ENTIDAD CERTIFICADORA RAÍZ DEL ESTADO PLURINACIONAL DE BOLIVIA

AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES - ATT

LINEAMIENTOS PARA TERCEROS ACEPTANTES QUE ACTÚEN EN EL MARCO DE LA INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN DIGITAL DEL ESTADO PLURINACIONAL DE BOLIVIA - LT

Datos del documento	
Título del documento	Lineamientos para terceros aceptantes que actúen en el marco de la Infraestructura Nacional de Certificación Digital del Estado Plurinacional de Bolivia
Identificador documental	ECR-Lineamientos para Terceros (LT)
Criticidad:	Alta
Fecha	13 de noviembre de 2018
Autor	ATT
Versión	2.0
Comentario	
Publicación	Público

I-LP-15466

Noviembre 2018

CONTENIDO

I-LP-15466

1. ÁMBITO DE APLICACIÓN

El presente documento contiene los lineamientos generales que deben seguir los terceros aceptantes que actúen en el marco de la Infraestructura Nacional de Certificación Digital de Bolivia – INCD, cuando verifiquen la validez de las firmas digitales.

En su redacción se han tenido en cuenta lo establecido enlos "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente, en el Decreto Supremo N° 1793, así como los estándares RFC 3647 y 5280 del IETF (Internet Engeneering Task Force) e ITU-T X.509, entre otros, y las buenas prácticas y experiencias internacionales en la materia.

Cabe aclarar en cuanto a la figura del tercero aceptante, que la Declaración de Prácticas de Certificación, introduce esta figura como uno de los participantes de la PKI (Infraestructura de Claves Públicas, por sus siglas en inglés).

A la luz de esta incorporación y de las experiencias normativas internacionales, un tercero aceptante puede ser definido comola persona natural o jurídica que recibe un documento firmado digitalmente y que debiendo verificar dicha firma digital, realiza una serie de acciones, entre las cuales se encuentra la generación de una consulta para corroborar la validez del certificado digital correspondiente.

2. OBJETIVO GENERAL Y ALCANCE

Es objetivo de este documento es establecer los lineamientos técnicos generales relativos a los pasos necesarios que debe seguir un tercero aceptante para validar una firma digital, desde la perspectiva tanto de un tercero aceptante individual como la de un sistema informático que realice dicho proceso en forma automática.

Se aclara que el presente documento no constituye una guía exhaustiva de los procesos técnicos que se desarrollan a partir de la voluntad de un tercero aceptante de validar una firma digital.

Su alcance es la identificación de los principales aspectos técnicos a tener en cuenta al momento de desarrollar los procedimientos específicos que un tercero aceptante individual o una aplicación deben seguir para validarlas firmas digitales y los certificados correspondientes.

3. RESPONSABILIDADES GENERALES

Las responsabilidades de cumplimiento de lo indicado en este documento corresponden a todo aquel que deba determinar la validez de una firma digital y de los certificados involucrados, en el marco de la INCD del Estado Plurinacional de Bolivia. Comprende también a los responsables de desarrollos informáticos de cualquier naturaleza, que tengan por objetivo realizar las verificaciones antes mencionadas de manera automática.

I-LP-15466

4. DESPLIEGUE Y DESARROLLO

4.1 ASPECTOS GENERALES

La validación de una firma digital y de los certificados involucrados, comprende las siguientes verificaciones:

a. Que los certificados involucrados hayan sido emitidos usando los formatos y contenidos establecidos en el marco legal aplicable a la INCD;

b. Que la firma digital haya sido generada durante el período de vigencia del certificado correspondiente y cuando éste no se encontraba revocado;

c. Que el certificado que contiene la clave pública correspondiente a la firma digital que se pretende verificar fue emitido por una Entidad Certificadora Autorizada – ECA, en el marco de la INCD de Bolivia y que la cadena de verificación correspondiente pueda ser apropiadamente verificada.

d. Que el certificado y las claves están siendo utilizados dentro de los usos permitidos en la Política de Certificación correspondiente.

A continuación, se describen con mayor detalle los pasos de verificación señalados.

4.2 VALIDACIÓN LOCAL DEL CERTIFICADO

Este primer paso comprende la verificación de la validez de un certificado digital que es efectuada localmente, es decir sin necesidad de recurrir a entidades externas.

Generalmente es realizada en forma automática por el sistema informático involucrado, ya sea que se trate de un producto comercial adquirido, como puede ser el caso de un cliente de correo electrónico, o como un desarrollo particular realizado con un fin específico.

En líneas generales, comprende los siguientes pasos:

a. Corroboración de que el certificado es un documento en notación ASN.1

b. Verificación de que su estructura se corresponde con un certificado X.509

c. Obtención del contendido del campo *Nombre Distintivo* (DISTINGUISHED NAME) de la entidad emisora (ISSUER) y opcionalmente, de la extensión *Identificador de la clave de la Autoridad* (AUTHORITY KEYIDENTIFIER), para acceder al certificado de la Entidad Certificadora Autorizada - ECA que lo emitió (ver punto siguiente respecto a la cadena de certificación). Esto último se puede realizar accediendo al almacén de certificados de la instalación utilizada o bien, bajándolo del sitio de la ECA o de la Entidad Certificadora Raíz – ECR.

d. Obtención de la clave pública contenida en el certificado para verificar la firma digital.

Si como resultado de los pasos antes indicados, la verificación es exitosa, se concluye que el certificado presentado fue emitido por una ECA de la INCD del Estado Plurinacional de Bolivia y por lo tanto, es válida.

I-LP-15466

Si en cambio, algunos de los pasos descritos arrojan un resultado erróneo debe rechazarse la firma digital por inválida.

4.3 VALIDACIÓN DE LA CADENA DE CERTIFICACIÓN

Para la validación de la cadena de certificación, es decir la verificación de que los certificados digitales son válidos, debe controlarse o verificarse lo siguiente para el certificado correspondiente a la firma digital del documento o transacción:

- Ha sido emitido por una ECA,
- Que el certificado se encuentra dentro de su período de vigencia
- Que no se encuentre revocado ni suspendido

Respecto al certificado de la ECA se debe corroborar que:

- Ha sido emitido por la ECR de la INCD,
- Que el certificado se encuentra dentro de su período de vigencia
- Que no se encuentre revocado

En ambos casos corresponde la verificación de las correspondientes Listas de Certificados Revocados - CRL, por sus siglas en inglés, tanto de la ECA que emitió el certificado digital como de la ECR.

Cabe añadir que en el largo plazo, la verificación de una firma digital implica la determinación de que la misma fue producida durante el plazo de vigencia del certificado digital, considerando su eventual revocación o suspensión. Esto implica la disposición de mecanismos tales como los sellos de tiempo ("time stamps") y de estándares de conservación en el largo plazo de documentación electrónica firmada digitalmente.

Alternativamente puede recurrirse a otros mecanismos indirectos, como la prueba de que un documento fue aceptado por un sistema solo en razón de que en su momento se pudo realizar tales verificaciones. Sin embargo, estos mecanismos pueden resultar más complejos a la hora de ofrecerlos como prueba.

Otra cuestión a tener en cuenta, es que se debe verificar si se trata de un certificado emitido para un usuario final (persona natural o jurídica o de cargo) o para una entidad certificadora. Para el utilizado para verificar la firma digital del documento o de la transacción, debe corroborarse el primer caso mientras que, a lo largo de toda la cadena de confianza, que cada certificado involucrado es un certificado de Entidad Certificadora.

Esta información surge del propio certificado digital, bajo la extensión Restricciones Básicas (*basic Constraints*) y se la identifica con la sigla CA.

Por consiguiente, si CA=True, entonces se trata de un certificado de una entidad certificadora y su suscriptor se encuentra habilitado para emitir certificados. Son los casos de la ECR y la ECA. Si en cambio CA=False, entonces no puede ser usado para emitir certificados. Como consecuencia, la validación de una cadena de confianza con un certificado intermedio que contenga el valor CA=False debe ser rechazada y lo mismo ocurriría en el caso de un certificado de persona natural o jurídica o de cargo, si CA=True.

I-LP-15466

4.4 VALIDACIÓN DEL USO DEL CERTIFICADO

Dentro de las Políticas de Certificación de la ECR y de una ECA, se establece que se deberán detallar los usos permitidos para dichos certificados, así como también, las restricciones impuestas a tal utilización.

En consiguiente, se interpreta que cada Política de Certificación de una ECA bajo la cual se emiten determinados certificados tiene asociado una serie de usos específicos, que deben ser corroborados y verificados por el tercero aceptante antes de dar por válida una firma digital. Esto es así ya que un uso no permitido podría invalidar la firma, restando validez jurídica al documento o a la transacción con la cual se encuentra vinculada.

Para revisar si el uso se encuentra dentro de lo permitido, el tercero aceptante debe tener acceso a la Política de Certificación correspondiente. Para ello, el propio certificado digital involucrado contiene la extensión Políticas de Certificación (*certificate Policies*) que contiene un enlace (URI) de Internet donde se encuentra publicada la Política de Certificación.

Adicionalmente, el tercero aceptante debe verificar una serie de datos que también se encuentran en el certificado digital, con el fin de determinar si el uso que se le está dando corresponde con el contexto en el que está siendo empleado.

En este sentido, se debe validar la extensión Uso de Claves (*keyUsage*) que se define como un campo crítico para todos los certificados que describe los usos permitidos de la clave pública mediante la habilitación o deshabilitación de una serie de campos.

En otras palabras, en esta extensión se registran una serie de bits que al encontrarse habilitados tomando el valor "1", se permiten usos para la clave pública incluida en el certificado. Dichos usos se registran a través de los siguientes atributos, de acuerdo a lo indicado en el artículo referido en el párrafo anterior, que a su vez refleja el texto del RFC 5280 y son los siguientes:

- digitalSignature: Utilizado para verificar la firma digital en procesos de autenticación de entidades, autenticación de datos y de integridad.
- nonRepudiation: Utilizado para proporcionar un servicio de no repudio que proteja la firma contra la denegación por parte del firmante.
- keyEncipherment: Utilizado para cifrar claves u otra información de seguridad.
- dataEncipherment: Utilizado para cifrar datos de usuario, pero no claves u otra información de seguridad
- keyAgreement: Utilizado para indicar que se utiliza la clave pública para realizar un acuerdo de claves
- keyCertSign: Utilizado para indicar que se utiliza la clave pública para verificar las firmas en los certificados

I-LP-15466

- cRLSign: Utilizado para indicar que la clave pública es empleada para la verificación de firmas en las listas de revocación de certificados

- encipherOnly: Utilizada para cifrar los datos durante la realización de un acuerdo de claves

- decipherOnly: Utilizada solo para descifrar los datos durante la realización de un acuerdo de claves

Al respecto y dentro del marco de la INCD según lo establecen los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente, según el tipo de certificado, estos bits deben reflejar lo siguiente:

Tipo de certificado	Uso de clave
ECR	keyCertSign = 1, cRLSign = 1
ECA	keyCertSign = 1, cRLSign = 1
Persona Natural	digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 1, dataEncipherment = 1
Persona Jurídica	digitalSignature = 1, nonRepudiation = 1, keyEncipherment = 1, dataEncipherment = 1

Finalmente, otra extensión a tener en cuenta es la denominada Uso de claves extendido (*extendedKeyUsage*). Esta extensión describe usos adicionales a los antes mencionados, mediante la habilitación de distintos atributos. De acuerdo al estándar RFC 5280, pueden usarse los siguientes:

- Autenticación de SSL/TLS en modo servidor (Certificado de Sitio) - serverAuth
- Autenticación de SSL/TLS en modo cliente - clientAuth
- Firma de código - codeSigning
- Autenticación, firma y cifrado de correo electrónico - emailProtection
- Firma de Sellos de Tiempo (Timestamping) - timeStamping
- Firma de respuestas para el Protocolo de en línea del estado de un certificado (OCSP) -
- OCSPSigning

En los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigentese toman los siguientes valores:

Tipo de certificado	Uso extendido de clave
Persona Natural	clientAuth, EmailProtection
Persona Jurídica	clientAuth, EmailProtection, serverAuth

I-LP-15466

5. LISTA DE CERTIFICADOS REVOCADOS

Las listas de certificados son archivos digitales que contienen la lista con los números de serie de los certificados muestran el estado del certificado a los fines de su verificación, como revocado. Las listas de revocación son obligatorias las ECA deben implementar servicios de validación del estado del certificado en línea (OCSP), dada la criticidad de las operaciones y su utilización en tiempo real de forma permanente.

6. REVISIÓN Y ACTUALIZACIÓN DEL DOCUMENTO

Estos lineamientos serán revisados al menos una vez al año, salvo consideraciones contrarias tomadas por la ATT en su calidad de ECR en las que requiera hacerlo antes, por razones operativas, originadas en un cambio tecnológico o vinculadas a un cambio de normativa aplicable.

7. REFERENCIAS NORMATIVAS COMPLEMENTARIAS

El presente documento complementa los "Estándares Técnicos y otros Lineamientos establecidos para el funcionamiento de las Entidades Certificadoras" aprobados por la Resolución Administrativa Regulatoria vigente y demás normativa aplicable y ha sido elaborado teniendo en cuenta los estándares internacionales citados precedentemente.

I-LP-15466