DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)

OCSP

DPC DE LA ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, S.A.

INDICE

1. MARCO LEGAL

1.1. Base Legal

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento; Ley Orgánica de Defensa del consumidor, Ley Orgánica de Transparencia de la Información y Acreditación de CONATEL.

1.2. Vigencia

El presente documento entrará en vigencia a partir de la fecha de su aprobación.

1.3. Soporte Legal

a) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 577 de 17 de abril de 2002.

b) De conformidad con lo dispuesto en el Art. 37 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el Consejo Nacional de Telecomunicaciones es el Organismo de autorización, registro y regulación de las Entidades de Certificación de Información y Servicios Relacionados Acreditados.

c) Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedido mediante Decreto Ejecutivo No. 3496 publicado en el Registro Oficial 735 de 31 de diciembre de 2002, y reformas constantes en Decreto Ejecutivo 1356 de 29 de septiembre de 2008, publicadas en el Registro Oficial No. 440 de 6 de octubre de 2008.

d) Que, el segundo artículo enumerado agregado por el artículo 4 del Decreto Ejecutivo No. 1356 a continuación del artículo 17 del Reglamento General a la Ley de Comercio EJectr6nico, Firmas Electrónicas y Mensajes de Datos, dispone que la acreditación como entidad de certificación de información y servicios relacionados, consistirá en un acto administrativo emitido por el CONATEL a través de una resolución que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados.

e) Resolución 477-20-CONATEL-2008 de 08 de octubre de 2008, se aprobó el modelo de resolución para la Acreditación como Entidad de Certificación de Información y Servicios Relacionados.

f) Resolución No. TEL-640-21-CONATEL-2010 de 22 de octubre de 2010, aprobó la petición de Acreditación de la Compañía SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. como Entidad de Certificación de Información y Servicios Relacionados, para los cual la SENATEL suscribió el respectivo acto administrativo, conforme el modelo aprobado por el Consejo Nacional de Telecomunicaciones.

2. INTRODUCCIÓN

2.1. Presentación

El presente documento contempla la Declaración de Prácticas de Certificación (DPC) del servicio de OCSP de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

Esta DPC del servicio OCSP especifica y contempla lo establecido en la DPC de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL estableciendo un conjunto de reglas que indican los procedimientos seguidos por la Entidad de Certificación en la prestación de sus servicios para la solicitud del estado de un certificado por medio del servicio OCSP, así como los límites de uso, el ámbito de aplicación y las características técnicas de este tipo de servicio.

Esta Declaración de Prácticas de Certificación (DPC) del servicio de OCSP, junto con la DPC de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, están dirigidas a cualquiera que confíe en este tipo de servicio digital.

2.2. Nombre del Documento

2.2.1. Identificación

Nombre:	Declaración de Prácticas de Certificación (DPC)
Versión:	3.0
Descripción:	Servicio de OCSP
Fecha de Emisión:	14 de Diciembre 2012

2.2.2. Publicación

Este documento puede obtenerse libremente en la dirección electrónica https://www.securitydata.net.ec

2.3. Definiciones y Acrónimos

2.3.1. Definiciones

- **Certificado Electrónico:** Es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

- **Certificado Reconocido:** Certificado expedido por una Entidad Acreditada que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

- **Clave Pública y Clave Privada:** La criptografía asimétrica en la que se basa la PKI emplea un par de claves (podrían ser dos pares de claves), lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

- **Datos de Creación de Firma (Clave Privada):** Son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la firma electrónica.

- **Datos de Verificación de Firma (Clave Pública**): Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

- **Dispositivo Seguro de Creación de Firma (DSCF):** Instrumento que sirve para aplicar los datos de creación de firma.

- **Firma Electrónica**: Es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

- **Firma Electrónica Avanzada:** Es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

- **Función Hash:** Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

- **Listas de Certificados Revocados (CRL):** Lista donde figuran las relaciones de certificados revocados o suspendidos.

- **Módulo Criptográfico Hardware (HSM):** Módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

- **Sellado de tiempo:** Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

- **Autoridad de Sellado de Tiempo (TSA):** Entidad de confianza que emite sellos de tiempo.

- **Autoridad de Validación (VA**): Entidad de confianza que proporciona información sobre la validez de los certificados digitales y de las firmas electrónicas.

2.3.2.Acrónimos

AC:	Autoridad de Certificación
AC Sub:	Autoridad de Certificación Subordinada
AR:	Autoridad de Registro
PC:	Política de Certificación
DPC:	Declaración de Prácticas de Certificación
CRL:	Lista de Certificados Revocados (Certificate Revocation List)
HSM:	Módulo de seguridad criptográfico (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Infraestructura de Clave Public (Public Key Infrastructure)
PSC:	Prestador de Servicios de Certificación
TSA:	Autoridad de sellado de tiempo (Time Stamp Authority)
VA:	Autoridad de validación (Validation Authority)
ECI:	Entidad de Certificación de Información
OID:	Identificador de objeto único (Object identifier)
DN:	Nombre Distintivo (Dinstinguished Name)
C:	País (Country), Atributo del Nombre Distintivo
CN:	Nombre Común (Common Name), Atributo del Nombre Distintivo
O:	Organización (Organization), Atributo del Nombre Distintivo
OU:	Unidad Organizacional (Organizational Unit), Atributo del Nombre Distintivo
SN:	Apellido (SurName), Atributo del Nombre Distintivo
ISO:	International Organizational for Standarization
PKCS:	Public Key Cryptography Standars, Estándares PKI
UTF8:	Unicode Transformation Format – 8 bits.

3. ENTIDADES PARTICIPANTES

3.1. Entidad Acreditada (EA)

Security Data Seguridad en Datos y Firma Digital es un Entidad Acreditada (EA) que emite certificados reconocidos según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de

Datos. Security Data Seguridad en Datos y Firma Digital es la entidad emisora de los certificados y responsable de las operaciones del ciclo de vida de los certificados. Las funciones de autorización, registro, emisión y revocación respecto de los certificados personales de entidad final, pueden ser realizadas por otras entidades por delegación soportada contractualmente con Security Data Seguridad en Datos y Firma Digital, que actuarán como intermediarios. Security Data Seguridad en Datos y Firma Digital también ofrece servicios de validación de firmas electrónicas y de sellado de tiempo, regidos por sus políticas particulares, no incluidas en este documento.

3.2. Autoridad de Certificación (AC)

El sistema de certificación de Security Data Seguridad en Datos y Firma Digital está compuesto por diversas Autoridades de Certificación (en inglés CA o Certificate Authority) organizadas bajo una Jerarquía de Certificación.

3.2.1. Autoridad de Certificación Raíz

Se denomina Autoridad de Certificación Raíz (AC Root) a la entidad dentro de la jerarquía que emite certificados a otras autoridades de certificación, y cuyo certificado de clave pública ha sido autofirmado. Su función es firmar el certificado de las otras ACs pertenecientes a la Jerarquía de Certificación.

3.3. Autoridad de Registro (AR)

Una Autoridad de Registro (en inglés RA o Registration Authority) de Security Data Seguridad en Datos y Firma Digital, es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado
- Gestionar la generación de claves y la emisión del certificado
- Hacer entrega del certificado al suscriptor.

Podrán actuar como AR de Security Data Seguridad en Datos y Firma Digital:

- Cualquier Corporación que sea cliente de Security Data Seguridad en Datos y Firma Digital, para la emisión de certificados a nombre de la corporación o a miembros de la corporación.
- Cualquier entidad de confianza que llegue a un acuerdo con Security Data Seguridad en Datos y Firma Digital para actuar como intermediario en nombre de Security Data Seguridad en Datos y Firma Digital.
- La propia Security Data Seguridad en Datos y Firma Digital directamente.

Security Data Seguridad en Datos y Firma Digital formalizará contractualmente las relaciones entre ella y cada una de las entidades que actúen como AR de Security Data Seguridad en Datos y Firma Digital.

La entidad que actúe como AR de Security Data Seguridad en Datos y Firma Digital podrá autorizar a una o varias personas como Operador de la AR para operar con el sistema informático de emisión de certificados de Security Data Seguridad en Datos y Firma Digital en nombre de la AR.

Allí donde la ubicación geográfica de los suscriptores represente un problema logístico para la identificación del suscriptor y en la solicitud y entrega de certificados, la AR podrá delegar estas funciones a otra entidad de confianza. Dicha entidad deberá tener una especial vinculación con la AR y una relación de proximidad con los suscriptores de los certificados que justifique la delegación. La entidad de confianza deberá firmar un acuerdo de colaboración con la AR en el que se acepte la delegación de estas funciones. Security Data Seguridad en Datos y Firma Digital deberá conocer y autorizar de manera expresa el acuerdo.

3.4. Solicitante

Solicitante es la persona física que, en nombre propio o en representación de un tercero, solicita la emisión de un certificado a Security Data Seguridad en Datos y Firma Digital. Los requisitos que debe reunir un solicitante dependerán del tipo de certificado solicitado y estarán recogidos en la "Política de Certificación" de cada tipo de certificado concreto.

3.5. Suscriptor

El Suscriptor es la persona física o jurídica que ha contratado los servicios de certificación de Security Data Seguridad en Datos y Firma Digital. Por lo tanto será el propietario del certificado. En general, el suscriptor de un certificado de Security Data Seguridad en Datos y Firma Digital será una Corporación (empresa privada, entidad pública, persona física), la identidad de la cual aparecerá en el propio certificado.

3.6. Firmante

El Firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona jurídica a la que representa.

El Firmante será responsable de custodiar los datos de creación de firma, es decir, la clave privada asociada al certificado.

3.7. Custodio de las Claves

La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico

3.8. Tercero que confía en los Certificados

Se entiende como tercero que confía en los certificados (en inglés, relaying party) a toda persona u organización que voluntariamente confía en un certificado emitido por Security Data Seguridad en Datos y Firma Digital.

Los certificados reconocidos emitidos por Security Data Seguridad en Datos y Firma Digital tienen carácter universal y están aceptados por la mayoría de los organismos públicos del estado ecuatoriano, como Ministerios, Secretarías ,etc.

Las obligaciones y responsabilidades de Security Data Seguridad en Datos y Firma Digital con terceros que voluntariamente confíen en los certificados se limitarán a las recogidas en la DPC de Security Data Seguridad en Datos y Firma Digital.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

4. OCSP

El servicio de Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado de forma actualizada, rápida y segura. El servidor OCSP responde a las consultas de validez de un certificado, enviando una respuesta firmada sobre el estado del mismo.

El usuario que quiera consultar el estado de un certificado crea una petición OCSP que contiene una huella de la llave pública del firmante. Esta petición es enviada a la autoridad de validación que viene a ser Security Data S.A

El "OCSP responder" busca el estado de revocación del certificado del firmante, usando la huella que creó el usuario que envió la consulta, en la base de datos de Security Data S.A. Si el certificado ha sido revocado, esta será la única localización de confianza donde ese hecho será registrado.

En cualquier caso el "OCSP responder" devuelve una respuesta OCSP firmada para comunicar el estado del certificado consultado.

Este servicio cumple con los estándares RFC 2560 y RFC 5019 y soporta más de 500 solicitudes por segundo.

4.1. ¿Cómo se solicita el servicio de OCSP?

Este servicio no tiene costo para el usuario, simplemente se debe configurar el servidor o software cliente para que busque el siguiente enlace:

URL: http://ocspgw.securitydata.net.ec/ejbca/publicweb/status/ocsp

Este enlace permite redireccionar la solicitud del servicio OCSP hacia los servidores internos de Security Data para brindar el servicio mencionado.

4.2. ¿Cómo se solicita el estado de un certificado por medio de OCSP?

Para solicitar el servicio de OCSP simplemente se debe configurar el servidor o software cliente para que busque uno de los siguientes enlaces

- URL: http://ocspgw.securitydata.net.ec/ejbca/publicweb/status/ocsp

Los certificados de Security Data S.A. están configurados en su Punto de Distribución para que el estado sea verificado además de en la CRL, en el servidor OCSP.

5. REVISIONES

Documento: Declaración de Prácticas de Certificación/OCSP					
Revisión	**1**	**2**	**3**	**4**	**5**
Publicado	**01/08/2011**	**09/11/2012**	**14/12/2012**		
Autor(es)	**XC**	**LV**	**LV**		
Fecha de revisión					
Revisado por					
Fecha aprobado					
Aprobado por					