

PROPUESTA PARA ESTANDARIZAR EL FORMATO DE LOS DOCUMENTOS ELECTRÓNICOS FIRMADOS DIGITALMENTE EN COSTA RICA¹

Carlos Aguilar Mata²
Alexander Barquero Elizondo³
Daniel Chavarría Alvarado⁴
Marcela Fernández Coto⁵
Karolina Solano Solano⁶

Recibido: 07/04/2014 - Aprobado: 10/09/2014

RESUMEN

El objetivo de la presente investigación consiste en proponer un formato estándar y de uso masivo de documento electrónico firmado digitalmente en Costa Rica. La adopción generalizada del estándar propiciaría la interoperabilidad de las aplicaciones informáticas y facilitaría la gestión de los documentos electrónicos en las diferentes instituciones costarricenses. En la investigación se analizan las diferentes alternativas de formato, se hacen recomendaciones y las justificaciones correspondientes, y por último se presenta la propuesta de estándar de documento electrónico firmado digitalmente el cual, posterior al análisis realizado, se considera el más adecuado para las necesidades de Costa Rica.

Palabras clave: Firma digital, Documento electrónico, CAdES, XAdES, PAdES

ABSTRACT

The main objective of this research is to make a proposal of a standard and massive use format for digitally signed electronic documents in Costa Rica. The global adoption of the standard will encourage the interoperability of IT applications and will make the management of electronic documents in Costa Rican institutions easier. The research

-
1. Trabajo ganador del premio “José Luis Coto Conde” de investigación archivística.
 2. *Chief Technology Officer en Guink*. Correo electrónico: carlos@guink.co.
 3. Director de Certificadores de Firma Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones. Correo electrónico: alexbarquero@gmail.com
 4. Consultor en el Banco Interamericano de Desarrollo. Correo electrónico: dchavarria@iadb.org
 5. Especialista en seguridad de TI en el Banco Central de Costa Rica. Correo electrónico: marceferc@gmail.com
 6. Coordinadora de equipos de trabajo en el Banco Central de Costa Rica, División de Servicios Tecnológicos. Correo electrónico: Ksolano@gmail.com

analyses different signature formats, gives recommendations along with their justifications and presents the proposal of a standard for digitally signed electronic documents that, after the analysis, is considered the most appropriate for Costa Rica's needs.

Keywords: Digital signature, Electronic document, CAeS, XAdES, PAeS

1. INTRODUCCIÓN

La función de la archivística, así como su relación con los documentos y los archivos que los contienen, se ha mantenido constante desde sus orígenes. La conservación y organización de documentos siempre han sido pilares fundamentales de la disciplina. Sin embargo, como consecuencia del surgimiento de las tecnologías de la información, la aparición de los documentos electrónicos ha traído consigo una serie de nuevos desafíos para la archivística.

Durante la mayor parte de la historia los documentos producidos, como resultado de las actividades humanas, han constituido objetos físicos, plasmados en una variedad de materiales mediante diferentes técnicas las cuales evolucionaron de la mano con el desarrollo tecnológico de las civilizaciones. El uso extendido y continuamente creciente de los documentos electrónicos representa un cambio de paradigma, dadas sus particularidades.

Muchos profesionales de la archivística consideran que aún no se puede trasladar el manejo documental de las organizaciones hacia el mundo electrónico en su totalidad. Sin embargo, el vertiginoso paso al que avanza la tecnología informática y la creciente presencia de ésta en las actividades humanas hace difícil que esta posición sea compartida por aquellos que desconocen los retos que este traslado representa para la archivística. Una migración hacia documentos electrónicos que no haya sido bien planificada podría resultar en la pérdida de información importante, ya sea para un solo individuo o una organización; pero un trabajo profesional y multidisciplinario, alineado con las mejores prácticas que existen en el mundo al respecto, puede generar grandes beneficios para los usuarios y para el ejercicio de la conservación del patrimonio documental de los ciudadanos, de las instituciones y del país.

Alrededor del mundo, muchos expertos en archivística, gobiernos, comisiones y organismos internacionales se han dado a la tarea de desarrollar iniciativas para reducir el impacto del inevitable movimiento hacia la documentación electrónica. Estas iniciativas buscan mitigar el riesgo de la pérdida de la información y asegurar la conservación del enorme cuerpo documental producido por la humanidad que existirá únicamente en el mundo electrónico. Iniciativas como el Proyecto InterPARES, MoReq, el estándar ISO 15489 y el programa Memoria del Mundo, para mencionar sólo algunos, intentan atacar la problemática de la archivística y los do-

cumentos electrónicos desde diferentes ángulos. Estas iniciativas ofrecen grandes avances e ideas, pero aún no existe ninguna que ofrezca una solución definitiva a todos los desafíos traídos por la migración hacia el mundo electrónico.

En Costa Rica, la Ley 8454: “Ley de Certificados, Firmas Digitales y Documentos Electrónicos”, promulgada en el 2005, estableció la equivalencia funcional entre la firma autógrafa y la firma digital. Con esta ley, se abrieron las puertas para que los documentos electrónicos fueran considerados una alternativa válida al documento físico, y su uso ha ido creciendo desde entonces. El aumento en el uso de documentos electrónicos tiene muchas ventajas, pero también crea desafíos para las instituciones encargadas de manejarlos. En el Artículo 6 de la Ley 8454, se estipula que “La Dirección General del Archivo Nacional dictará las regulaciones necesarias para asegurar la gestión debida y conservación de los documentos, mensajes o archivos electrónicos” (Gobierno de Costa Rica, 2005). Como resultado el Archivo Nacional cumple un papel fundamental sobre las decisiones que permitan estandarizar la manera en que se firman los documentos electrónicos.

La presente investigación, titulada “Propuesta para estandarizar el formato de los documentos electrónicos firmados digitalmente en Costa Rica”, consiste en proponer un formato de documento electrónico firmado digitalmente en Costa Rica, de tal forma que las instituciones y particulares lo adopten para facilitar la interoperabilidad de las aplicaciones, y coadyuvar a garantizar la calidad archivística en la producción, la gestión y la conservación de los documentos electrónicos de las instituciones y del patrimonio histórico y cultural de nuestro país.

2. DESARROLLO

2.1. Conceptos Base

2.1.1. Documento electrónico firmado

“Documento electrónico firmado” es aquel documento electrónico, cualesquiera que sean su contenido, contexto y estructura, que tiene lógicamente asociada una firma digital. De esta forma, debe entenderse “documento electrónico firmado” como un objeto conceptual que contiene tanto el documento electrónico como una firma digital, sin importar que estos u otros componentes puedan encontrarse separados (es decir, ser representados por elementos digitales independientes). Existen diferentes maneras de firmar digitalmente un documento electrónico, así como variadas formas de asociar el documento electrónico a su firma digital y validarla.

2.1.2. Firma Digital

De la misma manera en que la firma manuscrita y los sellos han sido utilizados durante siglos sobre los documentos tradicionales, surgió la necesidad de “firmar” los documentos electrónicos para vincularlos a su autor como resultado del aumento en su uso por parte de las organizaciones e individuos. Como respuesta a esta necesidad, apareció el concepto de firma electrónica. La ley costarricense no proporciona una definición de firma electrónica (conocida como firma electrónica simple en otros países), pero en general, existe un consenso a nivel internacional sobre el significado de ésta. La firma electrónica se ve como un conjunto de datos que se adjunta o asocia a otro conjunto de datos y es capaz de identificar al firmante. (Gobierno de España, 2003) (FDIC, 2009) (Bravo Lilli, n.d., p. 6).

Existen muchos mecanismos de firma electrónica. Algunos de estos son fáciles de implementar, ya que una firma electrónica puede ser representada por cualquier objeto digital que se asocia a un documento electrónico y es capaz de identificar a su autor. Un ejemplo de esto es una imagen escaneada de la firma manuscrita o datos biométricos como una grabación de la voz o una imagen de las huellas digitales de una persona. Sin embargo, usualmente la firma electrónica no constituye un mecanismo equivalente a la firma manuscrita. Por lo general, la firma manuscrita se considera confiable por una serie de elementos jurídicos y técnicos que le dan cierto peso probatorio. Cuando se está tratando con el mundo digital, uno de los factores de los que depende la confiabilidad de cualquier mecanismo es la seguridad de la información. A continuación, se explican tres características fundamentales de la seguridad de la información, y cómo se relacionan con la confiabilidad de una firma electrónica.

2.1.2.1. Autenticidad

La autenticidad se refiere a la “Calidad o carácter de verdadero o autorizado” (Word Reference, 2011), que en el contexto de un documento, significa que éste proviene de donde dice que proviene y que el firmante es responsable por él. Tradicionalmente, los trazos que conforman una firma manuscrita se pueden asociar unívocamente a una persona, y cualquier disputa sobre el origen de una firma se puede resolver mediante la grafotecnía, estudio de la escritura a mano para identificar y detectar falsificaciones (Liñán Barreto, 2009).

Una firma sobre un documento, ya sea físico o electrónico, debe dar garantía de que la persona a la que está asociada dicha firma se está comprometiendo con el documento. De esta forma, la firma debe asegurar la autenticidad del documento, estableciendo la identidad del firmante y funcionando como evidencia del origen del documento.

2.1.2.2. Integridad

La integridad, en el contexto de la seguridad de la información, se refiere a que la información no sufre alteraciones no autorizadas (Qian y Wiederhold, n.d.). Una firma manuscrita se puede considerar confiable, en cuanto a integridad, dadas las propiedades del medio, ya que una modificación a un documento en papel puede ser fácilmente detectada.

Un proceso de firma debe incluir mecanismos que aseguren que no se puedan hacer modificaciones no autorizadas al documento, o bien, en caso de que sean hechas, éstas pueden ser detectadas.

2.1.2.3. No repudio

El no repudio significa “(...) la habilidad de asegurar que una parte de un contrato o comunicación no pueda negar la autenticidad de su firma en un documento o el envío de un mensaje que haya originado.” (Rouse, 2001). La firma manuscrita funciona como instrumento de no repudio ya que existe garantía de que en caso de una disputa sobre su origen, ésta será invalidada únicamente si el presunto firmante no es realmente quien la generó.

En caso de que una parte intente rechazar o negar su compromiso sobre un documento previamente firmado, un esquema de firma debe garantizar que existen elementos suficientemente robustos para demostrar si efectivamente la firma fue realizada por el firmante o no.

2.1.3. Relación entre firma electrónica y firma digital

Como se señaló anteriormente, la firma electrónica es cualquier objeto digital que vincula a una persona con un documento electrónico. Este objeto, al no encontrarse normado, no necesariamente posee las tres características mencionadas. La firma electrónica por sí sola no representa una prueba confiable de autenticidad, integridad y no repudio, dada la facilidad con la que algunos de los archivos digitales con los que es representada pueden ser copiados, alterados y eliminados sin rastro alguno. Las firmas digitales son un subconjunto de las firmas electrónicas que, dada su correcta implementación basada en criptografía asimétrica y certificados digitales, buscan atender estas deficiencias. En otras palabras, toda firma digital es una firma electrónica, pero no toda firma electrónica es una firma digital.

El sitio Web Dictionary.com ofrece la siguiente definición de “firma digital”: “un código digital encriptado adjunto a un documento electrónico para verificar que fue creado por una fuente conocida y que no ha sido alterado.” (Dictionary.com, 2011). El sitio de firma digital del Sistema Nacional de Certificación Digital del Ministerio de Ciencia y Tecnología de Costa Rica complementa la definición de la siguiente manera: “Es un

método que asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo.” (MICITT, 2011).

La firma digital es aquella firma electrónica que es generada con ciertas técnicas criptográficas y que utiliza cierta infraestructura confiable de tal forma que: 1) vincula unívocamente al firmante con el documento, 2) permite que cualquier modificación no autorizada sea detectada y 3) ofrece elementos para impedir que el firmante eluda su responsabilidad; con lo que cumple las características de autenticidad, integridad y no repudio. Sólo hasta que una firma electrónica cumpla con estas tres características puede ésta considerarse funcionalmente equivalente a la firma manuscrita, y desde la perspectiva técnica esto se logra al generar la “firma digital” a partir de un objeto electrónico que permite lo antes mencionado: el certificado digital, que para nuestros efectos se entiende como una especie de cédula de identidad electrónica.

En Costa Rica, la “Ley N° 8454: Ley de Certificados, Firmas Digitales y Documentos Electrónicos” establece una serie de elementos jurídicos y técnicos que permiten que los mecanismos de firma digital que cumplan con dicha ley presenten las características de autenticidad, integridad y no repudio (Gobierno de Costa Rica, 2005). De esta forma, los mecanismos de firma digital que cumplen con la Ley 8454 se pueden considerar funcionalmente equivalentes a la firma manuscrita.

2.1.4. Formatos de firma digital

Los formatos de firma digital son especificaciones donde se define la estructura de un documento firmado digitalmente. Esta investigación considera inicialmente los siete formatos más conocidos e implementados nacional e internacionalmente:

- CMS (firma de datos binarios)
- PKCS#7 (firma de datos binarios)
- Firma PDF (firma de documentos en formato PDF)
- XMLDSig (firma de documentos en formato XML)
- CAdES (firma de datos binarios)
- PAdES (firma de documentos en formato PDF)
- XAdES (firma de documentos en formato XML)

Cuatro de los siete formatos considerados no establecen, en sus especificaciones, una forma estandarizada para poder verificar la validez de la

firma digital tras largos períodos de tiempo. Dada la importancia de esta característica para un formato estándar de firma digital que buscará ser adoptado de forma generalizada, estos cuatro formatos no serán considerados para la propuesta. Por lo tanto, los formatos CMS, PKCS#7, Firma PDF y XMLDSig se descartan, dejando únicamente los formatos CAdES, PAdES y XAdES para ser considerados como objeto de la propuesta.

2.2. Desarrollo de la Propuesta de Estándar de Documento Electrónico Firmado Digitalmente en Costa Rica

La propuesta de estándar de documento electrónico firmado digitalmente en Costa Rica se elabora con base en la investigación documental realizada, y tiene la estructura que se explica a continuación. En la sección 2.2.1, se enumeran y explican las características identificadas como indispensables para determinar el formato de documento firmado digitalmente que será propuesto como estándar en Costa Rica. Además, se evalúan los formatos candidatos en el contexto de las características identificadas.

Seguidamente, en la sección 2.3, se agrupan en categorías los escenarios donde podrían utilizarse documentos electrónicos firmados digitalmente en el país. Estos escenarios permiten discriminar entre los formatos candidatos de acuerdo a su idoneidad para atenderlos.

Finalmente, en la sección 2.4, se presenta la propuesta de formato estándar de documento electrónico firmado digitalmente para Costa Rica. Esta contempla el estándar elegido y una serie de elementos que es necesario definir para asegurar la interoperabilidad de los desarrollos que lo utilicen.

2.2.1. Características del Formato de Documento Electrónico Firmado Digitalmente.

Una vez que se identificaron los diferentes estándares existentes de documento electrónico firmado digitalmente, se procedió a determinar las características puntuales que permiten discriminar entre las opciones disponibles. Para decidir qué compone esta colección de características deseadas, se tomaron como referencia encuestas sobre el uso de firma digital en otros países, entrevistas realizadas a expertos internacionales e investigaciones realizadas sobre los diferentes estándares de documento electrónico firmado digitalmente, con el fin de alinearse con las tendencias mundiales en el tema. También se consideró necesario tomar en cuenta la realidad nacional, por lo que se utilizaron encuestas realizadas a diversas instituciones, interesados y expertos costarricenses, las condiciones de implementación de la PKI nacional, las necesidades del Archivo Nacional de Costa Rica, consideraciones explícitas en las leyes y propuestas de ley relacionadas con firma digital y neutralidad tecnológica en el desarrollo de los servicios de gobierno electrónico en Costa Rica.

Producto de esta investigación se definieron las siguientes características que debe soportar, como mínimo, el estándar elegido. Se enumeran primero todas las características, y luego se describe cada una con más detalle.

Debe permitir la utilización de algoritmos criptográficos robustos.

Debe respetar el principio de neutralidad tecnológica:

- a- Debe ser un estándar abierto.
- b- Debe poder utilizarse en escenarios multiplataforma.
- c- No debe estar sujeto a un determinado producto licenciado.

Debe contar con una adecuada documentación técnica.

Debe permitir la incorporación de múltiples firmas en el documento.

Debe implementar los principios de un mecanismo de firma confiable:

- a. Debe implementar un mecanismo de validación que asegure la autenticidad del documento firmado.
- b. Debe implementar un mecanismo de validación que asegure la integridad del documento firmado.
- c. Debe permitir la ubicación fehaciente del documento firmado en el tiempo.
- d. Debe permitir la preservación y validación de la firma digital en el tiempo.

2.2.1.1. Debe permitir la utilización de algoritmos criptográficos robustos

El proceso de aplicación de una firma digital conlleva la utilización de algoritmos criptográficos tanto para generar el resumen o *hash* del documento que se está firmando digitalmente, como para cifrar el resumen del documento y validar la firma digital asociada. Para esto, se deben utilizar algoritmos de *hash* y algoritmos de cifrado asimétrico.

Todos los algoritmos de cifrado y de *hash* están expuestos a vulnerabilidades y podrían ser violentados en el tiempo. Por ejemplo, los algoritmos *hash* pueden ocasionar colisiones que cuando se descubren producen una pérdida de confianza en el algoritmo al abrirse la posibilidad de que dos documentos diferentes puedan llegar a generar un mismo *hash*. De igual manera, debido al avance en las capacidades computacionales de los microprocesadores, con el paso de los años se posibilitan algunos tipos especializados de ataques informáticos que tratan de descifrar un contenido

cifrado en una cantidad de tiempo razonable, por lo que sería necesario aumentar el tamaño de las llaves criptográficas que se están utilizando.

La fortaleza de la firma digital depende en gran medida de los algoritmos utilizados para crearla. Es por esta razón que el formato de firma digital debe permitir el uso de algoritmos *hash* y algoritmos criptográficos robustos, donde por robusto se entiende que sea resistente y confiable con relación a la capacidad computacional actual y proyectada a mediano y largo plazo. Además, el formato debe ser capaz de adaptarse y permitir la actualización del algoritmo utilizado conforme se descubran otros algoritmos más robustos y/o se requieran tamaños de llaves mayores.

2.2.1.2. Debe respetar el principio de neutralidad tecnológica

Para efectos de esta investigación, y con base en las mejores prácticas y las recomendaciones que existen al respecto sobre la adopción de tecnologías en el mundo, se determina que el o los formatos seleccionados deben cumplir con la característica de ser un estándar abierto, para así respetar el principio universal de neutralidad tecnológica.

Para que un estándar de documento firmado digitalmente sea considerado abierto, sus especificaciones técnicas deben ser de acceso público. Cumpliendo este requerimiento, se eliminaría la dependencia hacia proveedores o fabricantes específicos, ya que cualquier persona o institución con los conocimientos técnicos requeridos podría realizar una implementación que cumpla con el estándar.

Los formatos abiertos son, por lo general, estándares determinados por autoridades públicas u organizaciones internacionales para las cuales uno de sus objetivos es el de establecer normas para la interoperabilidad del software. De igual manera, existen formatos abiertos que son promovidos por compañías que optan por hacer de conocimiento público la especificación de sus formatos. (Puigpinos, 2010)

Al seleccionar un estándar abierto como formato de documento firmado digitalmente, se garantiza que cualquier institución puede realizar una implementación de firma digital sin comprometerse con un proveedor o tecnología específica, ya sea con relación a las herramientas de software que se utilizan, o bien, la plataforma tecnológica sobre la cual funcionan. Adicionalmente, no es necesario incurrir en gastos por licenciamiento relacionados específicamente con la utilización del formato, lo que hace más factible que se puedan hacer desarrollos de firma digital incluso en las instituciones que cuentan con un bajo presupuesto para este fin.

2.2.1.3. Debe contar con una adecuada documentación técnica

Hasta hace poco, la firma digital fue un tema poco explorado, principalmente en el ámbito nacional, por lo que el conocimiento al respecto aún no ha permeado en una gran cantidad de organizaciones. Además, según las encuestas nacionales realizadas en las diferentes instituciones de gobierno, entidades financieras y empresas interesadas, la mayoría de los desarrollos que hoy en día implementan o planean utilizar la firma digital en sus servicios utilizan dos formatos específicos: PKCS#7 y XMLDSig. De proponerse un formato distinto a los mencionados, la experiencia con la que se cuenta actualmente a nivel nacional para implementar aplicaciones que lo soporten podría ser muy limitada o inclusive nula.

Para evitar entorpecer futuros desarrollos y una mayor adopción e interoperabilidad de firma digital en el país, es de suma importancia que el formato propuesto brinde una documentación clara y precisa sobre su implementación y utilización.

Por documentación técnica se entiende cualquier tipo de información, ya sea la especificación técnica del formato, guías de su uso, implementaciones de código abierto que lo utilicen y otros documentos relacionados.

Esta característica está estrechamente relacionada con la característica de neutralidad tecnológica, ya que de no ser un formato abierto, la adquisición de documentación técnica de apoyo podría significar aún más gastos para las organizaciones que desearan realizar sus propias implementaciones.

2.2.1.4. Debe permitir la incorporación de múltiples firmas en el documento.

En algunos escenarios se requiere aplicar más de una firma sobre un documento, como en el caso de un contrato que involucre varias partes o la aprobación mancomunada de un documento. Para estos escenarios, es necesario que el formato de documento electrónico firmado digitalmente permita la incorporación de varias firmas en el mismo documento.

El formato de firma digital debe permitir el uso de firmas en paralelo y firmas en serie. Las firmas en paralelo se refieren a firmas realizadas sobre un mismo contenido, mientras que las firmas en serie se refieren a firmas que se hacen sobre un documento previamente firmado, de tal forma que la nueva firma también encapsula la firma anterior. El tipo de firma que se utilice en un documento dependerá de la naturaleza del mismo y de las necesidades en el momento de realizar la firma digital.

2.2.1.5. Debe implementar los principios de un mecanismo de firma confiable

Como se explicó anteriormente en la sección 2.2.1, un esquema confiable de firma digital, y por lo tanto el formato propuesto, debe presentar las siguientes tres características: garantizar la autenticidad del documento firmado, garantizar la integridad del documento firmado y permitir la ubicación fehaciente del documento firmado en el tiempo, mediante la incorporación de sellos de tiempo.

- Debe implementar un mecanismo de validación que asegure la autenticidad del documento firmado

La autenticidad de un documento electrónico garantiza la identidad del (de los) firmante(s) del documento. Esto significa que la firma presentada en el documento efectivamente corresponde al firmante (Adams & Lloyd, 1999).

Garantizar la identidad del (de los) firmante(s) del documento es un concepto importantísimo en el contexto de firma digital. Esto porque el vincular jurídicamente a una persona, física o jurídica, con su firma digital, solamente es posible si se puede garantizar que la firma incluida en el documento le pertenece y sólo pudo haber sido realizada por el dueño de la misma.

Los mecanismos utilizados para garantizar y validar la autenticidad del (de los) firmante(s) del documento se contemplan en la infraestructura de llave pública. Esto sucede porque, en infraestructuras de llave pública se implementan estándares que permiten garantizar que la llave privada (utilizada para asegurar los documentos que se firman) no abandone el dispositivo (como ISO 21188 y FIPS 140-2), por lo que la llave privada está protegida en dicho dispositivo criptográfico (tarjeta inteligente). Como medida adicional, para acceder a la llave privada, el dispositivo criptográfico requiere que el usuario ingrese un número de identificación personal (PIN por sus siglas en inglés) que sólo él conoce. Esto se logra garantizando que se entrega el certificado digital a la persona correcta y estableciendo el PIN de manera personal contra su entrega. El PIN posteriormente se solicita cada vez que se intenta firmar digitalmente un documento (Carballo Chavarría, 2011).

Por todo lo antes visto, el formato por elegir como estándar de documento electrónico firmado digitalmente en Costa Rica, debe contener todos los elementos requeridos para asegurar que la garantía de autenticidad proporcionada por la adecuada implementación de la PKI se pueda representar en la firma digital.

- Debe implementar un mecanismo de validación que asegure la integridad del documento firmado

Un documento electrónico se considera íntegro cuando su contenido se mantiene libre de modificaciones no autorizadas. Cuando se transfiere un documento, la integridad asegura que si se compara el documento enviado con el documento recibido, éstos serán exactamente iguales (Qian y Wiederhold, s.f.). En el contexto en el cual se desea utilizar la firma digital es muy importante que un documento mantenga su integridad, ya que de ello depende la vinculación jurídica entre el documento y el firmante (quien es responsable sobre el contenido del documento). De no asegurarse la integridad del documento, se podría poner en duda la responsabilidad del firmante sobre el contenido del documento, ya que dicho contenido puede haber sido modificado.

Por todo lo antes visto, el formato por elegir como estándar de documento electrónico firmado digitalmente en Costa Rica, debe contener todos los elementos requeridos para asegurar que cualquier modificación no autorizada realizada sobre el documento firmado pueda ser detectada.

- Debe permitir la ubicación fehaciente del documento firmado en el tiempo

En algunos escenarios es necesario ubicar la firma digital en el tiempo, es por esta razón que el formato utilizado para firmar digitalmente un documento electrónico debe permitir incorporar un sello de tiempo cuando sea necesario dejar prueba de la existencia de un dato en un momento específico en el tiempo. El sello de tiempo debe ser otorgado por una autoridad de sellado de tiempo oficial. Ejemplos de elementos que pueden requerir prueba de su existencia en un momento determinado son contratos, declaraciones juradas, transacciones, así como las respuestas OCSP o CRLs, como evidencia de que se realizaron verificaciones de validez de los certificados en el momento de procesamiento de dichos documentos.

El formato propuesto debe contemplar mecanismos para la gestión del sellado de tiempo en los documentos electrónicos. Un servicio de sellado de tiempo funciona como un tercero de confianza que da fe de la fecha y hora en un momento dado. El sello de tiempo se utiliza para garantizar la existencia de algún dato en un momento específico del tiempo. (Adams et al, 2001)

Es importante notar que si bien el formato debe soportar el sellado de tiempo, su uso queda a criterio de la organización que lo implemente según las necesidades del servicio que lo utilice. En escenarios donde el momento de la verificación del certificado es determinante para garantizar la validez del documento firmado, como por ejemplo un contrato, el for-

mato de documento firmado debe soportarlo. Si no se cuenta con un sello de tiempo otorgado por un tercero de confianza, cualquiera de las partes podría negar haber realizado la firma en el momento del tiempo que se indica en el documento firmado y de esta manera tergiversar cláusulas que dependen de la fecha y hora en que se realizó la firma.

El formato de documento electrónico firmado digitalmente que será propuesto como estándar, debe soportar la inclusión de toda la información y mecanismos necesarios para garantizar y validar la identidad del (de los) firmante(s), la integridad del documento firmado y la evidencia que lo ubique fehacientemente en el tiempo, mediante un sello de tiempo emitido por una TSA oficial.

2.2.1.6. Debe permitir la preservación y validación de la firma digital en el tiempo.

En el mundo físico se han hecho esfuerzos para tener la capacidad de verificar, en cualquier momento del tiempo, la validez de un documento archivado que se encuentre firmado. En el mundo electrónico, es necesario atender este mismo escenario. Esta validación debería poder realizarse en cualquier momento del tiempo, sin importar si el certificado digital que se utilizó para firmar el documento ha vencido o ha sido revocado, si la autoridad certificadora que lo emitió ya no existe o bien, si el algoritmo que se utilizó para hacer la firma digital ha sido quebrantado.

Para realizar esta validación en el mundo electrónico, es necesario contar una serie de elementos, incluyendo la cadena de certificación, CRLs o respuestas OCSP, y otros, incluso si han pasado años desde la creación del mismo. El formato elegido debe ser capaz de almacenar todos los elementos que se requieren para validar las firmas digitales en cualquier momento del tiempo.

Es de suma importancia que el formato seleccionado cumpla con esta característica, ya que cualquier documento electrónico firmado digitalmente puede llegar a convertirse en un elemento probatorio en un juicio o disputa. En este caso, puede ser necesario verificar que la firma digital del documento fue válida en un momento particular del tiempo.

A pesar de que hay escenarios en los que no se requiere que un documento electrónico firmado digitalmente sea validado a través del tiempo, existen muchos otros escenarios en los que esto es de vital importancia y es por esta razón que se considera una característica indispensable en el formato que se elija.

2.2.2. Evaluación de formatos con respecto a las características

Una vez que se describen todas las características deseables para un formato, se considera necesario revisar las opciones de formatos con los que se cuenta. A continuación se presenta una matriz comparativa (Cuadro 1) con la evaluación de los diferentes formatos. En las filas se observan todas las características deseables en un formato propuesto y en las columnas todos los formatos estudiados. Cuando un formato cumple con una determinada característica, se coloca una X en la casilla respectiva.

Cuadro 1. Matriz de evaluación de formatos

	CAdES	XAdES	PAdES
Algoritmos criptográficos robustos	X	X	X
Neutralidad tecnológica	X	X	X
Adecuada documentación técnica	X	X	X
Incorporación de múltiples firmas	X	X	X
Características de firma confiable	X	X	X
Validación de firma a largo plazo	X	X	X

Producto del análisis del cuadro comparativo, se observa que todos los formatos de firma avanzada AdES cumplen a cabalidad con las características propuestas para determinar un formato estandarizado a nivel nacional.

Ya que existen tres alternativas en lugar de una sola, y buscando maximizar el objetivo de interoperabilidad planteado por esta investigación, se procedió a evaluar la posibilidad de migrar entre los diferentes formatos, para así determinar la factibilidad de hacer una propuesta de estándar con múltiples opciones. Sin embargo se concluyó que, dada la imposibilidad de traducir de un formato a otro por razones técnicas relacionadas con las diferencias en la representación de los datos, sería necesario desarrollar dos o tres tipos de implementaciones de interfaces o servicios de firma digital en cada organización interesada para poder ser receptor de cualquier tipo de documento firmado. Este escenario de múltiples implementaciones va en contra de los objetivos de interoperabilidad, y por lo tanto obstaculiza la masificación del uso de firma digital que persigue esta investigación.

Por todas las razones aquí expuestas, se determinó la necesidad de hacer un análisis más detallado de los diferentes formatos de firma avanzados, para así poder descartar dos de las tres opciones y definir un único formato que será el recomendado, producto final de la investigación en cuestión.

2.3. Escenarios de uso de firma digital en Costa Rica

Al haberse considerado necesaria la evaluación más detallada de las tres posibles alternativas de formato de documento electrónico firmado digitalmente que resultaron candidatas para propuesta de estándar nacional, se decidió primero realizar una categorización y análisis de los escenarios en donde podría utilizarse la firma digital.

Tomando como base la información obtenida en las encuestas realizadas a instituciones nacionales, entrevistas a expertos nacionales e internacionales, e investigación realizada sobre el uso de firma digital a nivel mundial, se decidió catalogar todos los posibles usos de firma digital en diferentes contextos de aplicación que permiten agruparlos y analizarlos de una manera más efectiva. A continuación, se enumeran y explican las diferentes categorías elegidas para construir los escenarios de uso de firma digital.

2.3.1. Categorías/características para la definición de escenarios

Tipo de participante: se refiere a los tipos de participantes que pueden estar firmando y/o recibiendo el documento. Los distintos tipos de participantes que pueden interactuar con un documento electrónico firmado son:

- Persona física.
- Sistema informático.

Tipo del sistema: se refiere al contexto del paquete de software mediante el cual se están procesando los documentos firmados, siempre desde el punto de vista de la organización o el individuo que lo utiliza. Los distintos tipos de desarrollo son:

- Sistema a la medida.
- Sistema de terceros (ej.: Microsoft Word).

Tipo de entorno para el uso del sistema y de los documentos firmados: se refiere al contexto de uso del sistema y de los documentos firmados, específicamente si estos documentos se usan sólo a nivel de una organización en particular o si deben intercambiarse con otras organizaciones. Los distintos tipos de entorno son:

- Sistemas de uso interno.
- Sistemas que pueden interoperar.

Tamaño del documento firmado: como el nombre lo indica, se refiere al posible tamaño en memoria del documento que se desea firmar. Esto tiene particular importancia en caso de que una determinada implementación de software que utilice firma digital se hiciera con el fin de firmar objetos digitales de gran tamaño (bases de datos o películas) y este tamaño exceda la capacidad de procesamiento de los equipos con que se cuente en ese momento. Con el objeto de agrupar el tamaño de los documentos firmados, se establecieron los siguientes dos bloques de tamaño:

- Documentos normales (para efectos de esta investigación, menores a 1 Gigabyte de tamaño en memoria).
- Documentos extensos (para efectos de esta investigación, mayor o igual a 1 Gigabyte de tamaño en memoria).

Contexto de uso de los documentos firmados: se refiere a si un determinado documento firmado, o una solución para firmar documentos, podría o no interactuar con documentos firmados que provienen de otros países en donde se utilicen soluciones de firma digital diferentes. Los tipos de contexto son:

- Documentos de uso local (nacional).
- Documentos de uso internacional.

Tipo de solución según etapa de desarrollo: dado que en Costa Rica ya existen diversas entidades que cuentan con soluciones de software que implementan firma digital, soluciones que están en proceso de desarrollo y soluciones sin firma digital pero que podrían utilizarla en el futuro, es importante considerar los esfuerzos adicionales que puede representar la migración o implementación de alguno de los formatos propuestos. Con el objeto de agrupar los tipos de soluciones según su etapa de desarrollo, se determinaron los siguientes grupos:

- Soluciones con requerimientos de firma digital que ya implementan dicha funcionalidad.
- Soluciones con requerimientos de firma digital que aún no se encuentran en proceso de desarrollo.

Volumen transaccional: se refiere a la cantidad de firmas digitales que una aplicación debe procesar y almacenar en un momento dado. Una aplicación podría procesar y almacenar firmas por demanda, es decir, cada vez que entra una solicitud para realizar una tarea de generación, almacenamiento o validación de firmas digitales, o podría hacerlo por lote, y procesar juntas muchas firmas digitales. Se definieron los siguientes grupos:

- Procesamiento y almacenamiento de firmas digitales por demanda.
- Procesamiento y almacenamiento de firmas digitales por lote.

2.3.2. Análisis de los escenarios

De la investigación realizada, se determinó que a pesar de que existen muchas otras categorías mediante las cuales se podría catalogar y analizar los diferentes escenarios más relevantes de uso de firma digital en Costa Rica, las categorías previamente enumeradas son las que mejor permiten agrupar los usos de firma digital actuales y futuros en el país. El uso independiente o la combinación de dos o más de las categorías descritas, son la herramienta que permite determinar los diferentes escenarios que deben considerarse al analizar, a la luz de las tres posibles alternativas de formatos de documento electrónico firmado digitalmente, cuál es el que mejor se ajusta a las necesidades del país y a los objetivos planteados por este trabajo de investigación.

Se generaron tres escenarios a partir de la categoría de tipo de participante, mientras que las categorías de tipo de sistema y tipo de entorno se combinaron para generar cuatro escenarios más. Estos escenarios fueron analizados con el fin de identificar cuáles de ellos son los que mejor reflejan el uso que se le dará a la firma digital en Costa Rica por conveniencia, impacto y relevancia, y así evaluar las tres alternativas disponibles con respecto a su utilidad en esos escenarios.

A continuación, se describen los escenarios considerados determinantes para la elección de uno de los formatos AdES, dada su relación intrínseca con los objetivos de interoperabilidad del proyecto. Los escenarios generados a partir de las categorías de tamaño del documento firmado, contexto de uso de los documentos firmados, tipo de solución según etapa de desarrollo, y volumen transaccional fueron analizados pero no se desarrollan en la siguiente sección porque no se consideraron determinantes en la elección de uno de los formatos. Sin embargo, fueron considerados para explicar una serie de situaciones especiales relacionadas con el formato propuesto, las cuales se explican más adelante en el documento.

2.3.2.1. Escenarios por tipos de participante

Cuando un documento es firmado digitalmente el proceso puede haber sido realizado con la participación activa de una persona física interesada, quien posee tanto el dispositivo criptográfico como el PIN para accederlo; o por solicitud explícita de un sistema informático (ej.: el caso de un documento firmado por un certificado de sello electrónico). Este documento firmado a su vez puede tener como destino final otra persona física, o un sistema que lo procesa y ejecuta flujos de trabajo automatizados según el contenido del documento en cuestión.

Partiendo de esta situación, se observa que existen tres diferentes escenarios según los tipos de involucrados en una transacción en la que medie un documento electrónico firmado digitalmente, cada uno con diferentes

características. Para identificarlos más fácilmente, se reutiliza la nomenclatura usual referente a los participantes en una transacción comercial electrónica, a saber, B2B (*business-to-business*), B2C (*business-to-consumer*) y C2C (*consumer-to-consumer*).

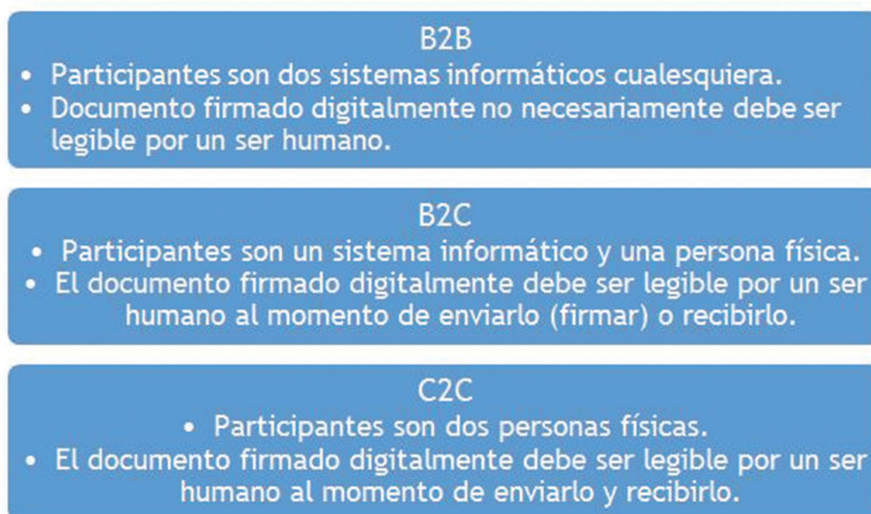


Figura 1. Escenarios por tipos de participantes involucrados

Como puede observarse en la figura 1, la interacción de una persona física en un proceso donde se requiere el intercambio de documentos firmados digitalmente, ya sea con otra persona o con un sistema informático, implica que la o las personas físicas involucradas deberían, como mínimo, ser capaces de observar el documento original previo al firmado, así como poder obtener un documento que haya sido firmado por el sistema en cuestión y ser capaz de verlo y validar la firma.

En el caso de las interacciones B2B, el documento firmado no necesariamente debe ser legible por un ser humano. En el contexto de desarrollo de sistemas a la medida, esto podría implicar considerablemente menos esfuerzo por parte de los desarrolladores, ya que no es necesario generar interfaces o traductores adicionales que transformen un documento optimizado para intercambio de datos entre dos sistemas en un documento diseñado específicamente para ser leído por personas.

Es importante aclarar que, desde la perspectiva de los formatos AdES, los tres escenarios pueden ser cubiertos por cualquiera de los tres formatos sin problema, aunque en algunas implementaciones de cada formato, dependiendo del escenario, sí se requiere más de esfuerzo de desarrollo. En el caso de B2B, se favorece el uso de XAdES y CAdES como formatos op-

timizados para intercambio de datos entre sistemas por encima de PAdES, mientras que este último tiene ventajas nativas de visualización de datos de manera legible para una persona física por sobre los otros, específicamente en los escenarios de B2C y C2C. No obstante, aunque PAdES parece tener ventajas nativas de visualización, si la firma digital está en un documento separado en los formatos CAdES y XAdES no se afectará la legibilidad natural del documento.

Por las razones aquí descritas, no se consideró que los escenarios por tipos de participantes fueran factores determinantes que permitan descartar o favorecer alguno de los formatos. Sin embargo, sí se deben tener en cuenta para garantizar que, de utilizarse XAdES o CAdES, se evalúe la posibilidad de manejar la firma digital como un archivo separado del documento electrónico. De esta forma, se reducen los costos de implementación de modificaciones de firma digital sobre soluciones existentes donde hay personas físicas como participantes, ya que la firma se procesa por aparte, y el procesamiento del documento electrónico no sufre cambios con la incorporación de ésta.

2.3.2.2. Escenarios por tipo de desarrollo y entorno de uso

Para evaluar los siguientes escenarios, se decidió agruparlos según el tipo de desarrollo y el entorno de su uso. Por esta razón, en la siguiente figura 2, se observan cuatro cuadrantes que agrupan las diferentes combinaciones posibles de ambas categorías.

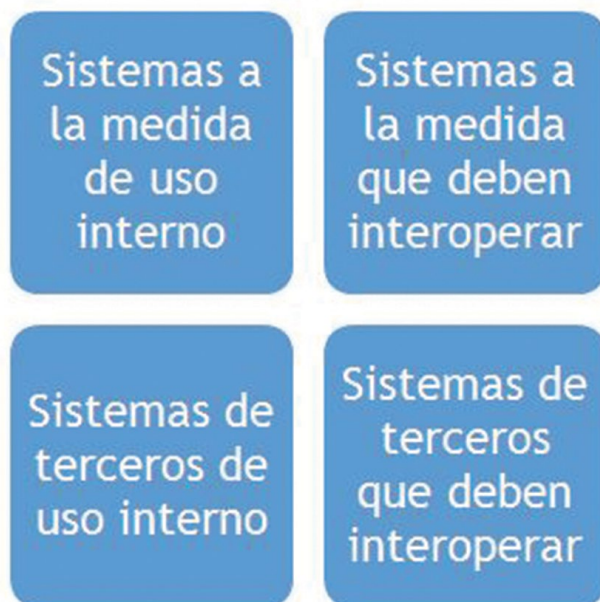


Figura 2. Escenarios por tipo de desarrollo y entorno de uso

Dado que el objetivo central del proyecto se basa en la estandarización del formato de documento firmado en pro de la interoperabilidad de los sistemas de las instituciones nacionales, se determina que el primer cuadrante (cuadrante superior derecho) es el de mayor importancia para la propuesta de la investigación, ya que es donde mayor impacto podría tener su aplicación y donde mayor influencia puede ejercerse para impulsar la interoperabilidad de las soluciones que hagan uso de firma digital. Por esta razón, se procede a otorgar a los formatos mayor relevancia frente a los otros en tanto mejor funcionen para atender el primer cuadrante. El cuadrante inferior derecho también tiene un gran impacto, pero al no presentar capacidad de adaptación, en la mayoría de los casos no es posible ejercer influencia para propiciar la interoperabilidad. Los sistemas pertenecientes a este cuadrante se consideran una situación especial, descrita más adelante.

Después de realizar un estudio más detallado de los formatos identificados como candidatos en la sección 2.2.2, y utilizando como base su idoneidad en los diferentes escenarios de aplicación desarrollados en la presente sección, se procedió a realizar la propuesta de estándar de documento electrónico firmado digitalmente en Costa Rica.

2.4. Propuesta de Documento Firmado Digitalmente en Costa Rica

Una vez discutidas las características requeridas en un formato de documento electrónico firmado digitalmente para que sea viable proponer como estándar en Costa Rica, realizada la evaluación de los formatos estudiados con respecto a estas características e identificados los escenarios de aplicación en los que será posible normar el formato que se utilizará, se realizó la propuesta. Se determinó que el formato que más se ajusta a las necesidades del país en cuanto a desarrollos de firma digital, maximizando la interoperabilidad y asegurando un nivel satisfactorio de confiabilidad para la firma digital, es el formato XAdES.

En la presente sección se enumeran las razones de la elección de XAdES como formato propuesto para estándar de documento electrónico firmado digitalmente en Costa Rica. También se explicarán varias situaciones especiales que se deben tener en cuenta si se decide adoptar XAdES como estándar a nivel nacional y se explicarán aspectos técnicos que es necesario tratar para delimitar algunas posibilidades que ofrece el formato, con el fin de alcanzar la interoperabilidad de los sistemas y su atención a las necesidades reales de los usuarios.

2.4.1. Razones de la elección de XAdES

Con el objetivo de buscar el mayor grado posible de interoperabilidad entre los sistemas de firma digital que utilicen el formato propuesto por la presente investigación, se decidió elegir solamente uno de los tres for-

matos identificados. Como se mencionó en la introducción a la presente sección, el formato elegido fue XAdES. A continuación, se enumeran las razones de por qué se prefirió XAdES sobre los otros dos formatos, y posteriormente se explicará cada una con más detalle:

1. Opinión de los expertos.
2. Tendencias del uso de los formatos de firma digital.
3. Afinidad con el uso de *Web services* y flujo de trabajo XML.
4. Flexibilidad para representar firmas en serie.

2.4.1.1. Opinión de los expertos

A lo largo de la presente investigación, se contactaron varios expertos internacionales con el objetivo de conocer su opinión sobre la elección de uno de los formatos avanzados de firma digital como estándar de documento electrónico firmado digitalmente en Costa Rica. Las personas contactadas fueron David LeBlanc, Arquitecto de Seguridad para la Suite de Office en Microsoft; David Blanco, Gerente General de Tractis, una plataforma de comercio electrónico internacional e intercambio de información sobre marcos normativos de firma electrónica; Martin Bosslett, consultor de la Comisión Europea en temas de implementación de firmas avanzadas; y Juan Carlos Cruellas, profesor de la Universidad Politécnica de Cataluña y uno de los redactores de la especificación de XAdES en la ETSI.

Con respecto a la elección de un único formato de documento electrónico firmado digitalmente para utilizarlo como estándar nacional en Costa Rica, ninguno de los expertos consultados afirmó que no fuera posible. Ciertamente cada uno de ellos está consciente de los beneficios que otorga el establecimiento de un único estándar para la interoperabilidad de los sistemas desarrollados que lo respeten. En cuanto a la coexistencia de tres estándares con funciones muy similares, Martin Bosslet afirmó que, al menos en el caso de la Unión Europea, las razones de esta situación son políticas, no técnicas (Bosslet, Selección entre formatos AdES, 2011). Un ejemplo de lo anterior son las inversiones previas o desarrollos existentes. Si bien es cierto que cada uno de los tres estándares considerados tiene algunas ventajas a la hora de generar y validar ciertos tipos de archivos, las opiniones de los expertos coincidieron en XAdES como el más adecuado para la interoperabilidad y el que mejor se ajusta a las tendencias actuales de los sistemas de información.

En una de las conversaciones con David LeBlanc, éste afirmó: “Para documentos, pienso que XAdES es por mucho su mejor elección. Es un estándar maduro, cubre todas las necesidades que pueda tener para validación a largo plazo de documentos, tanto (Microsoft) Office como Open Office lo soportan ahora, e interoperaría muy bien con Brasil y la Unión Europea.” (LeBlanc, 2011).

Las firmas digitales de la plataforma Tractis están basadas en el estándar XAdES (Blanco Giró, 2010). Cuando se le preguntó a David Blanco las razones de la elección de este estándar, respondió los siguientes puntos (Blanco, 2011):

- XAdES es el estándar más admitido dentro de la Unión Europea, se alinea muy bien con la Directiva 1999/93/CE y fue creado e impulsado por la ETSI.
- A pesar de que el mercado se inclinaba hacia PDF, éste no era un estándar (la iniciativa Tractis apareció en 2005, cuando PDF todavía era un formato propietario bajo el control de Adobe). Además, en aquel momento PDF implementaba las firmas digitales utilizando los formatos CMS y PKCS#7, los cuales no eran avanzados, y por lo tanto no se alineaban con la directiva.
- XAdES ofrecía características de firma digital avanzada y además estaba respaldado por la ETSI. Con el tiempo el mercado se orientó hacia XAdES, con las soluciones DigiDoc en Estonia, OpenDoc en Italia, Bélgica y Brasil, así como Office 2010.
- XAdES no es incompatible con ningún formato de datos. Permite firmar XML de forma nativa o cualquier contenido binario (convirtiéndolo a XML).

Por su parte, Martin Bosslet explicó que si bien es cierto es más simple implementar una solución de firma digital utilizando el formato CAdES, cuando se habla de interoperabilidad XAdES es superior, y afirmó que si estuviera obligado a elegir un formato para establecerlo como un estándar en un país, su elección sería XAdES (Bosslet, Selección entre formatos AdES, 2011). Explicó además que XAdES es más flexible que CAdES para la representación de firmas en serie.

Por último, Juan Carlos Cruellas también recomendó que si se debía elegir un solo formato, XAdES era el más adecuado. Las principales razones enumeradas por Cruellas fueron (Cruellas, Selección entre formatos AdES, 2010):

- Las soluciones XAdES han presentado menos problemas de incompatibilidad que las soluciones CAdES en los Plugtests de la ETSI.
- XAdES, por ser un formato basado en XML, funciona con más naturalidad a la hora de realizar transacciones Web.
- Si bien es cierto que un documento XML no necesariamente es de lectura amigable para los humanos, es posible aplicar

transformaciones XML para hacerlo legible. Con CADES podrían necesitarse procesamiento o software adicionales para producir un documento legible para los humanos, ya que se parte de un documento con base binaria.

2.4.1.2. Tendencias del uso de los formatos de firma digital

Un factor determinante en el éxito o fracaso de un estándar es el grado de adopción que se le dé a éste. Desarrollar sistemas siguiendo un estándar no resulta de mucha utilidad si nadie más lo utiliza. A través de la presente investigación se pudo determinar que el formato XAdES goza de un alto grado de adopción a lo largo de diferentes sectores del mercado.

Para empezar, se debe considerar el nivel de penetración con el que cuenta el estándar XML en muchos ámbitos, sobre todo en Internet. Como consecuencia de ser la elección natural cuando se debe firmar un documento XML, XAdES es capaz de aprovechar la presencia de la tecnología XML en la industria para posicionarse como un formato de firma digital ampliamente utilizado.

Para hablar de aplicaciones concretas, cabe señalar que tanto Office 2010 como el ODF (a partir de su versión 1.2) utilizan XAdES como la implementación de sus firmas digitales (LeBlanc, 2011). Los formatos de Office 2010 y el ODF, en conjunto, componen un segmento considerable de la totalidad de formatos para aplicaciones ofimáticas. Además, varios países como España, Estonia, Letonia y Lituania favorecen fuertemente el uso de XAdES. Los formatos DigiDoc de Estonia, eDoc de Letonia y BDOC de Estonia, Letonia y Lituania utilizan el estándar XAdES.

2.4.1.3. Afinidad con el uso de Web services y flujo de trabajo XML

Los *Web services* representan un componente muy importante del paradigma actual de desarrollo de sistemas de información. El estándar XAdES presenta la ventaja de que funciona naturalmente tanto con los *Web services* como con los flujos de trabajo XML, con lo que se facilita la implementación de sistemas que comparten y procesan información a través de Internet, sin necesidad de intervención humana y aprovechando las ventajas ofrecidas por la firma digital y por el estándar XML (desarrolladas con mayor detalle más adelante en el documento).

Las tecnologías que forman parte del estándar XML permiten la creación de sistemas capaces de recolectar información de varias fuentes distribuidas en Internet, procesarla para obtener el resultado deseado, y luego aplicar una transformación con el fin de generar un documento legible para el ser humano, o para ser utilizado como insumo por otro componente o sistema. El estándar XAdES, por estar basado en XML, puede manejar las

firmas digitales a lo largo de todo este proceso con mayor facilidad que otros estándares.

2.4.1.4. Flexibilidad para representar firmas en serie

Las firmas en serie son firmas digitales que se aplican sobre documentos electrónicos que ya han sido firmados digitalmente, de tal manera que tanto el documento como la firma son firmados. El estándar XAdES, al estar basado en un formato de documento estructurado, presenta más flexibilidad a la hora de elegir el contenido sobre el que se desea aplicar una firma en serie. Mientras que CAdES únicamente permite firmar otra firma (lo que se conoce como firma en serie envolvente), XAdES ofrece la posibilidad de firmar además la totalidad del documento (lo que se conoce como firma en serie total). Esta flexibilidad permite a los sistemas implementados con XAdES tener un mayor control sobre qué partes del documento se firman, lo que puede resultar ventajoso para ciertas aplicaciones según la naturaleza de su negocio.

2.4.2. Consideraciones especiales

Una vez expuestas las razones de por qué XAdES es el formato de documento electrónico firmado digitalmente más adecuado para las necesidades de interoperabilidad de sistemas y confiabilidad de firma digital en Costa Rica, es necesario hacer varias aclaraciones con respecto al establecimiento del formato como estándar.

Si bien es cierto que XAdES es el formato que mejor cumple con los requerimientos establecidos por la presente investigación, se debe recordar que los otros dos formatos avanzados de firma digital (CAdES y PAdES) son también ampliamente utilizados en muchos países, y ninguno de los tres formatos se puede considerar superior a los otros dos en términos absolutos. Esto sucede como resultado de la existencia de muchos formatos de archivo diferentes que son capaces de representar los mismos datos (aunque algunos sean más adecuados que otros según la situación).

Existe una serie de situaciones asociadas a algunos de los escenarios vistos anteriormente en la sección 2.3 que serán enumeradas a continuación y luego discutidas con más detalle, en los que XAdES podría no ser la elección óptima para el desarrollo de una solución, o en los que no existe manera de garantizar la interoperabilidad de las soluciones al cien por ciento. A pesar de esto, se recomienda seguir el estándar propuesto hasta donde sea posible. Sin embargo, la decisión queda a criterio de los implementadores, basándose en las explicaciones desarrolladas a continuación y entendiendo que, de no utilizarlo, se abandonan los beneficios de interoperabilidad expuestos en esta investigación. Se aclara que esta lista no es exhaustiva y podrían existir otras situaciones que podrían no haber sido considerados en la investigación, para las cuales sería necesario realizar un análisis similar. Estos escenarios son:

1. Firma de documentos de gran tamaño.
2. Rendimiento y almacenamiento de gran cantidad de firmas.
3. Implementación de soluciones que no requieran normalizar los datos.
4. Firma y validación de documentos provenientes de otros países.
5. Aplicaciones, paquetes de software y soluciones ya existentes.

2.4.2.1. Firma de documentos de gran tamaño.

Existen casos en los que es necesario aplicar una firma digital a un documento electrónico de gran tamaño. Un ejemplo de esta situación es cuando se debe firmar una base de datos entera. Por la forma en que las aplicaciones procesan los archivos XML, una solución basada en XAdES que quiera producir una firma que esté adjunta al documento XML original deberá manipular la totalidad del contenido del documento en memoria. Dependiendo del tamaño del documento y de la capacidad de la memoria del hardware, podrían darse casos en los que el equipo se quede sin memoria antes de que se complete la generación de la firma (Bosslet, 2011). Casos como el descrito anteriormente son muy poco frecuentes, ya que por lo general los documentos que se desean firmar no son de un tamaño tal que se agote la memoria del equipo que los está procesando, y la frecuencia de este problema disminuirá aún más conforme aumente la capacidad de la memoria de los sistemas computacionales.

2.4.2.2. Rendimiento y almacenamiento de gran cantidad de firmas

En escenarios de alto volumen de transacciones, los sistemas generan o validan grandes cantidades de firmas digitales de manera transaccional (por ejemplo, un sistema de procesamiento por lotes (Bosslet, 2011)). En estos casos el rendimiento podría convertirse en un factor que se debe tomar en cuenta. El cálculo del digest de un documento cuando se está utilizando CAdES se realiza directamente sobre los bytes que componen el documento, mientras que en XAdES es necesario aplicar evaluaciones XPath, transformaciones, codificaciones y normalizaciones para calcular el digest, lo que podría afectar negativamente el rendimiento (Bosslet, 2011). Si la cantidad de firmas que se deben generar o validar es muy grande, la diferencia de tiempo de procesamiento entre una implementación XAdES y una implementación CAdES podría llegar a ser considerable.

Otro factor que se debe tomar en cuenta, sobre todo para el almacenamiento de documentos a largo plazo, es que las firmas CAdES son más compactas que sus equivalentes en XAdES, lo que implica la necesidad de más espacio de almacenamiento para guardar la misma cantidad de datos si se utiliza XAdES (Bosslet, 2011).

No obstante, es importante señalar que los efectos negativos de las situaciones descritas anteriormente se reducen conforme aumenta la capacidad de procesamiento de los sistemas computacionales y disminuye el costo del espacio de almacenamiento.

2.4.2.3. Implementación de soluciones que no requieran normalizar los datos

XML no es un formato de datos canónicos, o normalizados, por sí solo, esto quiere decir que un documento XML con el mismo contenido puede tener diferentes representaciones físicas según la implementación que lo generó. Para que una solución de firma digital basada en XAdES sea confiable, es necesario garantizar que, para un documento XML al que no se le hace cambio alguno, el *digest* calculado a la hora de generar la firma es el mismo que el calculado a la hora de validarla, lo que implica que el documento XML debe estar normalizado. Si no fuera así, podría darse el caso que un documento XML sin modificaciones produzca dos *digests* diferentes debido a las diferencias en la implementación de la aplicación que genera la firma y la aplicación que la valida.

La situación explicada anteriormente hace que la implementación de soluciones de firma digital basadas en XAdES requiera un paso adicional (la normalización de los datos que se van a firmar), lo que le agrega complejidad. Por lo general, los sistemas basados en CADES son más sencillos de implementar, ya que no requieren la transformación de los datos a una forma normalizada, siempre y cuando se esté utilizando una codificación canónica (como DER o CER, explicadas anteriormente) (Bosslet, 2011). Es necesario considerar esto en escenarios donde la simplicidad de la implementación de una solución de firma digital es un factor relevante.

2.4.2.4. Firma y validación de documentos provenientes de otros países

Al investigar las soluciones de firma digital en algunos países alrededor del mundo, se encontró que no existe ningún país en donde se haya impuesto un único formato estándar y que éste sea el único que se permite utilizar. El país que más se acerca a esta situación es Brasil, donde se exige por ley que los formatos utilizados sean XAdES o CADES, pero no hay preferencia de uno sobre el otro. Algunos países se están inclinando hacia XAdES, pero aún no existe nada en su legislación que refleje esto.

Es necesario recordar que para escenarios donde los documentos son de uso internacional, sea cual sea el formato de firma digital utilizado en un país, sin importar que sea un estándar legislado o un estándar de facto, si otro país utiliza el mismo estándar no hay garantía de que las soluciones de firma digital de ambos países vayan a interoperar si no existe acuerdo previo sobre el formato de los documentos que se van a intercambiar. No

basta con que dos países utilicen XAdES, ya que hay otros aspectos que se deben tener en cuenta (como el perfil y la política). Es cierto que si XAdES se establece en Costa Rica como estándar de documento electrónico firmado digitalmente y se van a intercambiar documentos con otro país que también utiliza XAdES, la interoperabilidad será más fácil. No obstante, existen aspectos de implementación que superan el alcance de ésta investigación, y que se deberán discutir a futuro entre ambos países, antes de poder plantear un escenario de interoperabilidad transfronterizo.

2.4.2.5. Aplicaciones, paquetes de software y soluciones ya existentes

Existen casos en los que una aplicación, paquete de software o solución existente tiene su propio formato de firma digital, que no necesariamente es el mismo que se recomendó en la presente investigación. Dado el alcance de la investigación, es necesario aclarar que resulta complicado recomendar un cambio del estándar de firma digital en estas situaciones, ya que recomendar XAdES como estándar podría generar un gran impacto, especialmente si las aplicaciones están muy posicionadas en la organización. Esto aplica tanto para aplicaciones que requieran interoperar como para las de uso interno.

Por ejemplo, muchas soluciones de correo electrónico basan sobre su implementación de firma digital en el formato CMS, que tiene más afinidad con CAdES que con XAdES. También, en las organizaciones que trabajan con documentos PDF, resulta mucho más sencillo utilizar el formato PAdES, ya que las herramientas de generación y lectura de PDF proporcionadas por Adobe generan y validan las firmas digitales en este formato, de una manera transparente para el usuario y configurable visualmente desde la herramienta. Otro caso que ilustra esta situación son las aplicaciones de uso interno, que ya producen y validan firmas digitales utilizando cierto formato, y que por razones de practicidad o técnicas no pueden o deben ser modificados.

Como se explicó en la sección 2.3 que trata sobre los diferentes escenarios de uso de firma digital que se consideraron para la investigación, el enfoque se centró principalmente en las aplicaciones desarrolladas a la medida que deben interoperar. Por lo tanto, resulta de suma importancia dejar claro que la recomendación de XAdES puede aplicar únicamente para desarrollos de soluciones donde se tiene el control total de la implementación del componente de firma digital. Esta aclaración no elimina la posibilidad de que una organización decida cambiar la implementación de una solución desarrollada previamente para que cumpla con la recomendación de XAdES con el fin de interoperar con mayor facilidad con otras soluciones conformes a la propuesta de estándar. Sin embargo, para paquetes de software adquiridos y aplicaciones especializadas sobre las que no se tiene control de su implementación, casi nunca es posible controlar el formato con el que se firmarán los documentos electrónicos, y en la ma-

yoría de los casos sustituir la aplicación por un desarrollo propio para que cumpla con la recomendación puede causar un impacto considerable. La situación anterior presenta la salvedad de que si un paquete de software de terceros o solución existente presenta la capacidad de ser configurada para que su formato de firma digital sea XAdES, en una versión compatible con la propuesta de estándar de la presente investigación, se recomienda proceder a realizar dicha configuración. Con esto, se aprovechan los recursos en los que ya se invirtió tiempo de desarrollo y/o dinero y a la vez se logra alcanzar el objetivo de interoperabilidad con otros sistemas que cumplen con el estándar.

En relación con lo anterior, es necesario señalar que el hecho de que una aplicación utilice XAdES para generar y validar las firmas digitales (como por ejemplo Microsoft Office 2010/2013) no garantiza por sí solo la interoperabilidad con las soluciones desarrolladas siguiendo la recomendación. Existen aspectos técnicos con respecto a la codificación binaria y la sintaxis utilizada para la creación del documento (conocido en el ámbito de la familia AdES como los perfiles y la política del formato) que son elementos trascendentales en la generación y validación de las firmas digitales entre diferentes plataformas. Como parte de la propuesta (localizada más adelante) de los tipos de XAdES que se pueden utilizar se recomienda la forma en la que se puede trabajar la política y los perfiles, con el fin de facilitar la interoperabilidad entre las soluciones desarrolladas. Sin embargo, si lo que se desea es la interoperabilidad de una solución desarrollada y un paquete de software ya existente, los implementadores deben antes asegurarse que los elementos técnicos con respecto a la construcción de la firma digital de los documentos utilizados por ambas partes sean capaces de producir firmas digitales XAdES compatibles entre sí.

En última instancia, se considera pertinente recomendar, si se desea interoperar y no es viable desarrollar un nuevo sistema o modificar uno existente para cumplir con el estándar, el desarrollo de una librería de componentes o un servicio capaz de generar y validar firmas compatibles con el estándar para los documentos electrónicos creados por las aplicaciones establecidas.

2.4.3. Tipos del estándar elegidos

El estándar XAdES tiene siete tipos de formatos definidos, cada uno de ellos con distintos niveles de seguridad a la hora de generar y validar una firma digital. A continuación se explica brevemente cada uno de estos tipos:

- XAdES-BES: firma digital básica, le incorpora propiedades a XMLDSig para calificar los datos firmados.
- XAdES-EPES: extiende el tipo XAdES-BES mediante la incorporación de un identificador de una política de firma.

- XAdES-T: agrega, al tipo XAdES-EPES, un sellado de tiempo sobre la firma digital.
- XAdES-C: además de todo lo del tipo XAdES-T, incluye referencias a la cadena de certificación, lista de revocación y/o respuesta OCSP.
- XAdES-X: asegura las referencias del tipo XAdES-C con un sello de tiempo, que se puede aplicar sobre todo el elemento de firma o sólo sobre las referencias.
- XAdES-X-L: además de las referencias firmadas de XAdES-X, XAdES-X-L agrega toda la cadena de certificación, listas de revocación y/o respuestas OCSP.
- XAdES-A: añade un sello de tiempo a toda la información contenida en XAdES-X-L y criterios para re-sellar periódicamente la firma digital a través del tiempo.

Si se utilizaran todos los tipos mencionados, un validador debería contemplar cada uno de éstos a la hora de validar una firma digital, lo que complicaría las implementaciones. Sin embargo, tampoco es posible escoger sólo un tipo, ya que ninguno de ellos se ajustaría completamente a la variedad de usos que puede tener una firma digital. Para dar un ejemplo, si se utilizara sólo el tipo XAdES-A, sería muy pesado en términos de rendimiento y espacio mantener toda la información de la firma para cada archivo que se maneje a lo interno dentro un contexto organizacional. Por otro lado, si se utilizara sólo el tipo XAdES-BES, para archivos de una alta importancia histórica y cuya firma quisiera ser validada a largo plazo, no se cumplirían los requerimientos necesarios.

Por las razones mencionadas anteriormente, se decidió escoger un subconjunto de los tipos mencionados para ser recomendados como parte del estándar. Se buscó elegir el subconjunto de menor tamaño posible, pero que a la vez fuera capaz de cubrir los escenarios más típicos de uso de firma digital. A continuación, se listarán los tipos elegidos, y luego se justificará su inclusión en el estándar:

- XAdES-EPES.
- XAdES-T.
- XAdES-X-L.
- XAdES-A.

2.4.3.1. XAdES-EPES

Este formato se escogió para poder ser utilizado en los escenarios más simples donde se utilice una firma digital, ya que es el tipo mínimo que respeta una política de firma digital. Una política es esencial para poder cumplir con los requisitos de interoperabilidad. Esto porque la política indica la forma en que debe realizarse la firma y la validación de la misma, si no se incluye esta información no es suficiente para poder garantizar interoperabilidad entre los servicios de firma.

Es importante recalcar que por ser el formato de firma digital más sencillo de los escogidos, XAdES-EPES sólo puede utilizarse en ciertos escenarios ya que no cumple con todos los requisitos de seguridad de los formatos más robustos. A continuación, se presentan los riesgos en que se puede incurrir al utilizar dicho formato.

- Riesgos al utilizar XAdES-EPES:

El formato XAdES-EPES no cuenta con un sello de tiempo sobre la firma digital, lo cual provoca que en las firmas realizadas con este formato no se puedan ubicar en el tiempo. Esto sucede porque al no existir un tercero confiable que certifique el momento en que se realizó la firma, el firmante puede cuestionar el momento en el que se efectuó. Para entender mejor esta situación se puede observar el siguiente ejemplo:

Suponga que una persona se va a jugar fútbol y se quiebra un pie, inmediatamente después del accidente ingresa a la página *Web* de una aseguradora y adquiere un seguro médico, cuya transacción está firmada digitalmente utilizando el formato de XAdES-EPES. Al no contar con un sellado de tiempo sobre la firma, no existe garantía legal para presumir que la hora en que se adquirió el seguro fue posterior a la hora en que dicha persona se quebró el pie. Queda como responsabilidad de ambas partes brindar evidencia que permita ubicar la transacción en el tiempo.

Otro riesgo de utilizar este formato, es que la firma digital podrá validarse en el tiempo mientras el certificado utilizado para realizar la firma no haya sido revocado o vencido y la entidad certificadora esté disponible. En caso de que posteriormente se revoque el certificado o cuando caduque, al no existir un sello de tiempo confiable no se puede verificar la validez del certificado en el momento en que se realizó la firma, sin recurrir a elementos probatorios adicionales que no poseen respaldo jurídico para presumir su veracidad.

Adicionalmente, la validación de la firma puede verse comprometida si los algoritmos, funciones o llaves utilizadas en el proceso de generación son expuestos a vulnerabilidades con el paso del tiempo.

2.4.3.2. XAdES-T

Se recomienda el uso del tipo XAdES-T para los escenarios que se requiera ubicar la firma digital en el tiempo. Esto se logra agregando un sello de tiempo obtenido de una autoridad confiable, que funciona como garantía oficial del momento en que se realizó la firma, lo que permitiría demostrar la validez del certificado haciendo uso de información adicional a la firma.

Además, debe ser utilizada cuando la información para validar la firma pueda ser obtenida por medios externos, ya que la firma en sí no contiene la cadena certificación ni la información de revocación.

- **Riesgos al utilizar XAdES-T:**

La firma digital realizada con este tipo podrá validarse en el tiempo mientras que la entidad certificadora esté disponible. En el momento en que la entidad certificadora deje de existir, no hay forma de verificar validez del certificado del firmante.

Adicionalmente, la validación de la firma puede verse comprometida si los algoritmos, funciones o llaves utilizadas en el proceso de generación son expuestos a vulnerabilidades con el paso del tiempo.

2.4.3.3. XAdES-XL

Se recomienda el uso del tipo XAdES-XL cuando es necesario validar la firma en cualquier momento, aun cuando la entidad certificadora no esté disponible. Esto se logra almacenando los valores de la respuesta OCSP, la lista CRL y los certificados en la firma, de manera que la información necesaria para validar el certificado se encuentra disponible dentro de la firma.

- **Riesgos al utilizar XAdES-XL**

La validación de la firma realizada con este formato, puede verse comprometida si los algoritmos, funciones o llaves utilizadas en el proceso de generación son expuestos a vulnerabilidades con el paso del tiempo.

El tamaño de las firmas digitales realizadas con XAdES-XL aumenta porque se almacenan la respuesta OCSP, la lista CRL y los certificados, por lo que se requiere de espacios de almacenamiento mayores conforme se archivan mayor cantidad de documentos firmados digitalmente.

2.4.3.4. XAdES-A

Se recomienda el uso del tipo XAdES-A para firmar documentos que van a ser utilizados en escenarios donde se pueda requerir verificar la firma en cualquier momento a futuro, por ejemplo en archivística y en ge-

neral en la conservación de cualquier documentación de valor científico cultural. En este tipo de firma se realizan sellados periódicos sobre la firma digital para garantizar la validez aun cuando los algoritmos utilizados para generar la firma original hayan sido comprometidos.

- **Riesgos al utilizar XAdES-A:**

Aún más que en el caso de XAdES-XL, conforme se generen y guarden más documentos firmados digitalmente, el espacio de almacenamiento puede crecer considerablemente debido al tamaño de la firma. Adicionalmente, el uso de este formato implica la implementación de un proceso periódico de re-sellado, el cual podría ser muy costoso en términos de procesamiento computacional, tiempo y costo de almacenamiento (conocido como *overhead*).

2.4.4. Otros riesgos

Es necesario aclarar que los riesgos explicados en la sección anterior son únicamente aquellos relacionados con la ausencia (o presencia) de ciertos datos en cada uno de los tipos de firma digital XAdES. Existen además otros riesgos que pueden presentarse al utilizar documentos electrónicos firmados digitalmente, relacionados con requerimientos del modelo de negocio que se está implementando y no con el uso de un formato de firma particular. Por ejemplo, el formato por sí solo podría no ser capaz de resolver disputas sobre temas como la fecha y hora en que se envió, recibió o procesó un documento, dado que la firma podría no necesariamente estar vinculada con dichos eventos.

A pesar de lo anterior, se debe señalar que si no se utiliza un formato de documento electrónico firmado digitalmente (como XAdES), capaz de presentar evidencia fehaciente de la ubicación del documento en el tiempo, validez del certificado digital en determinado momento, y otros, la resolución de estas disputas podría complicarse y quedaría sujeta a elementos ajenos a la firma digital. Sin embargo, se debe recordar que el solo hecho de utilizar un formato estándar de documento electrónico firmado digitalmente podría no ser suficiente, y que también se necesita un adecuado diseño de la solución y una utilización correcta de los elementos proporcionados por dicho formato para contar con evidencia robusta en caso de una disputa.

2.4.5. Tipos de firma XAdES descartados

2.4.5.5. XAdES-BES

XAdES-BES es el tipo más básico de XAdES. Los únicos elementos que diferencian una firma XAdES-BES de una firma XMLDSig son la fecha y hora de la firma, así como la referencia al certificado utilizado para generar la firma.

La principal razón por la que no se consideró el tipo XAdES-BES para formar parte de la propuesta de estándar de documento electrónico firmado digitalmente es que no tiene referencia explícita a una política de firma digital. La falta de una política de firma podría provocar que algunos elementos de implementación queden a discreción del implementador, lo que a su vez podría resultar en incompatibilidades entre diferentes implementaciones. Al ser la interoperabilidad uno de los principales objetivos de la presente investigación, el tipo XAdES-BES queda descartado por la falta de una referencia explícita a una política que norme algunos detalles de implementación, que serán discutidos más adelante.

2.4.5.2. XAdES-C

Las firmas de tipo XAdES-C contienen referencias a los elementos necesarios para verificar su validez, a saber, la cadena de certificación, las listas de revocación y las respuestas OCSP.

Existen dos razones por las que este tipo de firma XAdES fue descartado. La primera es porque, basado en la opinión de dos expertos consultados, XAdES-C existe principalmente a un nivel teórico para respetar una evolución incremental de los tipos, y no existen muchas aplicaciones prácticas que lo utilicen (Bosslet, 2011) (LeBlanc, 2010). La segunda razón por la que el tipo de firma XAdES-C fue descartado es porque, aunque la firma contiene las referencias a los elementos necesarios para su validación, los elementos en sí están en algún lugar externo a la firma, y la capacidad de validarla va a quedar sujeta a la disponibilidad de estos elementos. Esta disponibilidad muchas veces va ligada a la continuidad del funcionamiento de la CA responsable. En la mayoría de los casos esto no es problema, pero la idea de la inclusión de estas referencias es tener la capacidad de validar la firma en cualquier momento, lo que no está totalmente garantizado si se utiliza XAdES-C.

2.4.5.3. XAdES-X

Las firmas XAdES-X colocan un sello de tiempo sobre los elementos contenidos en el tipo XAdES-C. De esta forma, existe una garantía del momento en el que se consultó la cadena de certificación y la vigencia del certificado, lo que ofrece un mayor nivel de confianza en la validez de la firma, y además asegura la integridad de las referencias a los elementos de validación (LeBlanc, 2010). Sin embargo, este tipo de firma XAdES se descartó por las mismas razones por las que se descartó el tipo XAdES-C: dos de los expertos opinaron que no existen muchas aplicaciones prácticas que utilicen este tipo de firma (Bosslet, 2011) (LeBlanc, 2010), y no hay garantía total de la disponibilidad de los datos requeridos para validar la firma.

2.4.6. Tipos de envoltura XAdES

Existen diferentes tipos de envoltura de XAdES:

- Firma encapsulada, cuando la firma se encuentra dentro de un elemento del documento por firmar. Sólo se puede realizar sobre documentos XML.
- Firma encapsuladora, el documento se encuentra dentro de un elemento de la firma.
- Firma desacoplada, si la información firmada se encuentra en un documento distinto al elemento de firma. Existe la firma desacoplada externa, en la que la firma y el documento están en archivos diferentes, o desacoplada interna, en la que son “hermanos” dentro del mismo archivo.

Si se permite utilizar cualquier tipo de envoltura a discreción del generador del documento firmado, una organización que desee consumir dicho documento necesitaría desarrollar productos de software que acepten todos los tipos de envoltura. En la práctica, esto podría representar alcances más complejos, cronogramas más extensos y costos más altos para dichas organizaciones, quienes podrían optar por sólo utilizar uno o dos tipos de envoltura y omitir los otros que consideren de menor importancia para sus negocios.

Al igual que en secciones anteriores, y siempre con el objetivo de hacer una propuesta que potencie en el mayor grado posible la interoperabilidad de todas las futuras implementaciones y usos relacionados con firma digital, se decidió como parte de la investigación analizar y proponer la menor cantidad de configuraciones de envoltura XAdES razonables. Esta labor se realiza en el contexto de los posibles escenarios de uso expuestos previamente, de tal forma que los tipos de envoltura propuestos abarquen todos los escenarios de uso y los potencien o faciliten en tanto sea posible.

Producto de dicho esfuerzo de análisis de los tipos de envoltura y la revisión de la información recopilada a raíz de la investigación, se propone la utilización del tipo de envoltura desacoplada, siempre y cuando se observen las siguientes recomendaciones:

1. Para los nuevos desarrollos y siempre que sea posible, se recomienda utilizar la envoltura desacoplada almacenando el elemento de la firma y la información firmada en un mismo archivo.
2. Para los desarrollos existentes, y especialmente en los casos donde la alternativa anterior representa un costo que la organización no está en condiciones de asumir, se recomienda utilizar la envoltura desacoplada almacenando el elemento de la firma y la información firmada en archivos distintos.

En esta recomendación se contemplan todos los escenarios posibles de uso de firma digital en Costa Rica analizados previamente, ya que el tipo de envoltura desacoplada sirve para cualquiera de dichos escenarios.

El primer caso implica que cuando se desee intercambiar un documento firmado, sólo se transporte un único elemento digital que contiene tanto el documento original como el objeto de firma, lo que facilita su uso en aquellos escenarios donde personas físicas están involucradas directamente en la producción o el procesamiento de los documentos firmados. En el caso de la segunda alternativa que propone externamente desacoplada, se potencia el uso de XAdES en organizaciones que ya tienen o están en proceso con desarrollos utilizando XMLDSig para firmar documentos en el país.

La ventaja de que ambos escenarios sean atendidos por variantes de la envoltura desacoplada, radica en que la implementación de software requerida para poder consumirlos es muy similar, según la información recopilada durante esta investigación. Una organización que deseara poder recibir un documento firmado y encapsulado mediante cualquiera de los dos tipos de envoltura, realizaría el mismo procesamiento de los objetos que lo componen, únicamente variando la ubicación del objeto donde se aloja la firma.

Finalmente, el tipo de envoltura desacoplada se ajusta a los ideales de gestión documental que persigue la ciencia de la archivística. Un documento digital en archivística se conforma por un documento y sus metadatos, los cuales definen el contexto de dicho documento. En este escenario, la firma digital es un anexo o elemento de metadatos de un documento, y al separarlo del contenido mediante la envoltura desacoplada, se respeta esa visión de metadatos de archivística, lo que podría servir a las autoridades del Archivo Nacional en un futuro para apoyar sus esfuerzos en estandarizar la gestión de documentos digitales en el país

2.5. Documentos Técnicos Que Deben Crearse para Normar el Uso de XAdES en Costa Rica

Con el objetivo de potenciar la estandarización del uso de firma digital y la interoperabilidad entre todas las organizaciones y particulares que hagan uso de esta tecnología, y apoyados en las recomendaciones de la ETSI sobre el uso estandarizado de XAdES, el producto de esta investigación contempla la necesidad de la creación de una política y un perfil de firma digital que normen el contenido y la forma en que será utilizada a nivel nacional.

Actualmente no se cuenta con una especificación que defina la estructura que debe seguir un documento formal de política de firma; sin embargo, existe un grupo de especialistas de la ETSI trabajando en la propuesta del documento (Cruellas, 2010).

Por otro lado, la ETSI sí cuenta con un esquema (ETSI, 2002) en el cual se propone la estructura XML con el contenido esperado en una política de firma. Brasil se basó en este esquema para definir el documento que contiene las políticas de firma para su país (ICP Brasil, 2003).

Considerando la estructura base que debería tener una política de firma para un país, se recomienda que la elaboración de dicha política sea realizada por funcionarios de las autoridades correspondientes (Dirección de Certificadores de Firma Digital), que tengan la potestad de definir aspectos técnicos relacionados con el funcionamiento de la PKI nacional.

Además, para propiciar la interoperabilidad es necesario contar con un perfil orientado al escenario de aplicación. Este perfil tiene como objetivo orientar a los desarrolladores de aplicaciones para la implementación de firmas digitales compatibles entre sí. El alcance de un perfil de documento electrónico firmado digitalmente mediante XAdES se limita a establecer los elementos que el mismo contiene.

3. RECOMENDACIONES

Como resultado de esta investigación, se designa el formato XAdES como propuesta de formato de documento electrónico firmado digitalmente para Costa Rica, que deberá ser impulsado mediante la implementación de una política nacional al respecto por la Dirección de Certificadores de Firma Digital. Para su confección, se recomienda revisar constantemente los esfuerzos que la ETSI está trabajando, los cuales pretenden construir un estándar para la definición de políticas relacionadas con la adopción de formatos avanzados.

Para el desarrollo de aplicaciones interoperables en Costa Rica es necesaria la existencia de la política y la definición de un perfil base para la construcción de los documentos electrónicos firmados digitalmente. Se considera importante para Costa Rica que a nivel país se desarrollen librerías de formato abierto que cumplan con la política y perfil que se definan para el país, las cuales puedan ser utilizadas por las distintas instituciones tanto públicas como privadas para evitar esfuerzos aislados, con el fin de ahorrar tiempo y costos, y masificar el uso de la firma digital en Costa Rica.

En la entrevista realizada a Juan Carlos Cruellas se conversó sobre los eventos Plugtest, organizados por la ETSI, para probar la interoperabilidad de las soluciones que se implementan de acuerdo con los estándares desarrollados por la organización. Cruellas externó el interés de la organización por incluir a países latinoamericanos en esos eventos.

Una vez que se definan la política oficial y el perfil de firma digital oficiales para Costa Rica, se considera importante que instituciones con desarrollos de firma digital basados en los lineamientos nacionales participen en estos eventos, para verificar la interoperabilidad de las firmas digitales generadas en Costa Rica con respecto a otros países, y así mejorar las implementaciones en aras de buscar la interoperabilidad a nivel internacional.

4. CONCLUSIONES

En este documento se presenta el resultado del trabajo realizado para proponer un estándar de documento electrónico firmado digitalmente para Costa Rica. El producto resultante se utilizó como principal insumo para la elaboración de la “Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente”, emitida por la Dirección de Certificadores de Firma Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones, y oficializada mediante su anuncio en el Alcance Digital N° 92 de la edición N° 95 del Diario Oficial La Gaceta, el 20 de Mayo de 2013.

En primera instancia se realizó una investigación sobre el desarrollo de servicios de firma digital en el ámbito nacional. A partir de esta se determinó que la utilización de firma digital en Costa Rica se encuentra en una etapa inicial, donde no existen muchos desarrollos y la gran mayoría de ellos utilizan la firma digital simplemente para autenticar a los usuarios en sus sistemas.

Producto de esta investigación, también se identificó que los desarrollos de firma digital en el país todavía utilizan formatos desactualizados de documento electrónico firmado digitalmente como PKCS#7 y XMLDSig, por lo cual la incorporación de un formato con cualidades avanzadas como XAdES representa una oportunidad para brindar mayor seguridad a las aplicaciones desarrolladas y por desarrollar.

Posteriormente, se realizó una investigación sobre los formatos de documento electrónico firmado digitalmente utilizados alrededor del mundo. Como resultado de dicha investigación se logró determinar la tendencia mundial de utilizar la familia de formatos AdES como estándar en los desarrollos de firma digital y en la producción de los documentos electrónicos firmados digitalmente.

La información recopilada indicó que entre los países analizados el formato de preferencia es XAdES, debido a sus características inherentes de ser un formato estructurado y estar basado en XML. Sin embargo, la investigación también sirvió para demostrar que, aunque el formato más utilizado es el XAdES, en muy pocas ocasiones este formato tiene la connotación

de estándar de un país, producto de las debilidades que presenta en ciertos escenarios y las condiciones económicas y tecnológicas que varían en cada contexto.

Seguidamente, tomando como insumo las investigaciones realizadas, se identificaron las características que debe presentar el estándar de formato de documento electrónico firmado digitalmente para Costa Rica. Dichas características satisfacen los requerimientos que deben cumplirse para respetar las necesidades de firma digital del ámbito nacional, contemplando las mejoras prácticas establecidas en el contexto internacional. De igual forma al establecer las características, previo al análisis de los formatos de documentos electrónicos firmados digitalmente existentes, se establece un criterio de evaluación objetivo al cual deben someterse todos los formatos valorados.

Después, se sometieron los formatos de documento electrónico firmado digitalmente al criterio de evaluación establecido con las características identificadas. De dicha evaluación se determinó que existen tres formatos que cumplen a cabalidad con todas las características requeridas: XAdES, CAdES y PAdES. Los demás formatos analizados fallaron en cumplir la totalidad de características y por lo tanto dejaron de ser considerados como candidatos para la propuesta de estándar de formato de documento electrónico firmado digitalmente elaborada en este trabajo.

Luego, con el fin de seleccionar un formato entre los tres candidatos que superaron el filtro de las características, se identificaron escenarios donde pueden utilizarse documentos electrónicos firmados digitalmente y se analizó en cuáles de ellos es preferible utilizar un formato u otro. El análisis permitió identificar que no existe un formato óptimo para todos los escenarios, sino que cada formato candidato tiene ciertas ventajas dependiendo del escenario en que se utilice. Sin embargo, se determinó que el formato XAdES es el que presenta mejor se adapta en la mayoría de los escenarios y particularmente, es el que mejor se desempeña en los casos donde se requiere interoperabilidad. Por esta razón, se decidió escoger el formato XAdES como propuesta de estándar de formato de documento electrónico firmado digitalmente para Costa Rica.

Con el fin de propiciar la interoperabilidad, la propuesta realizada incluye no sólo la selección del formato de documento electrónico firmado digitalmente para Costa Rica (XAdES), sino que recomienda los tipos de XAdES que se deben utilizar, dependiendo del escenario en el que se utilicen. Se determinó que los tipos necesarios que se deben contemplar son: EPES, T, XL y A, dependiendo del peso probatorio que se le desee otorgar al documento electrónico firmado digitalmente y se explican los riesgos en los que se puede incurrir al utilizar los distintos tipos. Adicionalmente, se identificó que la envoltura apropiada para el formato del documento es

la desacoplada, recomendando internamente desacoplada para los nuevos desarrollos y externamente desacoplada para los desarrollos existentes. Al seleccionar el tipo de formato y envoltura se mejora la interoperabilidad entre las aplicaciones, ya que no se debe escoger entre tantas opciones, y al mantener una serie de tipos se permite que la complejidad de firmar digitalmente un documento se adapte de una manera adecuada a distintos escenarios y requerimientos.

También, se describieron las situaciones especiales donde el formato de documento electrónico firmado digitalmente XAdES no es la elección óptima. Esto permite evaluar la utilización del formato propuesto en escenarios donde podría utilizarse otro formato de una mejor manera, entendiéndose que si se elige utilizar otro formato se abandonan los beneficios de interoperabilidad. De esta forma en un escenario específico podría utilizarse un formato distinto a XAdES, siempre y cuando se cumpla con las características identificadas previamente y se tenga en cuenta que no se podrá interoperar con los sistemas que sí cumplen con el estándar propuesto.

Por último, se describió el trabajo futuro que debe darse para la adecuada implementación y uso del estándar de formato de documento electrónico firmado digitalmente propuesto, mediante la elaboración de una política nacional donde se establezca el formato oficial y los perfiles técnicos que se deben utilizar para su implementación en el país.

5. BIBLIOGRAFÍA

- ADAMS, Carlisle. y Steve Lloyd. 1999. *Core PKI Services: Authentication, Integrity, and Confidentiality* [en línea]. Estados Unidos de Norteamérica: Microsoft. Disponible en: <http://technet.microsoft.com/en-us/library/cc700808.aspx> [Consultado Abril 2011]
- ADAMS, Carlisle et al. 2001. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)* [en línea]. *The Internet Engineering Task Force (IETF)*. Disponible en: <http://tools.ietf.org/html/rfc3161> [Consultado Abril 2011]
- BLANCO Gir, David. 2010. **Política de Validación de Tractis** [en línea]. Tractis. Disponible en: <https://www.tractis.com/contracts/379026695> [Consultado Enero 2011]
- BLANCO Gir, David. 2011. [Correo electrónico]
- BRAVO Lilli, Cristian. s.f. **Modelos de Firma Electrónica Simple y su Auditabilidad** [en línea]. Chile: Ministerio Secretaría General de la Presidencia - Proyecto de Reforma y Modernización del Estado. Disponible en: [http://www.google.com/url?sa=t&rc=t=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCoQFjAA&url=http%3A%2F%2F163.247.57.117%2Fattachments%2F90%2FModelos%2520de%2520Firma%2520Electro%25CC%2581nica%2520Simple%2520y%2520su%2520Audita-bilidad%2520\(PPT\).pdf&ei=i3heU-SEM-exsQTy3IDwDA&usg=AF-QjCNHAbWaU4llzHMtxdbYT294fPJ7vpA&sig2=jNjhW5mI9UbZi-zUWQ2DVuQ&bvm=bv.65397613,d.cWc](http://www.google.com/url?sa=t&rc=t=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCoQFjAA&url=http%3A%2F%2F163.247.57.117%2Fattachments%2F90%2FModelos%2520de%2520Firma%2520Electro%25CC%2581nica%2520Simple%2520y%2520su%2520Audita-bilidad%2520(PPT).pdf&ei=i3heU-SEM-exsQTy3IDwDA&usg=AF-QjCNHAbWaU4llzHMtxdbYT294fPJ7vpA&sig2=jNjhW5mI9UbZi-zUWQ2DVuQ&bvm=bv.65397613,d.cWc) [Consultado Abril 2011]
- BOSSLET, Martin. 2011. [Correo electrónico]
- BOSSLET, Martin. 2011. [Conversación telefónica]
- BOSSLET, Martin. 2011. **Selección entre formatos AdES**. (C. Aguilar, A. Barquero, D. Chavarría, M. Fernández, & K. Solano, Entrevistadores)
- CARBALL Chavarría, Miguel Ángel. 2011. [Entrevista]
- CRUELLAS, Juan Carlos. 2011. [Conversación telefónica]
- CRUELLAS, Juan Carlos. 2010. **Selección entre formatos AdES**. (C. Aguilar, A. Barquero, D. Chavarría, M. Fernández, & K. Solano, Entrevistadores)
- Dictionary.com. 2011. *Digital Signature* [en línea]. Dictionary.com. Disponible en: <http://dictionary.reference.com/browse/digital+signature> [Consultado Abril 2011]

ETSI. 2002. *TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies* [en línea]. Unión Europea: Instituto Europeo de Estándares en Telecomunicaciones (ETSI). Disponible en: http://docbox.etsi.org/EC_Files/EC_Files/tr_102038v010101p.pdf [Consultado Abril 2011]

FDIC. 2009. *The Electronic Signatures in Global and National Commerce Act (E-Sign Act)* [en línea]. Federal Deposit Insurance Corporation (FDIC). Disponible en:

<http://www.fdic.gov/regulations/compliance/manual/pdf/X-3.1.pdf> [Consultado Abril 2011]

Gobierno de Costa Rica. 2005. *Ley de Certificados, Firmas Digitales y Documentos Electrónicos* [en línea]. Costa Rica: Asamblea Legislativa de la República de Costa Rica. Disponible en: http://www.bccr.fi.cr/marco_legal/leyes/Ley_Firma_Digital_No8454.pdf [Consultado Abril 2011]

Gobierno de España. 2003. *Ley 59/2003, de 19 de diciembre, de firma electrónica* [en línea]. España: Gobierno de España. Disponible en:

http://www.dnielectronico.es/marco_legal/ley_59_2003.html [Consultado Abril 2011]

ICPBrasil. 2003. *Requisitos Mínimos para Políticas de Assinatura Digital NA ICP-Brasil* [en línea]. Brasil: Instituto Nacional de Tecnología de Información. Disponible en: http://www.iti.gov.br/images/consulta-publica/encerradas/DOC-ICP-15.03_-_Requisitos_Minimos_para_Politicas_de_Assinatura.pdf [Consultado Abril 2011]

LEBLANC, David. 2011. [Correo electrónico]

LEBLANC, David. 2010. *Office 2010 Digital Signatures and XAdES* [en línea]. Estados Unidos de Norteamérica: Microsoft. Disponible en:

http://blogs.msdn.com/b/david_leblanc/archive/2010/05/30/office-2010-digital-signatures-and-xades.aspx [Consultado 30 de Mayo, 2011]

Liñánn Barreto, Araceli Paola. 2009. *Grafotecnia forense* [en línea]. Monografías. Disponible en:

<http://www.monografias.com/trabajos44/grafotecnia-forense/grafotecnia-forense.shtml> [Consultado Abril 2011]

MICITT. 2011. *Información General* [en línea]. Costa Rica: Gobierno de Costa Rica. Disponible en: <http://www.firmadigital.go.cr/info.html> [Consultado Abril 2011]

- PUIGPINOS, Julio César. 2010. *Formatos abiertos y Formatos propietarios* [en línea]. Formatos Abiertos. Disponible en: <http://www.openformats.org/es1> [Consultado Abril 2011]
- QIAN, Xiaolei y Gio Wiederhold. s.f. *Knowledge-based Integrity Constraint Validation* [en línea]. Estados Unidos de Norteamérica: Universidad de Stanford. Disponible en: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.1809&rep=rep1&type=pdf> [Consultado Abril 2011]
- ROUSE, Margaret. 2001. *Nonrepudiation* [en línea]. TechTarget. Disponible en: <http://searchsecurity.techtarget.com/definition/nonrepudiation> [Consultado Abril 2011]
- Word Reference. 2001. *Autenticidad* [en línea]. WordReference.com. Disponible en: <http://www.wordreference.com/definicion/autenticidad> [Consultado Abril 2011]