Lineamientos para Terceros Aceptantes

Especificaciones Técnicas

Versión 1.1

Unidad de Certificación Electrónica

Infraestructura Nacional de Certificación Electrónica
República Oriental del Uruguay

Unidad de Certificación Electrónica

Índice

Unidad de Certificación Electrónica

1.Introducción, Objetivos y Alcance

La Unidad de Certificación Electrónica (UCE), en su Resolución N° 07/012, de 26 de diciembre del 2012, define los controles que un tercero aceptante debe realizar para aceptar una firma electrónica avanzada o, más precisamente, aceptar el certificado electrónico con el que una firma fue producida. Dichos controles se enuncian en modalidad declarativa, estableciendo así su necesidad, pero no los pasos necesarios para realizar cada uno de ellos.

El presente documento tiene como objetivo entonces establecer los lineamientos técnicos generales que son necesarios para realizar estas validaciones, desde la perspectiva de un desarrollador de sistemas que realicen las mismas. Si bien no pretende ser una especificación de requerimientos técnicos exhaustivos, sí otorga una guía de qué cosas se deben tener en cuenta al momento de construir un software de validación de certificados, o al utilizar uno en modalidad de usuario final.

El alcance del mismo comprende cualquier firma electrónica u operación de autenticación que se base en un Certificado Electrónico Reconocido dentro de la Infraestructura Nacional de Certificación Electrónica. Si bien los lineamientos pueden aplicar en la mayoría de los casos, no se encuentran estrictamente dentro del alcance las operaciones que se basen en certificados electrónicos fuera de la INCE.

Unidad de Certificación Electrónica

2.Comprobaciones

En la presente sección se especifican los pasos necesarios a seguir para realizar cada una de las comprobaciones que la UCE requiere en la citada resolución. No necesariamente cada una de las subsecciones se corresponden con una de las comprobaciones de la UCE, por motivos de claridad algunas se han agrupado.

2.1.Estructura y pertenencia a la INCE

El certificado es válido y fue emitido por un PSCA de la INCE.

Esta comprobación es la más básica de todas, porque se realiza localmente sobre el certificado. En la mayoría de los casos es realizada por el sistema informático en forma completamente automática, rechazando completamente el certificado si fallan estos controles. Implica realizar las siguiente comprobaciones:

1. Interpretar el certificado como un documento en notación ASN.1, y verificar que su estructura es X.509.

2. Obtener el campo ISSUER y opcionalmente la extensión AUTHORITY KEY IDENTIFIER, y con esos datos encontrar el certificado del PSCA emisor del certificado presentado dentro del almacén de certificados del equipo. En algunos casos, y dependiendo del formato de firma utilizado en el documento, puede que el certificado del PSCA ya se encuentre en el mismo y no sea necesario buscarlo. De todas formas, esto no invalida las siguientes comprobaciones.

3. Obtener la clave pública del certificado del PSCA emisor, y utilizarla para realizar una verificación de la firma del certificado presentado. Si la verificación es exitosa, se puede concluir que el certificado presentado fue emitido por el PSCA y por lo tanto, es legítimo.

Si el PSCA no es conocido (su certificado no está en el almacén), entonces es necesario repetir el proceso del punto 2 pero con el certificado de la ACRN como emisor, para verificar que sea un PSCA de la INCE.

2.2.Vigencia según fechas

La fecha de validación del certificado debe ser posterior a la fecha de entrada en vigencia del certificado y anterior a la de expiración.

Para validar la fecha simplemente se deben tomar los campos VALID FROM y VALID TO, y verificar que la fecha de la firma esté dentro de ese rango. Si está fuera, directamente no se debe considerar como una firma válida, por haber sido producida con un certificado expirado o con uno que aún no había entrado en vigencia.

La fecha en la que interesa validar el certificado es en general la fecha en la que se declara haber firmado el documento. Esto es seguro siempre y cuando la fecha en que se realiza la validación también esté dentro del rango de validez del certificado, porque se conoce que el mismo no ha expirado en el presente. Cuando la fecha de validación está dentro del rango de validez, pero la fecha actual no lo está, se deben tener consideraciones adicionales para asegurarse que la firma no fue producida con un certificado vencido, a saber:

1. Si la firma contiene un *token* de una autoridad de timestamp, garantizando que el documento fue firmado en el momento en que declara haberlo sido, entonces se está ante una *Firma Longeva*, y sólo importa que la fecha de firma declarada esté dentro del período de validez del certificado, no importa la fecha actual.

2. Si la firma no contiene este *token*, a priori no se la debería validar, pues no hay garantías de que la fecha declarada sea real. De todas formas, si se cuenta con algún tipo de evidencia de que el documento fue validado en el pasado, en algún momento en que el certificado estuviera vigente, entonces se puede validar esa firma, en la medida en que se confíe en esa evidencia. Un ejemplo de esto es una bandeja de entrada de documentos que hace validación de firmas en el ingreso, y una revisión posterior que los procesa algunos meses después. Para la revisión posterior alcanza con la evidencia del sistema de validación de entrada para confiar en la firma realizada.

3. Si no se tiene *token* de tiempo, ni ninguna evidencia asociada a una validación previa, entonces la firma no debe validarse, puesto que puede haber sido realizada con un certificado expirado y descuidado por su suscriptor, y falsificada la fecha de firma.

Estos controles se ralizan comúnmente en forma asistida, es decir, existe un sistema informático que procesa las fechas e informa de los resultados al usuario. Si se está en uno de los primeros casos más sencillos, el sistema marca sólo su conformidad, pero si se está en alguno de los segundos tres, éste informa al usuario de la situación, para que tome la decisión en base a la información que le provee.

2.3.Estado de revocación

El certificado no se encuentra revocado en la última CRL emitida por el PSCA a la fecha de la validación, o el servicio de validación online OCSP provisto por el PSCA lo reporta como válido.

Los certificados se emiten por los PSCA y se distribuyen libremente, no teniéndo más control sobre los mismos de parte del prestador. Para solucionar situaciones de compromiso de claves, contravención de las normas de uso, etc, existe el mecanismo de revocación. Mediante esta operación, el PSCA termina prematuramente la validez del certificado, y además publica información y servicios para que al realizar las validaciones se pueda consultar este estado.

Dependiendo del prestador, y de los servicios contratados con el mismo, se puede realizar la validación mediante Lista de Revocación (CRL) u OCSP (Online Certificate Status Protocol):

1. Validación por CRL

    1.1. En el certificado, se obtiene de la extensión CRL DISTRIBUTION POINT, la URL donde el prestador publica la CRL. Es posible también tener configurado en un sistema en forma previa esta URL, ya que no debería cambiar con frecuencia.

1.2. Desde esa URL se descarga la última lista de revocación, que se almacena temporalmente.

1.3. Se interpreta la CRL para verificar que esté en sintaxis ASN.1 y formato X.509, y que además esté vigente comparando la fecha actual con la fecha de expiración que contiene.

1.4. Usando el certificado del PSCA, de la misma forma que se realiza en el punto 2.1, se valida la firma electrónica de la CRL, para verificar que fue efectivamente emitida por ese PSCA.

1.5. Una vez autenticada la CRL, se obtiene el SERIAL NUMBER del certificado que se está validando, y se lo busca en la CRL. Si está presente, entonces tendrá asociada una fecha de revocación y, opcionalmente, un código de motivo.

2. OCSP

2.1. En el certificado se obtiene la extensión AUTHOTITY INFORMATION ACCESS (aunque en algunos casos puede ser CRL DISTRIBUTION POINT también), y de ella la URL donde se encuentra publicado el servicio OCSP del emisor.

2.2. Se construye una consulta OCSP incluyendo el número de serie del certificado, obtenido desde el campo SERIAL NUMBER del mismo, y se la envía al servicio, quien realiza la validación y retorna un mensaje firmado electrónicamente por la autoridad de validación.

2.3. Se verifica la firma del mensaje de respuesta, junto con el certificado de la autoridad de validación, siguiendo los mismos pasos de este documento. Si la firma es correcta, se examina la respuesta para ver el estado de revocación del certificado consultado.

Si la fecha de revocación es anterior a la fecha de la firma, no se debe validar la misma. Si por el contrario es posterior, se debe tener en cuenta que la fecha de revocación no necesariamente implica que el compromiso de claves se dio en ese momento, puede

haber sido anterior y se está asumiendo un riesgo en este sentido. Lo que es peor, si se revocó por un compromiso de claves, se pueden producir documentos con fechas falsificadas, por lo que salvo alguna excepción muy particular, no se debería validar las mismas. En general los sistemas informáticos resuelven completamente las operaciones desde el punto 1.1 al 1.5 de la CRL y 2.1 a 2.3 del mecanismo OCSP, y se le da la información necesaria para que el usuario tome la decisión relativa a la validación, para lo cual se deben tener en cuenta los riesgos planteados.

2.4.Estado de la Cadena de Confianza

El certificado del PSCA emisor es válido de acuerdo con la Política de Certificación de la ACRN y *El certificado de la ACRN es válido.*

De la misma forma en que se valida el certificado con el que se produjo una firma que se está validando, también es necesario validar los certificados utilizados para firmar el certificado presentado, realizando lo que se denomina la validación de la cadena de confianza.

Una vez obtenido el certificado del PSCA emisor del certificado presentado, se realizan las mismas comprobaciones en este documento expuestas sobre él, en un proceso recursivo. Como a su vez ese certificado fue emitido por el de la ACRN, se debe realizar también una validación de éste. La diferencia en este paso base es que el certificado de la ACRN es *autofirmado*, es decir, no existe la validación de su emisor y, por lo tanto, se corta la cadena.

Es común que tanto los estados de revocación como el estado de la cadena de confianza sean almacenados en un *caché* por parte de los sistemas informáticos. El tercero aceptante debe ser consciente que el riesgo de no detectar una anomalía por no actualizar los *cachés* a tiempo es su responsabilidad exclusiva, y ni el suscriptor ni el PSCA serán responsable ante incidentes que deriven de escenarios de ese estilo.

2.5.Usos del certificado

El certificado se está utilizando para uno de los usos permitidos en la Política de Certificación correspondiente.

En este punto, ya realizados todos los controles anteriores, se puede asumir que el certificado es correcto, y por lo tanto que la firma también lo es, asumiendo por supuesto que la firma fue validada en forma previa a estos pasos. De todas formas, cada tipo de certificado tiene asociado un uso específico, que debe ser respetado, y verificado por parte del tercero. Esta validación se logra contrastando cierta información que se encuentra en el certificado con el contexto en el que está siendo empleado.

En un primer nivel, se debe validar a lo largo de toda la cadena de confianza la restricción más básica: si cada certificado de la cadena es un certificado de CA o no. Esto se logra mediante la consulta a la extensión BASIC CONSTRAINTS. Si se tiene CA=True, entonces es un certificado de CA y puede emitir certificados (caso de la ACRN y los PSCA), pero si tiene CA=False, entonces no puede ser usado para emitir certificados. La validación de una cadena de confianza con un certificado intermedio que contenga el valor CA=False debe fallar en cualquier caso.

En un segundo nivel, se debe validar la extensión KEY USAGE. Esta extensión es una máscara de bits que se habilitan según los usos más básicos que se pueden tener. En la siguiente tabla se explicita qué bits deben estar habilitados para los usos más comunes que se pueden encontrar en el contexto de la INCE.

Uso	**Bits**
Autenticación o Firma simple (sin exigir no repudio)	digitalSignature
Firma Electrónica Avanzada de documentos o transacciones	digitalSignature y contentCommitment o nonRepudiation, puede variar según el PSCA.
Cifrado de Datos	dataEncipherment
Cifrado de Claves	keyEncipherment
Firma de Certificados (CA)	keyCertSign
Firma de CRL (CA)	crlSign

A modo de ejemplo, si se está validando una firma electrónica de un documento PDF para el cual se requiere no repudio posterior, se debe asegurar que el certificado tenga habilitado el bit *contentCommitment*, que también puede ser llamado *nonRepudiation*.

En un tercer nivel se encuentran propiedades más avanzadas, expresadas en la extensión EXTENDED KEY USAGE. Es análoga a Key Usage, y la siguiente tabla muestra los usos más comunes para la misma:

Unidad de Certificación Electrónica

Uso	Bits
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 e-mail	emailProtection
Firma de Tokens de Tiempo (Autoridad de Timestamping)	timeStamping
Firma de respuestas OCSP (Servicio de validación OCSP)	OCSPSigning

Cabe destacar que cuando se especifica algún Extended Key Usage (si está presente la extensión) puede estar o no la extensión Key Usage, y en caso de estarlo, tendrá bits que son compatibles con el uso que se le está dando a través del Extended Key Usage. A modo de ejemplo, si se tiene Extended Key Usage OCSPSigning para firmar mensajes OCSP, y además se tiene Key Usage especificado, necesariamente deberá tener el bit digitalSignature activado, y posiblemente tenga también contentCommitment. De todas formas, no lo restringe a que además el certificado tenga otros bits encendidos, habilitándolo además a hacer otras cosas, aunque esta práctica no sea común en la INCE.

Como se puede observar, todas estas validaciones son genéricas para certificados X.509, y hablan sobre las operaciones concretas que se están realizando. Sin embargo, existen escenarios donde por motivos jurídicos o de seguridad se deben exigir cierto tipo específico de certificados. La UCE elabora las políticas de certificación mediante las cuales se emiten y utilizan los certificados electrónicos reconocidos de la INCE. Cada Política de Certificación tiene asignado un identificador único de objeto (OID), y ese OID es estampado en cada certificado que es emitido bajo esa política, independientemente del prestador que lo haya hecho. Recuperando el OID del campo CERTIFICATE POLICIES del certificado, se puede conocer el OID de la política de certificación que le da respaldo, y en base a eso tomar la decisión de si es el tipo de certificado que se espera que la contraparte esté utilizando en la operación. En la siguiente tabla se resumen los OID de los diferentes tipos de certificados disponibles en la INCE.

OID	Política
2.16.858.10000157.66565.0	Autoridad Certificadora de la INCE
2.16.858.10000157.66565.2	Persona Física
2.16.858.10000157.66565.4	Persona Jurídica

El hecho de que un certificado electrónico contenga entonces uno de estos OID en su extensión Certificate Policies, indica que fue emitido bajo las condiciones que la política de igual OID establece. Los terceros pueden, y deberían, leer la política para conocer el perfil de los certificados, puesto que en ella se especifican los controles que los PSCA aplican en el registro, emisión renovación y revocación de ese tipo de certificado, explicitando garantías y obligaciones para las tres partes: prestador, suscriptor y tercero aceptante.

Unidad de Certificación Electrónica

3.Control de versiones

Versión	Fecha	Modificación	Autor
1.0	10/01/2013	Versión inicial	Guillermo Dotta
1.1	06/02/2013	Modificaciones menores de redacción y ajustes para publicación	Guillermo Dotta