Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente

Dirección de Certificadores de Firma Digital
Ministerio de Ciencia y Tecnología

OID 2.16.188.1.1.1.2.1
Versión: Consulta pública
26 de Julio, 2012


MICIT
Ministerio de
Ciencia y Tecnología

Control de versiones

Fecha	Versión	Autor(es)	Aprobado	Descripción
26/07/12	Consulta pública	Comité Asesor de Políticas	Alexander Barquero Director DCFD	Se presenta la versión para discusión del CAP y aprobación del Director de la DCFD.

Índice

1. Introducción

La presente política define las características que conforman los formatos oficiales de documentos electrónicos firmados digitalmente, para el gobierno de Costa Rica. Dichas características deberán ser incorporadas ya sea por el firmante, receptor o validador de un documento electrónico en los procesos de generación o validación de la firma digital, y verificadas por cualquier receptor del documento electrónico en el respectivo proceso de validación de la firma digital del mismo.

Los formatos oficiales serán acogidos por cualquier entidad pública (o cualquier empresa privada o particular que así lo desee) como el estándar en el cual basarán sus documentos electrónicos firmados digitalmente, mismos que generan o consumen en sus respectivos procesos de negocio apoyados en sistemas de información. Los documentos en formatos oficiales tienen una serie de mecanismos que le garantizan mayor robustez a los procesos y a las organizaciones que los utilizan e implementan, y su uso potencia la interoperabilidad de procesos digitales y documentos electrónicos firmados digitalmente entre las diferentes instituciones del país. Los riesgos que se atienden con una implementación basada en formatos oficiales se explican en la política.

1.1 Administración de la Política

1.1.1 Organización que administra el documento

Dirección de Certificadores de Firma Digital

Ministerio de Ciencia y Tecnología, dirección: San José, Calles 17 y 19, Avenida Segunda (50 metros Este del Museo Nacional). Apartado Postal: 5589-1000 San José, Costa Rica.

1.1.2 Persona de contacto

Director de Certificadores de Firma Digital, Dirección de Certificadores de Firma Digital. Correo Electrónico: informacion@firmadigital.go.cr. Tel. (506)2248-1515, ext. 232 o 183.

2. Resumen

Esta política detalla las características que un documento electrónico firmado digitalmente debe tener para considerar que implementa un formato oficial nacional. Además, se explican los riesgos que se asumen si no se contemplan las características mencionadas al usar o implementar aplicaciones con firma digital.

3. Definiciones, conceptos generales y abreviaturas

3.1 Definiciones y conceptos generales

Para los propósitos del presente documento, se aplican los siguientes términos y definiciones:

Documento electrónico: cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático. En otras palabras, cualquier conjunto de datos creado, preservado, transmitido o visualizado por medios electrónicos puede ser considerado un documento electrónico.

Documento electrónico firmado digitalmente: aquel documento electrónico, cualesquiera que sean su contenido, contexto y estructura, que tiene lógicamente asociada una firma digital. En otras palabras, es un objeto conceptual que contiene tanto el documento electrónico como una firma digital, sin importar que estos dos elementos puedan encontrarse representados por conjuntos de datos diferentes.

Token de sellado de tiempo: Respuesta estandarizada de una TSA que permite relacionar un conjunto de datos con un tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo. Los token de sellado se emiten de acuerdo al RFC 3161 “Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)”. También se conocen con el nombre de estampas de tiempo.

Autoridad de Sellado de Tiempo (TSA por sus siglas en inglés Time Stamping Authority): sistema de emisión y gestión de token de sellado de tiempo basado en una firma digital acreditada dentro de la jerarquía nacional de certificadores registrados.

Ruta de certificación: corresponde a la cadena de certificados que soportan un certificado en particular, empezando en el certificado raíz y terminando en el certificado en cuestión, siempre dentro de la jerarquía nacional según el Sistema Nacional de Certificación Digital.

Información de revocación: se refiere al conjunto de datos que permiten determinar la validez de un certificado en un momento dado del tiempo. Los mecanismos tradicionales de información de revocación son las Listas de Revocación de Certificados (CRLs por sus siglas en inglés) y la respuesta del Protocolo En Línea de Estado de Certificados (OCSP por sus siglas en inglés).

Listas de Revocación de Certificados (CRLs): mantiene un listado de todos los certificados que han sido revocados y del momento en que se dio su revocación. La autoridad certificadora define un tiempo de validez para la CRL, de tal forma que una vez que caduque debe ser actualizada.

Protocolo en Línea de Estado de Certificados (OCSP): protocolo de implementación de servicios de respuesta en línea del estado de un certificado en el momento en que es solicitado. Requiere de comunicación en línea con la autoridad certificadora.

Formato de Firma Digital: especificación donde se define la estructura y codificación de un documento firmado digitalmente.

3.2 Abreviaturas

Abreviatura	Descripción
CA	Autoridad Certificadora (Certificate Authority)
CAdES	CMS Advanced Electronic Signature
CRL	Lista de Revocación de Certificados (Certificate Revocation List)
OCSP	Protocolo En Línea de Estado de Certificado (Online Certificate Status Protocol)
PAdES	PDF Advanced Electronic Signature
TSA	Autoridad de Sellado de Tiempo (Time-Stamping Authority)
TST	Token de Sellado de Tiempo (Time-Stamp Token)
XAdES	XML Advanced Electronic Signature

4. Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente

4.1 Resumen

La Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente establece el conjunto de reglas generales para el procesamiento de documentos electrónicos firmados digitalmente. Además, la Dirección de Certificadores de Firma Digital está en plena potestad de modificar o emitir nuevas políticas, así como otros instrumentos documentales y técnicos aún no especificados, que permitan atender con mayor detalle y robustez las necesidades de gestión de documentos electrónicos firmados digitalmente del país.

4.2 Identificación

Este documento es la "Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente", y se referencia mediante el identificador de objeto (OID): 2.16.188.1.1.1.2.1

OID	Descripción
2	joint-iso-itu-t
16	Country
188	Costa Rica
1	Organización
1	Dirección de Certificadores de Firma Digital
1	Políticas
2	Políticas de Documentos Electrónicos Firmados Digitalmente
1	Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente

4.3 Comunidad de usuarios y aplicabilidad

Esta política tiene como objetivo guiar a las diferentes entidades públicas y privadas que deseen proveer o consumir servicios en internet con mecanismos de firma digital, a los proveedores y desarrolladores de soluciones de software con mecanismos de firma digital, a los usuarios de los servicios o soluciones antes mencionados y a los ciudadanos que deseen conocer o utilizar mecanismos de firma digital en general.

4.4 Cumplimiento

Las entidades públicas que deseen implementar soluciones con mecanismos de firma digital, deberán cumplir con los lineamientos establecidas en esta política para generar y procesar documentos mediante el uso de formatos oficiales, según el conjunto de responsabilidades que les corresponda (firma y/o validación de la firma del documento electrónico). Esto aplicará también para las instituciones privadas o particulares que decidan implementar sus mecanismos de firma digital utilizando los formatos oficiales.

5. Especificación de los Formatos Oficiales

5.1 Uso de Formatos Avanzados

En el Sistema Nacional de Certificación Digital, se conocerán como formatos avanzados todos aquellos formatos de firma digital que definen de manera estandarizada los atributos suficientes para garantizar la verificación de la validez del documento en el tiempo, que estén auspiciados por alguna entidad internacional reconocida, y que sus especificaciones técnicas sean de acceso público. Esta definición se basa en los estándares promulgados por el Instituto de Estándares de Telecomunicaciones Europeo (ETSI por sus siglas en inglés), a partir de la Directiva 1999/93/EC emitida por la Unión Europea.

Los formatos oficiales de los documentos electrónicos firmados digitalmente en Costa Rica serán solo aquellos que la Dirección de Certificadores de Firma Digital determine. Bajo esa premisa, se define que los formatos oficiales de los documentos electrónicos firmados digitalmente en Costa Rica serán aquellos construidos con base en los formatos avanzados emitidos como normas técnicas y estándares por la ETSI, en un nivel de especificación que contemple la inclusión de todos los atributos necesarios para garantizar la verificación de su validez en el tiempo de manera irrefutable. Dichos formatos avanzados y configuración de niveles son los que se especifican a continuación:

- **CAdES-X-L**
  - Basado en la especificación ETSI TS 101 733, en su última versión oficial.
- **PAdES Long Term (PAdES LTV)**
  - Basado en la especificación ETSI TS 102 778, en su última versión oficial.
- **XAdES-X-L**
  - Basado en la especificación ETSI TS 101 903, en su última versión oficial.

Sin importar las diferencias en codificación y forma inherentes a cada especificación, los niveles de configuración de los formatos avanzados aquí mencionados cumplen con las siguientes características determinantes para su selección:

- Permiten la utilización de algoritmos criptográficos robustos.
- Respetan el principio de neutralidad tecnológica:
  - Son estándares abiertos.
  - Pueden ser empleados en escenarios multiplataforma.
  - No están sujetos a un determinado producto licenciado.
- Cuentan con una adecuada documentación técnica.
- Permiten la incorporación de múltiples firmas en un documento electrónico.
- Implementan los principios de un mecanismo de firma confiable:
  - Garantía de la autenticidad del documento electrónico.
  - Garantía de la integridad del documento electrónico.
  - Ubicación fehaciente del documento electrónico en el tiempo.
- Especifican mecanismos estandarizados para garantizar la preservación y verificación de la validez de las firmas digitales del documento electrónico en el tiempo:
  - Inclusión de sellos de tiempo en el documento electrónico.
  - Inclusión de la ruta de certificación en el documento electrónico.
  - Inclusión de la información de revocación en el documento electrónico.

5.2 Responsabilidades

En el ciclo de vida de un documento electrónico firmado digitalmente mediante el uso de un formato oficial, se identifican dos conjuntos de responsabilidades relacionados con mecanismos de firma digital, a saber la firma y la verificación de validez de la firma, cada uno con una serie de actividades que deben realizarse para garantizar la validez del documento electrónico firmado digitalmente en el tiempo. La ubicación y codificación de estos atributos responde a lo indicado en las especificaciones de la ETSI mencionadas anteriormente, según corresponda.

5.2.1 Firma del documento electrónico

Cuando se firma un documento electrónico, será responsabilidad del sistema o sistemas que implementan los mecanismos de firma digital incluir, respetando el estándar que corresponda, los atributos descritos a continuación:

Nombre del Atributo	Descripción del Atributo	Etapas de Proceso Posibles para la Inclusión del Atributo en el Documento
Resumen hash encriptado (digest)	Mecanismo criptográfico que permite garantizar la integridad y autenticidad del documento.	Emisión
Certificado del firmante	Copia del certificado del firmante que permite verificar la autoría del documento.	Emisión
Token de sellado de tiempo[1]	Solicitados a una TSA de la jerarquía del Sistema Nacional de Certificación Digital.	Emisión, Recepción o Validación
Rutas de certificación	Cadenas de certificados que ubiquen el certificado del firmante y de los sellos de tiempo en la jerarquía del Sistema Nacional de Certificación Digital.	Emisión, Recepción o Validación
Información de revocación	Respuestas de validez del certificado del firmante, de los sellos de tiempo y de todos los certificados de sus respectivas rutas de certificación.	Emisión, Recepción o Validación

[1] Los token de sellado de tiempo que se utilizan de manera estandarizada en los formatos oficiales son para determinar la existencia de un conjunto de datos en un momento determinado del tiempo (por ejemplo, para garantizar que el certificado no estaba vencido al momento de la firma), y no necesariamente para identificar el momento de realización de la firma por parte del firmante ni del momento de la recepción del documento por parte de un receptor del mismo.

5.2.2 Verificación de la validez de la firma del documento electrónico

Cuando se verifica la validez de un documento electrónico firmado digitalmente en el formato oficial, es imperativo que se realicen las siguientes validaciones de los diferentes atributos que el documento contiene:

Nombre del Atributo	Descripción de la Actividad de Validación
Resumen hash encriptado (digest)	Verificar que el hash encriptado corresponda con el documento electrónico.
Certificado del firmante	Verificar que la firma del documento corresponda con el certificado del firmante.
Token de sellado de tiempo	Verificar que los tokens de sellado de tiempo son de fechas previas a la fecha de vencimiento de los certificados del firmante o de las rutas de certificación e información de revocación según corresponda, y así garantizar que todos los certificados y cadenas eran vigentes y válidas cuando se usaron.
Rutas de certificación	Verificar que todos los certificados del documento correspondan a certificados de la jerarquía del Sistema Nacional de Certificación Digital.
Información de revocación	Verificar que todos los certificados del documento eran válidos (vigentes y no revocados) en el momento de su inclusión en el documento.

6. Riesgos de la no adopción de Formatos Oficiales

6.1 Verificación de la Validez del Documento Electrónico en el Tiempo

El formato oficial contempla el uso estandarizado de tokens de sellado de tiempo, que junto a la información de revocación y las rutas de certificación, permiten verificar la validez de las firmas digitales de los documentos electrónicos en el tiempo. Sin esa información, ciertos estados del ciclo natural de los certificados de la jerarquía nacional podrían servir como argumentos de repudio ante la necesidad de verificar la validez de algún documento electrónico firmado digitalmente. Un ejemplo de esto es el vencimiento de los certificados de persona física, lo que implicaría que, sin haber utilizado tokens de sellado de tiempo, no existan argumentos suficientes como para garantizar que el documento efectivamente fue firmado en un momento en que los certificados de la persona en cuestión se encontraban en estado vigente.

6.2 Documento Auto-contenido

Los documentos electrónicos firmados digitalmente que no implementan el formato oficial no son documentos electrónicos inválidos, pero podría ser necesario revisar una serie de factores del contexto del documento (la aplicación que lo genera y firma, los rastros de auditoría de las bases de datos donde reside el documento, la información de revocación de las Autoridades Certificadoras involucradas, entre otros) para obtener toda la información necesaria que permita dar garantía de la integridad, autenticidad y no repudio de las firmas digitales del mismo.

En aras de no trasladar esa responsabilidad, técnicamente costosa, a cada sistema, a cada ciudadano, o a los jueces y peritos involucrados en procesos judiciales en donde deseen verificar la validez de un documento electrónico firmado digitalmente, el formato oficial contempla toda la información que podría ser requerida directamente dentro del documento. Dicha información es suficiente ante la falta de conexión a Internet o del sistema que generó el documento o la firma, o incluso ante la desconexión o desaparición de cualquiera de las Autoridades Certificadoras que estuvieron involucradas en la firma del documento electrónico.

6.3. Interoperabilidad

En un escenario sin normativa o recomendación alguna sobre formatos oficiales de documentos electrónicos firmados digitalmente, existen una infinidad de posibilidades en el tipo de los documentos que serán intercambiados entre los diferentes sistemas con mecanismos de firma digital y las diferentes instituciones o ciudadanos que utilizan dichos sistemas. La adopción de un formato oficial podría incrementar el escenario de interoperabilidad documental entre las diferentes instituciones que lo adopten y hacer más transparente el uso de documentos electrónicos firmados digitalmente para todos los interesados en el país.