



Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente

Dirección de Certificadores de Firma Digital
Ministerio de Ciencia, Tecnología y Telecomunicaciones



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.
08/05/13	Borrador	Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Se incorporan las observaciones de la consulta pública, de acuerdo al aviso publicado el día lunes 13 de Agosto del 2012, en el diario oficial "La Gaceta", número 155.
20/05/13	1.0	Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Oficialización y entrada en vigencia de la política.

Índice

1.	Introducción	1
1.1	Administración de la Política	2
1.1.1	Organización que administra el documento.....	2
1.1.2	Persona de contacto	2
2.	Resumen	2
3.	Definiciones, conceptos generales y abreviaturas	2
3.1	Definiciones y conceptos generales	2
3.2	Abreviaturas	3
4.	Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente	4
4.1	Resumen.....	4
4.2	Identificación.....	4
4.3	Comunidad de usuarios y aplicabilidad.....	4
4.4	Cumplimiento.....	4
4.5	Vigencia.....	5
5.	Especificación de los Formatos Oficiales.....	6
5.1	Uso de Formatos Avanzados	6
5.2	Responsabilidades.....	7
5.2.1	Firma digital del documento electrónico	7
5.2.2	Verificación de la validez de la firma digital en el documento electrónico.....	8
5.2.3	Consideraciones adicionales para la inclusión de los atributos.....	8



1. Introducción

La presente política define las características que conforman los formatos oficiales de documentos electrónicos firmados digitalmente, al amparo de la Ley No. 8454 Ley de Certificados, Firmas Digitales y Documentos Electrónicos y de su Reglamento. Dichas características deberán ser incorporadas por el firmante, receptor o validador de un documento electrónico en los procesos de generación o validación de la firma digital, según corresponda, 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 toda entidad pública, empresa privada o particular, 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 o individuos 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.

- 1.1 Administración de la Política
- 1.1.1 Organización que administra el documento

Dirección de Certificadores de Firma Digital

Ministerio de Ciencia, Tecnología y Telecomunicaciones, 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: firmadigital@micit.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.

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)
CAeS	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)
PAeS	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, tanto para la realización de la firma digital como para la verificación de su validez en cualquier momento en el tiempo.

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, empresas privadas o particulares que deseen implementar soluciones con mecanismos de firma digital, tanto para soluciones internas, interinstitucionales, o para los servicios ofrecidos a sus clientes o administrados, deberán cumplir con los lineamientos establecidas en ésta política para generar y procesar documentos mediante el uso de formatos oficiales, según el conjunto de responsabilidades que les corresponda (firma digital y/o validación de la firma digital).



4.5 Vigencia

La “Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente” rige a partir de su publicación.

Se establece un periodo transitorio de 24 meses naturales a partir de su publicación para que las entidades públicas, empresas privadas o particulares que utilizan documentos electrónicos firmados digitalmente en sistemas informáticos a la medida o mediante soluciones ofimáticas ya instaladas, utilicen el formato oficial como soporte electrónico estandarizado cuando sea necesario el uso de firmas digitales.

Cualquier nuevo uso de firma digital, así como cualquier nuevo sistema informático a la medida que contemple el uso de mecanismos de firma digital y que sea desarrollado a partir de la publicación de la presente Política, deberá acogerse a ésta y cumplir con los formatos oficiales establecidos.

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.
 - Para documentos con información codificada en binario.
 - Para su codificación en soluciones a la medida, se propone el perfil CADES Baseline Profile de la ETSI, el cual puede encontrarse en la especificación ETSI TS 103 173, en su última versión oficial.
- **PAdES Long Term (PAdES LTV)**
 - Basado en la especificación ETSI TS 102 778, en su última versión oficial.
 - Para documentos en formatos PDF y sus formatos extendidos.
 - Para su codificación en soluciones a la medida, se propone el perfil PAdES Baseline Profile de la ETSI, el cual puede encontrarse en la especificación ETSI TS 103 172, en su última versión oficial.
- **XAdES-X-L**
 - Basado en la especificación ETSI TS 101 903, en su última versión oficial.
 - Para documentos en formatos XML.
 - Se recomienda para el desarrollo de soluciones informáticas en donde sea necesaria la interoperabilidad con otras instituciones.
 - Para su codificación en soluciones a la medida, se propone el perfil XAdES Baseline Profile de la ETSI, el cual puede encontrarse en la especificación ETSI TS 103 171, 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: la firma digital y la verificación de validez de la firma digital. Para la emisión de un documento electrónico firmado digitalmente, y para la recepción o verificación de su validez, se establecen una serie de actividades que deben realizarse para garantizar que la firma digital asociada tenga valor en el tiempo. El lugar y la manera en que se codifican estos atributos en el documento electrónico corresponden con lo indicado en las especificaciones de la ETSI mencionadas anteriormente.

5.2.1 Firma digital del documento electrónico

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

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
Tokens de sellado de tiempo¹	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

¹ Los tokens 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. Pueden utilizarse otros tokens de sellado de tiempo, adecuadamente controlados y documentados en las herramientas, para tales fines.

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
----------------------------------	--	---------------------------------

5.2.2 Verificación de la validez de la firma digital en el 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.
Tokens 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.

5.2.3 Consideraciones adicionales para la inclusión de los atributos

Tal y como se desprende de la presente política y de los estándares a los que hace referencia, los atributos “Resumen hash encriptado (digest)” y “Certificado del firmante” solo pueden agregarse en presencia de cada uno de los firmantes titulares de los certificados que realizan un ejercicio de firma sobre el documento electrónico. Los restantes atributos, “Tokens de sellado de tiempo”, “Rutas de certificación” e “Información de revocación”, pueden agregarse posterior al ejercicio de firmado del/de los firmantes del documento, ya sea al momento de la recepción o durante la validación del documento. Esto último es cierto siempre y cuando los certificados de los firmantes, y los certificados de la jerarquía, no hayan vencido ni tampoco hayan sido revocados.

El escenario descrito es una medida existente para atender el riesgo de que, al tratar de hacer una firma digital en formato oficial, los servicios de respuesta en línea o los repositorios de información de revocación no estén disponibles; con el objetivo de que dicha eventualidad no limite la creación de firmas digitales en documentos electrónicos, a los que posteriormente pueden incluirse todos los atributos adicionales que permiten la verificación de la validez de la firma digital del documento electrónico a largo plazo.