 181 de 2002, del Ministerio de Economía, Fomento y Turismo, vengo en solicitar a usted, en su calidad de Entidad Acreditadora de Firma Electrónica Avanzada, tener por presentada la solicitud de la empresa BPO-Advisors SpA, para implementar un nuevo procedimiento de emisión de firma electrónica avanzada de nuestros usuarios utilizando la tecnología de HSM con uso de PIN bajo exclusivo control del suscriptor de los certificados electrónicos, de acuerdo a los requisitos de la ley y el reglamento.

Antecedentes del Solicitante:

1. **Razón Social:** BPO-Advisors SpA.
2. **Rut:** 76.610.718-4.
3. **Representante Legal:** Marcelo Mora Saa.
4. **Rut del Representante Legal:** 10.407.742-0.
5. **Domicilio Social:** Kennedy N°7100 Oficina 610, comuna de Vitacura, Santiago.
6. **Dirección de Correo Electrónico:** marcelo.mora@bpo-advisors.net

Documentos que se acompañan:

1. Procedimiento Técnico de emisión de certificados bajo servicio de HSM.

Sin otro particular, y esperando una buena acogida de la presente solicitud se despide atentamente:

MARCELO MORA SAA

GERENTE GENERAL, BPO-ADVISORS

Firma Avanzada como Servicio

Antecedentes

Junto con solicitar un pronunciamiento sobre esta práctica, se solicita incorporar en nuestra declaración de prácticas de certificación, un procedimiento adicional para emitir certificados electrónicos de firma avanzada, donde el entorno de creación de firma electrónica es administrado por un proveedor de servicios de confianza en nombre del firmante.

El Articulo 2 de la Ley 19.799 define la Firma electrónica avanzada como "aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, y h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica."

El procedimiento de emisión certificados de firma avanzada en modalidad de servicio propuesto por BPO Advisors, delega la custodia de los certificados en el PSC IDOK (BPO Advisors) en un dispositivo criptográfico HSM (FIPS PUB 140-2), previniendo su pérdida o uso inadecuado y da acceso al uso de manera exclusiva al suscriptor mediante PIN privado bajo su exclusivo control.

Al respecto deseamos someter a la entidad acreditadora su pronunciamiento sobre el procedimiento de creación y custodia de los certificados electrónicos de firma avanzada creados en HSM modalidad como servicio, por el PSC acreditado BPO Advisors.

Para el desarrollo del servicio, se da cumplimiento a lo establecido por las Normas Técnicas de la Entidad Acreditadora:

Prácticas de Certificación:

- ETSI TS 102 042 V1.1.1 (2002-04).Technical Specification. Policy requirements for certification authorities issuing public key certificates.
- NCh2805.Of2003 Tecnología de la Información – Requisitos de las políticas de las autoridades certificadoras que emiten certificados de claves públicas.
- ETSI TS 102 042 V1.2.2 (2005-06).RTS/ESI-000043.Keywords e- commerce, electronic signature, public key, security.
- ETSI TS 102 042 V2.1.1 (2009-05).Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 042 V2.1.2 (2010-04) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

Seguridad:

- NCh27002.Of2009 Tecnología de la información – Código de práctica para la gestión de seguridad de la información.
- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (Mayo 2001).
- NCh.2820/1.Of2003 Tecnología de la información – Técnica de seguridad – Criterio de evaluación de la seguridad de TI – Parte 1: Introducción y modelo general.
- NCh2829.Of.2003 Tecnología de la Información – Requisitos de Seguridad para Módulos Criptográficos.

Estructura de Certificados:

- ISO/IEC 9594 – 8: 2005 Information Technology – Open Systems Interconnection – The Directory Attribute Certificate Framework. Correccion 2:2009.
- ITU – T Rec.X.690 (2002) / ISO/IEC 8825-1:2002. ASN.1 Basic Encoding Rules.
- NCh2798.Of2003 Tecnología de la Información – Reglas de codificación ASN.1 "Especificación de las reglas de codificación básica (BER) de las reglas de codificación canónica (CER) y de las reglas de codificación distinguida (DER).

Repositorio de Información:

- NCh2832.Of2003 Tecnología de la información – Protocolos operacionales de infraestructura de clave pública LDAPv2 para Internet X.509.
- RFC 2559 BOEYEN, S. et al., "Internet X.509 Public Key Infrastructure. Operational Protocols LDAPv2", Abril 1999.
- RFC 3377 LDAPv3: Technical Specification, September 2002, Lightweight Directory Access Protocol (v3): Technical.

ANEXO TECNICO

Procedimiento técnico para la emisión de certificados de firma avanzada en modalidad de servicio

La creación de firmas electrónicas avanzadas, se realiza en un entorno de creación de firma electrónica administrado por los servicios de confianza de la PSC IDOK y son utilizados bajo el exclusivo control del suscriptor. A continuación, se describe el ciclo de vida completo de la emisión de certificados de Firma Electrónica Avanzada IDOK.

SOLICITUDES

Todas las solicitudes de emisión deben comenzar con una primera instancia por parte del solicitante, mediante los tres canales dispuestos para ello: de forma presencial, mediante correo electrónico a contacto@idok.cl o mediante el formulario web dispuesto en la página psc.idok.cl.

Independiente del canal, la solicitud debe contener al menos tres datos:

- Rut del futuro suscriptor
- Email del futuro suscriptor
- Nombre Completo del futuro suscriptor

La PSC dará al solicitante las instrucciones para continuar con el procedimiento.

COMPROBACIÓN DE SOLICITUD

De manera interna, IDOK verificará que la evidencia generada en la solicitud de certificado de Firma Electrónica Avanzada sea veraz y exacta, utilizando todos los mecanismos, tecnologías o servicios tanto públicos como privados que tenga a su alcance.

Posterior a esto verificará que el suscriptor no tenga un certificado de firma Electrónica Avanzada IDOK vigente.

SOLICITUD ACEPTADA

Una vez confirmada la identidad del suscriptor se indicará al suscriptor mediante un canal electrónico seguro la creación del certificado y se solicitará el ingreso de un PIN de protección de la clave privada al interior del HSM.

El canal electrónico para emitir certificados en la modalidad de servicios, posee las siguientes características de seguridad para asegurar el exclusivo control del certificado por parte del suscriptor:

1. El PIN se encripta con la parte pública de una clave RSA generada dentro del HSM mediante wraping.
2. Al momento de generar la parte privada del certificado del usuario dentro del HSM, se desencripta el PIN del usuario utilizando la parte privada de la clave RSA de wraping

4. El servicio de firma envía el HASH del documento y el PIN encriptado al HSM.
5. El HSM desencripta mediante unwrap el PIN utilizando la parte privada de la clave RSA de wraping.
6. El HSM calcula la firma del documento obteniendo la parte privada del certificado del usuario que custodia utilizando el PIN.
7. El servicio de firmado inyecta la firma calculada en el documento y lo devuelve al usuario/sistema.
8. Respecto a las comunicaciones, todas las interacciones entre servidores se realizan con certificado SSL (HTTPS).

Ministerio de Economía Fomento y Turismo

Gobierno de Chile

Subsecretaría de Economía y Empresas de Menor Tamaño

Entidad Acreditadora de Firma Electrónica

Informe Custodia de Certificado Privado en HSM

Entidad Acreditadora
Ministerio de Economía, Fomento y Turismo
Gobierno de Chile

Contenido

Entidad Acreditadora
Ministerio de Economía, Fomento y Turismo
Gobierno de Chile

1. Antecedentes

De acuerdo a carta del 15 de mayo de 2018, dirigida al Sr. Ignacio Guerrero Toro – Subsecretario de Economía y Empresas de Menor Tamaño, remitida por el Sr. Marcelo Mora Saa – Gerente General del PSCA BPO-Advisors, se solicita el pronunciamiento de la Entidad Acreditadora respecto del procedimiento de emisión de Firma Electrónica Avanzada con custodia en un HSM bajo exclusivo control del firmante o suscriptor del certificado digital, de acuerdo a los requisitos de la Ley 19.799 y su reglamento (D.S. 181).

Se acompaña Procedimiento Técnico de emisión de certificados digitales custodiados en un HSM.

2. Marco Legal

Ley N°19.799, publicada el 12 de abril de 2002. Ministerio de Economía, Fomento y Reconstrucción. Subsecretaría de Economía, Fomento y Reconstrucción. Sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma.

Decreto Supremo N° 181. Aprueba Reglamento de la Ley 19.799 sobre documentos electrónicos, Firma Electrónica y la Certificación de dicha firma. Publicado el 17 de agosto de 2002. En particular las Disposiciones Transitorias.

3. Análisis

De acuerdo a los estándares referidos en las Disposiciones Transitorias del D.S. 181 del 17 de agosto de 2002, la clave privada debe quedar en un dispositivo que cumpla la norma FIPS 140-2 Nivel 3, lo que ocurre en el caso de los eTokens actuales así como por el HSM.

Se suma a lo anterior de que la clave privada debe quedar bajo la exclusiva custodia del firmante, lo que en este caso también se cumple, debido a la necesidad de ocupar un PIN para acceder.

En este caso, aplican:

- Ley N°19.799 Art. 17 a)
- Reglamento D.S. 181 Art. 17 a. y Disposiciones Transitorias

- Norma ETSI TS 102 042
- FIPS 140-2 L3

No obstante lo anterior, es necesario proteger las conexiones de red mediante cifrado (por ejemplo: usando VPN) y – además – se requiere que los datos viajen seguros por la red de punta a punta (o end to end), por lo que se requiere usar HTTPS (HTTP seguro), lo que también aplica a los "web-services".

4. Recomendaciones

1. Esta modalidad debe incluirse de manera explícita en la Política de Certificación (CP - requisito PO01).
2. Esta modalidad debe incluirse de manera explícita en la Declaración de Prácticas de Certificación (CPS – requisito PO02).
3. En contrato que se suscriba con el firmante debe incluir una cláusula de custodia de la clave privada. Se requiere un PIN de acceso y un PIN para firmar, este último es similar al que se le solicita al firmante cuando hace uso de un eToken.
4. El enrolamiento debe ser presencial o con prueba de vida, y lo debe realizar un enrolador capacitado por el PSCA.
5. El enlace entre el cliente intermedio (empresa u organismo estatal) que facilita la plataforma y/o aplicación al firmante (cliente final), debe contar con cifrado (tipo VPN).
6. Los flujos de información entre el cliente intermedio (empresa u organismo estatal) y el PSCA deben estar cifrados (HTTPS).
7. La comunicación y flujo de información entre el cliente intermedio (empresa u organismo estatal) y el cliente final (firmante) deben estar cifrados.
8. La capacitación de los enroladores debe realizarla el PSCA, debiendo actualizarla anualmente o en caso de actualización de la plataforma tecnológica. Debe realizar una auditoría anual del

proceso de enrolamiento. Debe guardar medios de prueba para presentarlos en la Inspección Anual Ordinaria.

5. Conclusión

De acuerdo al punto 3. Análisis y al punto 4. Recomendaciones, el personal técnico de la Entidad Acreditadora considera que la Firma Electrónica Avanzada custodiada en un HSM cumple con las normas técnicas requeridas siempre y cuando se apliquen las recomendaciones.

MARIO FERNANDO LEMUS VARAS

Firmado digitalmente por MARIO FERNANDO LEMUS VARAS
Fecha: 2018.06.26 11:26:52 -04'00'

Mario F. Lemus V.
Encargado Entidad Acreditadora

Subsecretaría de Economía y Empresas de Menor Tamaño

Gobierno de Chile

MEMORANDUM N° 160014318

A : **XIMENA VIAL**
Jefa División Jurídica

DE : **MARIO LEMUS**
Encargado Entidad Acreditadora

FECHA : SANTIAGO, 18 de junio 2018.

Junto con saludar, a través del presente solicito a Ud. Dar gestión a Solicitud Pronunciamiento para otorgar FEA de BPO-Advisors.

Se acompaña con informe (Adjunto).

Sin otro particular, saluda muy cordialmente,

MARIO FERNANDO LEMUS VARAS

Firmado digitalmente por MARIO FERNANDO LEMUS VARAS
Fecha: 2018.06.18 13:26:36 -04'00'

MARIO LEMUS
Encargado Entidad Acreditadora

ML/tp
Distribución
- Archivo Entidad Acreditadora
- Destinatario