La conservación a largo plazo de firmas digitales auténticas: reflexiones para el debate desde el punto de vista archivístico

Alejandro Delgado Gómez
Servicio de Archivo y Bibliotecas del Ayuntamiento de Cartagena
alejandro@ayto-cartagena.es

Introducción

La presente exposición aborda el problema de la conservación de firmas electrónicas, más allá del punto en que éstas autentican un documento, u objeto similar a documento, durante un plazo no definido, que depende de las necesidades y los intereses del creador, gestor o conservador de tal documento. Por ejemplo, es muy probable que la conservación de la firma electrónica que valida el pago de una compra en un supermercado sea necesaria para el comprador sólo hasta que se sale del supermercado, y para el vendedor sólo hasta que el banco del comprador hace eficaz el pago. Sin embargo, puede que sea necesario conservar la firma electrónica que valida un testamento o un proyecto urbanístico durante veinte, treinta, cincuenta o cientos de años, dependiendo, no sólo de necesidades organizativas y legales, sino también individuales y sociales. Existen varios motivos por los que se podría argumentar de manera concebible la afirmación de que las firmas electrónicas no han sido concebidas para perdurar a tan largo plazo, siendo el más evidente de ellos la evolución tecnológica, y la obsolescencia tecnológica asociada. Sin embargo, la presente exposición no aborda el problema mencionado desde la perspectiva exclusivamente tecnológica, sino en combinación con las necesidades de evidencia, tal y como son enunciadas, por ejemplo, en ISO 15489, y de conservación, tal y como son enunciadas, por ejemplo, en el Proyecto InterPARES, de los documentos, u objetos similares a documentos, de archivo. Desde este punto de vista, diversos autores han puesto de manifiesto, a partir de posiciones teóricas divergentes, el hecho de que la delineación y la autenticación de la identidad del firmante es problemática incluso en entornos analógicos[1]. Este

[1] Confróntense, por ejemplo, Cullen, Charles T: "Authentication of Digital Objects: Lessons from a Historian's Research". En: *Authenticity in a Digital Environment*. Washington D.C.: Council on Library

carácter problemático, por supuesto, se incrementa en entornos digitales distribuídos y de límites imprecisos, poblados además por objetos frecuentemente precarios, y desde el punto de vista del archivo, de carácter más lógico que físico. La presente exposición aborda algunos de las inseguridades detectadas, en lo que concierne a la conservación auténtica de firmas electrónicas, en tales entornos. De la dilucidación de tales inseguridades no se deriva la afirmación de que no deban utilizarse firmas electrónicas, primero, porque constituyen una realidad incuestionable; y, segundo, porque no utilizarlas supondría una regresión en la mejora de los procesos organizativos. Simplemente, se deriva la afirmación de que deben extremarse las precauciones técnicas y tecnológicas para incrementar la posibilidad de conservar tales firmas en forma auténtica durante un plazo no determinado a priori.

La inseguridad que la presente exposición aborda con mayor detalle es, como se desprende de su título, la de la conservación de componentes que deben asegurar que un documento digital es auténtico, no sólo ahora, sino en el curso del tiempo y el espacio, siendo estos componentes por sí mismos extremadamente perecederos. No obstante, también se mencionan en filigrana algunos otros problemas, interrelacionados de manera más o menos obvia con el problema de la conservación: la precariedad de las cadenas de confianza, la incorporación de intereses económicos en los procesos de asignación de firma, la ilegibilidad y caducidad de las firmas en plazos no especificados, la carencia de semántica de las firmas electrónicas, la combinación de elementos puramente técnicos con los procesos sociales de asignación de confianza, y el grave problema de los potenciales fraudes de identidad en red.

Para mantener bajo control estas potenciales fuentes de conflicto se están desarrollando tecnologías como procesos de refirmado o asignación de sellos de tiempo asociados a las firmas. Estas tecnologías, si bien acertadas, están fuertemente vinculadas a su momento, es decir, como se intentará sugerir más adelante, son tan fugaces como el objeto a proteger. En contraste con las mismas, la presente exposición quiere sugerir una técnica –o, desde el punto de vista archivístico- actividad, que es independiente del objeto y del proceso, en la medida

---

and Information Resources, 2002. P. 1-7; O'Toole, James M.: "On the Idea of Uniqueness". En: *The American Archivist*. Vol. 57, n. 4 (Fall 1994). P. 632-658.

en que se aplica a todos ellos a lo largo de todo su rango de vida. Se trata de la actividad continuada de asignación de metadatos a los objetos, agentes, funciones y procesos que intervienen en la creación, gestión y uso de los documentos de archivo, con el fin de garantizar la evidencia a efectos de responsabilidad y memoria. Esta perspectiva está basada en las propuestas de encapsulación de objetos de metadatos derivadas de los trabajos de, especialmente, David Bearman, orientados específicamente a la articulación de las condiciones de autenticidad del documento; y de Chris Hurley, orientados al uso de la descripción archivística como garantía de evidencia[2]; la finalidad de esta perspectiva es conservar la firma unida de la manera más inextricable posible a sus metadatos, de tal manera que, si finalmente la firma no es conservable (en el sentido, no de mero almacenamiento del objeto, sino de conservación auténtica para su legibilidad e interpretación), se le pueda proporcionar al menos continuidad a su significado, expresado mediante metadatos.

Por supuesto, este planteamiento no es novedoso, no es el único posible, y está sujeto a discusión, aunque goza de cierto grado de consolidación en el entorno archivístico y se ha tomado en cuenta para desarrollar normas y proyectos, bien de marcado carácter no archivístico, como ISO/TR 18492[3], bien con profundas connotaciones archivísticas, como Victorian Records Electronic Strategy, VERS[4]. Sería finalidad de la presente exposición el que este planteamiento generara igualmente reflexión y debate en el marco de las Jornadas en que se inscribe y, más allá, en las profesiones de la información asociadas a la gestión de firmas electrónicas en general.

---

[2] Confróntense, por ejemplo, Bearman, David: *Functional Requirements for Evidence in Recordkeeping*. University of Pittsburgh, School of Information Sciences. URL: http://web.archive.org/web/20000818163633/www.sis.pitt.edu/~nhprc/ (Consulta: 27-10-2007); Hurley, Chris: *Relationships in Records*. URL: http://www.sims.monash.edu.au/research/rcrg/publications/relationships-in-records-rev-3b.rtf (Consulta: 27-10-2007).

[3] *ISO/TR 18492:2005: Long-term preservation of electronic document-based information*. Geneva: Organización Internacional de Normalización, 2005.

[4] *Specification 3: VERS Standard Electronic Record Format*. URL: http://www.prov.vic.gov.au/vers/standard/spec_03/ (Consulta: 27-10-2007).

Alcance y definiciones

La técnica de asignación de firmas electrónicas, en conjunción con la necesidad de mantener la evidencia en plazos que no siempre están especificados, puede considerarse desde diferentes perspectivas, desde luego interrelacionadas, pero no siempre atentas a los mismos intereses. Dos perspectivas obvias, y de manera frecuente protagonistas, son la tecnológica y la jurídica. Sin embargo, tales perspectivas no coinciden de manera inequívoca con el punto de vista archivístico, en la medida en que, por una parte, el archivo es independiente de la tecnología, y crea, gestiona, conserva y pone en uso documentos con las tecnologías disponibles en cada momento; y, por otra, es también independiente de la noción legal de evidencia, puesto que la evidencia archivística tiene un alcance más amplio y social que la mera evidencia en los tribunales. Existe, pues, una primera restricción de alcance en la presente exposición, que no atiende a criterios exclusivamente tecnológicos y jurídicos, sino, sobre todo, a criterios archivísticos[5].

Por lo demás, si revisamos definiciones convencionales del objeto que nos ocupa, seremos capaces de establecer alguna otra restricción de alcance. En primer lugar, una firma es "el nombre o marca especial de una persona, fijado por la mano de una persona o por su agente autorizado sobre un documento, al efecto de aceptar la responsabilidad, aprobar, o validar todo o parte de su contenido"[6]. En diplomática, una firma es tradicionalmente uno de los componentes fundamentales que garantizan, bajo determinadas condiciones y en combinación unos componentes con otros, que un documento es auténtico. La traslación de la noción de firma al entorno digital es, también por convención, la siguiente, en lo que concierne a firmas electrónicas: "una marca digital que tiene la función de una firma en, está adjunta a, o lógicamente asociada con, un documento, y es utilizada por un firmante para asumir la responsabilidad de, o para dar consentimiento a, el contenido del documento"[7]. Por una parte, esta definición tiene la ventaja de que permite englobar técnicas específicas de implantación muy diversas, desde el rústico y poco fiable (aunque utilizado) sistema de insertar una imagen escaneada

[5] Confróntese, por ejemplo, Reed, Barbara: "Registros". En: McKemmish, Sue, Piggott, Michael, Reed, Barbara, Upward, Frnak (eds.): *Archivos: gestión de registros en sociedad*. Cartagena: Ayuntamiento: 3000 Informática, 2007.

[6] InterPARES 2 Project: *Terminology Database*. URL: http://www.interpares.org/ip2/ip2_terminology_db.cfm (Consulta: 27-10-2007).

[7] Cit.

de una firma manual en un documento de Word, hasta las técnicas de firma digital basadas en infraestructuras de clave pública. Por otra parte, sin embargo, deja la puerta abierta a la consideración de cualquier tipo de identidad digital, desde un nick en un chat o un alias de correo electrónico hasta las más sofisticadas técnicas mencionadas. Aunque este amplio abanico es terriblemente interesante y daría pie a explorar nociones como las de identidad, validez, documento o autenticidad en diferentes contextos, queda fuera del alcance de las presentes Jornadas, de modo que es posible establecer una segunda restricción, mediante la propuesta de una tercera definición, la de firma digital, que es "una firma electrónica basada en criptografía de clave pública"[8]. En el resto de la presente exposición, pues, haremos mención, no de las firmas electrónicas, sino de las firmas digitales, que son una implantación particular de aquéllas y se utilizan frecuentemente en los entornos organizativos objeto de las presentes Jornadas.

Como se adelantó, una firma es uno de los componentes que indican, en principio, que un documento es auténtico, de modo que tal vez convenga definir también qué se entiende por autenticidad, desde el punto de vista organizativo: "la confiabilidad de un documento como tal documento; esto es, la cualidad de un documento de que es lo que pretende ser y de que está libre de fraude o corrupción"[9]. De acuerdo con las ontologías elaboradas en el marco del Proyecto InterPARES, el grado de autenticidad es sólo uno de los tres componentes que garantizan la confiabilidad, siendo los otros dos la fiabilidad, que se obtiene examinando la completitud y el procedimiento de creación de los documentos; y la exactitud, que se obtiene examinando la medida en que un documento es preciso, correcto, verdadero y pertinente[10]. Aunque se trata de componentes interrelacionados, la presente exposición sólo aborda el componente auntenticidad, aproximándose a la fiabilidad y la completitud únicamente cuando vengan requeridos por la noción de autenticidad. En cualquier caso, la autenticidad de un documento viene dada por la capacidad para conservar otros dos componentes: su identidad, o "todas las características de un documento o un registro que lo identifican de manera única y lo distinguen de cualquier otro documento o registro"[11], y su integridad, o "la

[8] Cit.

[9] Cit.

[10] InterPARES 2 Project: *Concept of the Trustworthiness of a Record: Ontology C*. URL: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_ontology.pdf (Consulta: 27-10-2007)

[11] InterPARES 2 Project: *Terminology Database*, cit.

cualidad de estar completo e inalterado en todos los aspectos esenciales"[12]. Este conjunto de definiciones, si bien fuertemente basado en la teoría diplomática y con cierto grado de complejidad conceptual, es, a nuestro juicio, más exhaustivo que la noción de autenticidad definida en ISO 15489: "un documento auténtico es aquél del que se puede probar: a) que es lo que afirma ser; b) que ha sido creado o enviado por la persona que se afirma que lo ha creado o enviado; y c) que ha sido creado o enviado en el momento que se afirma"[13]. No obstante, debe reconocerse que esta segunda definición, proporcionada por ISO, es mucho más inmediata que la definición de InterPARES. Sin embargo, en combinación con otras propiedades del documento expresadas en la norma, como la exactitud concebida como correspondencia con los hechos; así como con una definición convencional de fraude[14], el concepto de autenticidad de ISO 15489 no disipa la posibilidad de tal fraude.

En lo que concierne a la presente exposición, y una vez definidos los conceptos creemos que centrales, la hipótesis de trabajo consistiría en la afirmación de que no es posible utilizar las firmas digitales para conservar documentos auténticos a largo plazo, porque no es posible tampoco conservar tales firmas digitales. Aunque existe un motivo empírico y de puro sentido común, como es el hecho de que ninguna firma digital tiene aún la edad suficiente como para verificar o falsar tal hipótesis, conviene, sin embargo, refinar en cierta medida la afirmación anterior. Así, en primer lugar, definiremos conservación como "todos los principios, políticas y estrategias que controlan las actividades diseñadas para asegurar la estabilización física y tecnológica y la protección del contenido intelectual de los materiales (datos, documentos o registros)"[15]; y largo plazo, o, de manera más estricta, longevidad, como "vida larga; larga duración de la existencia"[16]. Por supuesto, la implantación específica de las nociones de conservación y longevidad, como de

[12] Cit.

[13] *ISO 15489-1: Información y documentación – Gestión de documentos. Parte 1: Generalidades*. Madrid: Aenor, 2006. P. 10.

[14] De acuerdo con el Diccionario de la Real Academia, fraude es, en primera acepción, una "acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete"; y en segunda, un "acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros". URL: http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=fraude (Consulta: 8-11-2007)

[15] InterPARES 2 Project: *Terminology Database*, cit.

[16] Cit.

todas las demás definidas, es puramente contextual[17], pero de sus definiciones cabe derivar de manera argumentable la aseveración de que la conservación a largo plazo consiste en la adopción de medidas para garantizar que el contenido de los documentos –y nosotros añadiríamos que también su contexto, estructura en la medida de lo posible, forma y comportamiento[18]- sigue siendo el mismo, o, con mayor rigor, que se rinde de la manera en que una comunidad dada espera que se rinda, y que esto sucede bajo las condiciones de autenticidad aceptadas por esa comunidad, a lo largo del tiempo y el espacio. Es precisamente este tipo de conservación el que las firmas digitales no pueden abordar, como esperamos explicar en lo que sigue.

Noción de firma digital y problemas archivísticos asociados

El problema de la conservación a largo plazo de firmas digitales como componentes que dan fe de la autenticidad del documento ha sido ampliamente explorado y no esperamos decir nada original al respecto. En esta y las siguientes secciones, por tanto, haremos amplio uso del método de la garantía literaria, antes de proceder a exponer nuestra propia propuesta. Así, Filip Boudrez, a partir del examen de la compleja estructura de las firmas digitales avanzadas y sus procesos asociados, concluye que éstas no garantizan ni la identidad ni la integridad de los documentos[19]. De acuerdo con el autor belga, una firma digital avanzada no es un objeto simple, sino un conjunto de objetos y procesos, tanto internos como externos: una clave pública y otra privada, una autoridad externa de certificación

[17] Confróntese, por ejemplo, Thibodeau, Kenneth: "Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years". En: *The State of Digital Preservation: An International Perspective : Conference Proceedings Documentation Abstracts, Inc. Institutes for Information Science. Washington, D.C. April 24-25, 2002*. Washington D.C.: Council on Library and Information Resources, 2002. P. 4-31.

[18] En relación con la noción de comportamiento de los documentos digitales, confróntese, por ejemplo, *From digital volatility to digital permanence: Preserving databases*. The Hague: Digital Preservation Testbed, 2003. En general, todos los documentos del testbed holandés asumen esta noción. URL: http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-databases-en.pdf (Consulta: 27-10-2007). El matiz de la forma para los documentos digitales es introducido en Ketelaar, Eric: "Time future contained in time past: Archival science in the 21st century". En: *Journal of the Japan Society for Archival Science*. N. 1 (2004). P. 20-35.

[19] Boudrez, Filip: *Digital signatures and electronic records*. Antwerpen: Expertisecentrum DAVID vzw, 2005.

que valida ese par de claves, un proceso de conversión de un fichero a un cierto tipo de código basado en un algoritmo externo, ese algoritmo, el valor hash producido por el algoritmo, el proceso de encriptación del valor hash y la clave privada, el objeto firma resultante, el proceso de asignación de la firma al documento, el proceso de transmisión, el proceso de desencriptación, el proceso de recalcular el valor hash y de chequeo del mismo, el certificado digital que asegura que la clave pertenece a este emisor y no a otro, y la autoridad externa con capacidad para emitir estos certificados digitales. Probablemente de la anterior enumeración han desaparecido algunos objetos y procesos, pero esto no es lo interesante. Lo realmente interesante del complejo procedimiento para generar y utilizar una firma digital es el hecho de que esa firma digital, que debe validar documentos que son distribuídos, compuestos y perecederos, es ella misma un objeto distribuído, compuesto y perecedero. Es decir, de la enumeración anterior cabe derivar de manera argumentable que, en el momento de plantear una política de conservación de firmas digitales, deben tenerse en cuenta, desde el punto de vista archivístico, aspectos tales como:

- La dependencia de la validez de la firma digital de autoridades externas, que pueden ser duraderas o no serlo, cambiar de denominación o de competencias, ser públicas o privadas -con el consecuente peligro de la intromisión de intereses económicos-, etc., de tal modo que las propias cadenas de confianza pueden ponerse en cuestión, y mucho más si tienen que ser sostenibles, a efectos archivísticos, a largo plazo[20].

- La orientación de la firma digital hacia la transmisión segura de datos, no de documentos. Un documento digital está compuesto, por supuesto, por datos, pero no es equivalente a esos datos, sino a esos datos, más su contexto de creación, más su estructura mientras ésta se pueda mantener, más la forma mediante la que se reconoce ese documento, más su comportamiento. Todo esto es lo que conforma la identidad del documento, uno de los componentes esenciales de su autenticidad. La forma y la estructura mediante las que un

[20] Confróntese, por ejemplo, Iacovino, Livia, McKemmish, Sue: "Informe del Equipo de Investigación Australiano". En: Duranti, Luciana (ed.): *La conservación a largo plazo de documentos electrónicos auténticos: hallazgos del Proyecto InterPARES*. Cartagena: Ayuntamiento: 3000 Informática, 2005. P. 163-169.

documento digital refleja su identidad no tienen por qué ser siempre las mismas, y de hecho es imposible que lo sean, a medida que se produzcan procesos de migración. Estos procesos de migración generarán secuencias de bits diferentes, sin que ello implique que el documento pierde su identidad, si su contenido y sus circunstancias contextuales siguen siendo reconocibles. Pero, puesto que la firma digital protege secuencias de bits, datos en el momento de la transmisión, y no documentos, no puede garantizar la identidad y, en consecuencia, la autenticidad de los mismos[21].

- Esta misma orientación de la firma digital hacia la transmisión segura de datos impide garantizar la integridad del documento, sólo garantiza la integridad de una secuencia de bits en el momento en el que esta secuencia de bits se transmite. Como se ha argumentado en el párrafo anterior, el motivo reside en el hecho, bien admitido por parte de diversos proyectos de investigación de diversa orientación, como InterPARES o el Proyecto Pittsburgh, de que los documentos digitales no pueden conservarse, sólo puede conservarse la capacidad para reproducirlos, y para conservar esta capacidad es preciso alterar las propiedades de los documentos, supuesto que sus condiciones de autenticidad, o su contenido o significado, dependiendo de la orientación que se adopte, siguen siendo los mismos[22]. La firma digital, pues, garantiza que una secuencia de bits es íntegra en un punto del tiempo, no que un documento digital conserva su integridad a lo largo del tiempo.

- Además, desde el punto de vista archivístico, y a efectos de garantizar la autenticidad, las firmas son por naturaleza personales, irrevocables y no tienen fecha de caducidad[23]. Las tecnologías que han desarrollado

[21] Confróntese Boudrez, cit. P. 4-5.

[22] Confróntese, por ejemplo, "Informe del Grupo de Trabajo sobre Autenticidad". En: Duranti, Luciana, (ed.): *La conservación a largo plazo de documentos electrónicos auténticos*, cit. P. 25-82; Bearman, David: *Electronic Evidence: Strategies for Managing Records in Contemporary Organizations*. Pittsburgh: Archives & Museums Informatics, 1994; Suderman, Jim: *Estructurar el paradigma de conservación: un informe sobre los hallazgos del Proyecto InterPARES*. P. 5. URL: http://archivo.cartagena.es/recursos/texto0_suderman_01.pdf (Consulta: 27-10-2007); Boudrez, cit. P. 5-6.

[23] Confróntese Currall, James: "Digital Signatures: not a solution, but simply a link in the process chain". En: *Proceedings of the DLM-Forum 2002: access and preservation of electronic information: best practices and solutions*. Luxembourg: Office for Official Publications of the European Communities, 2002.

procedimientos de firma digital avanzada no tienen en cuenta estas tres propiedades: las firmas digitales se pueden revocar y caducan, por motivos de seguridad. De manera más alarmante, en ningún momento garantizan que la firma y los certificados asociados están unidos de manera inextricable a la persona X, sino a cualquiera que esté en posesión de la clave privada, lo cual incrementa el riesgo de fraude de identidad digital. De hecho, el uso de firmas digitales resultaría más prudente si se estableciera la analogía, no con las firmas analógicas, sino con los sellos analógicos, que no plantean problemas de identidad personal, sino corporativa, es decir, a un mayor nivel de generalidad[24].Téngase en cuenta que la firma analógica posee tradicionalmente una riqueza semántica de la que carece la firma digital, es decir, un firmante no sólo se hace responsable, también testifica, refrenda, da el visto bueno, etc., matices todos ellos que desaparecen al utilizar firmas digitales[25]. Los sellos analógicos carecen también de esta riqueza semántica, simplemente autentican en un punto del tiempo, no mantienen la autenticidad en el curso del tiempo y del espacio, y pueden considerarse como un tipo simple de firma electrónica que no es firma digital[26].

- La fuerte dependencia de la firma digital del desarrollo de la tecnología. Es decir, la firma digital es una solución tecnológica, pero las tecnologías evolucionan, se quedan obsoletas, son substituídas, y procedimientos de firma digital que no evolucionen de manera concomitante están condenados a generar firmas que en un futuro no definido resulten ilegibles y, por tanto, inutilizables a efectos de autenticidad. Así, por ejemplo, la muy activa

---

P. 499-507; Boudrez, cit. P. 4. El DLM-Forum del año 2002, celebrado en Barcelona, ya adelantaba varias aproximaciones interesantes a los aspectos técnicos y legales asociados a la firma digital.

[24] Confróntese Currall, James, cit.

[25] Confróntese Lynch, Clifford: "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust". En: Authenticity in a Digital Environment. Washington D.C.: Council on Library and Information Resources, 2002. P. 32-50.

[26] Confróntese la definición de sello y de sello electrónico proporcionada por el Proyecto InterPARES: "Una pieza de cera, plomo u otro material sobre el que se ha hecho una impresión y que se adjunta a un documento o se aplica a su superficie. Originalmente sirvió como un medio de autenticación del autor de un documento y del documento mismo. Un sello electrónico es un medio para autenticar un documento y a su autor, o un medio para proteger la confidencialidad del documento asegurando que el documento sólo es abierto por el destinatario pretendido. Es un tipo distinto de firma electrónica". *Terminology Database*. URL: http://www.interpares.org/ip2/ip2_terminology_db.cfm (Consulta: 8-11-2007)

Computer Security Division del National Institute of Standards and Technology (NIST) ya desaconsejaba en 2004 el uso de mecanismos como MD5 y la substitución de SHA-1 por SHA-256 y SHA-512[27]. Como se sabe, MD5, o Message Digest 5, 128 bits, es el algoritmo que genéricamente substituyó a MD4, después de detectarse debilidades en éste. Según parece, desde 1996 se están detectando también colisiones, o un solo *output* para dos *inputs* diferentes en una función hash, en MD5. Por su parte. SHA-1 (o, como se sabe, algoritmo hash seguro, utilizado por la administración norteamericana) parece haber sufrido ataques desde 2004, por lo que su substitución por la familia SHA-2 parecería recomendable a corto plazo[28]. En cualquier caso, lo interesante no son los intrincados vericuetos tecnológicos de este proceso de substitución, sino el acelerado proceso de substitución mismo, del que sus responsables y protagonistas parecen no ser conscientes.

Por los motivos indicados, pues, y en lo que concierne a la presente exposición, diríase que las firmas digitales, o, en sentido estricto, la función de provisión de autenticidad de las mismas, sólo son útiles para autenticar una transmisión de datos en un punto dado del tiempo, lo cual no es poco, ya que en el actual entorno digital se ha convertido casi en un axioma el afirmar que cada vez que los datos se mueven en el tiempo o el espacio quedan expuestos a riesgo[29]; pero no permiten garantizar la autenticidad de documentos digitales a lo largo del tiempo y del espacio. No obstante, puesto que se generan documentos digitales con firmas asociadas a los mismos, debiera explorarse algún tipo de solución a la conservación auténtica, bien de los documentos, bien de las firmas asociadas, bien de ambos. A esbozar algunas propuestas elaboradas hasta el momento se aplica la siguiente sección de la presente exposición.

---

[27] Boudrez, cit. P. 7. Por lo demás, una fuente particularmente aconsejable para adquirir consciencia del grado en que la utilidad de las firmas digitales puede verse seriamente dañada por el paso del tiempo es la propia página de publicaciones de la citada Computer Security Division del NIST: http://csrc.nist.gov/publications/index.html (Consulta: 27-10-2007).

[28] Burr, William E.: *NIST Comments on Cryptanalytic Attacks on SHA-1*. URL: http://csrc.nist.gov/groups/ST/hash/statement.html (Consulta: 27-10-2007); *Tentative Timeline of the Development of New Hash Functions*. URL: http://csrc.nist.gov/groups/ST/hash/timeline.html (Consulta: 27-10-2007).

[29] Confróntese: Informe del Grupo de Trabajo sobre Estrategia. En: Duranti, Luciana, (ed.): *La conservación a largo plazo de documentos electrónicos auténticos*, cit. P. 155.

La conservación archivística de documentos digitales autenticados mediante procedimientos de firma digital

En años recientes, y sobre todo desde que la firma digital comenzó a ser regulada por ley a diferentes niveles de competencia, se han propuesto diversos métodos para conservar, o bien la propia firma digital, o bien el significado de la misma, es decir, su propiedad de validación de la autenticidad de los documentos. Tales métodos cubren un amplio abanico que comprende desde la eliminación de la firma en el momento de su paso al archivo hasta la conservación de todos sus componentes en un proceso hasta cierto punto similar al de la emulación del hardware y el software. Así, por ejemplo, aproximaciones como las de los archivos nacionales finlandeses, holandeses, canadienses y, parcialmente, de los Estados Unidos, contemplan la posibilidad de, e incluso obligan a, en el caso de Canadá, eliminar la firma una vez que ha cumplido su finalidad de autenticar una transmisión a corto plazo. En el caso de Canadá, se adopta esta aproximación sobre la base de que una firma cumple simplemente la función protectora de un sobre u otro envoltorio, de tal modo que no es relevante a efectos de conservación a largo plazo de la autenticidad o del significado del documento[30]. La aproximación estadounidense permite la conservación de la firma digital, siempre que también se conserven de forma inmediatamente legible el nombre del firmante y la fecha de la firma[31]. La aproximación finlandesa se apoya en el uso de un sistema de registro muy sólido que proporciona los metadatos necesarios para asegurar la identidad e integridad del documento, deviniendo de tal modo la conservación de la firma innecesaria[32]. Esta es también, en cierto modo y como se expondrá más tarde, la aproximación de la presente exposición: en ausencia de garantías de que la firma será conservable con significado, debieran establecerse procedimientos reglados de asignación de metadatos, mediante un sistema de registro o cualquier otro que se

[30] *Guidelines For Records Created Under a Public Key Infrastructure Using Encryption And Digital Signatures*. URL: http://www.collectionscanada.ca/information-management/002/007002-3015-e.html (Consulta: 27-10-2007).

[31] *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*. URL: http://www.archives.gov/records-mgmt/faqs/pdf/electronic-signiture-technology.pdf (Consulta: 27-10-2007)

[32] Pohjola, Raimo: "Implications of electronic signatures — the situation in Finland: The act on electronic service in the administration and the act on electronic signature". En: *Proceedings of the DLM-Forum 2002*, cit. P. 490-494.

determine formalmente, para que estos metadatos sirvan como tal garantía de autenticidad. Si bien se ha argumentado que este procedimiento desplaza la responsabilidad desde el certificado digital hacia el proceso de asignación de metadatos[33], la diferencia reside en el hecho de que, en este segundo caso, la autenticidad no dependería de cadenas de confianza precarias, sino de un proceso continuo ejercido por el archivo, en cuanto tercera parte fiable.

En el otro extremo del espectro, Dumortier y Van den Eynde proponen, a partir de la evidencia de que conservar sólo el documento y su firma no es suficiente, la conservación de todos los componentes asociados a la firma digital, incluídos el hardware y el software de conservación y uso, junto con componentes adicionales, como un sello de tiempo que justifique inmediatamente antes del uso de la firma la posesión de un certificado que la valide, o una validación o refirmado permanente de todo proceso de migración[34]. Desde el punto de vista archivístico, esta aproximación plantea varias prevenciones, algunas de las cuales, paradójicamente, vienen recogidas por los propios autores. Así, por ejemplo, un proceso de refirmado genera un documento por completo diferente, en el mejor de los casos similar a una copia certificada, y, aunque en un entorno digital el principio de mejor evidencia queda notablemente relativizado, susceptible de ser rechazado a efectos jurídicos o a efectos de garantía de la propiedad de no repudiación, dentro o fuera de un tribunal. Bien es cierto que se puede contra-argumentar que la no repudiación no es una propiedad intrínseca de la firma digital, sino, más bien, que ésta es un medio que contribuye a aquélla, pero para esto tendríamos que salir fuera del diseño de investigación propuesto por los autores[35], es decir, incorporar al diseño los fuertes mecanismos sociales de asignación de confianza que acompañan a todo mecanismo puramente tecnológico[36]: básicamente, a partir del argumento de que cualquiera que esté en posesión de la clave privada puede firmar un documento, una firma digital deviene tan repudiable como una firma analógica. Por

[33] Confróntese Dumortier, Jos, Van den Eynde, Sofie: "Electronic signatures and trusted archival services". En: *Proceedings of the DLM-Forum 2002*, cit. P. 520-524.

[34] Dumortier, Jos, Van den Eynde, Sofie, cit.

[35] Confróntese Adams, Carlisle, Lloyd, Steve: *Understanding Public-Key Infrastructures: Non-Repudiation*; y, desde otra perspectiva, McCullagh, Adrian, Caelli, William: "Non-Repudiation in the Digital Environment". En: *First Monday*. Vol. 5, n. 8 (7 August 2000). URL: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/778/687 (Consulta: 27-10-2007)

[36] Lynch, Clifford, cit.

lo demás, cualquier solución orientada por la tecnología corre los mismos riesgos explicados más arriba con respecto a la firma digital. Finalmente, la emulación es una técnica sometida aún a muchos interrogantes, de costes imprecisos y, en la fase de conocimiento actual, forzada a un proceso de escalabilidad *ad infinitum*. De hecho, incluso ha dejado de ser tomada en consideración en ciertas normas técnicas bien consolidadas[37]. Sorprende, pues, la lucidez con la que los autores cuestionan algunos de los mecanismos de conservación, como la canonicalización XML[38], sobre la base de su fugacidad y carácter infinito, mientras que apoyan otros, igualmente fugaces e infinitos.

Una aproximación intermedia, por último, es la australiana, cuyos Archivos Nacionales no conservan documentos encriptados, pero reconocen la posibilidad de conservar las firmas, junto con los metadatos, que son los componentes que realmente proporcionan evidencia, así como el derecho del firmante a conservar los componentes originales[39].

Es la tarea a la que se aplica la siguiente sección la breve descripción de la aproximación basada en el uso de metadatos para la conservación, no tanto del objeto firma o de los componentes que lo constituyen, sino más bien de su significado como garantía de autenticidad.

Los metadatos como procedimiento para garantizar la autenticidad de los documentos digitales y sus firmas asociadas

Las soluciones basadas en la asignación de metadatos como medio para garantizar la autenticidad de los documentos no son novedosas, y se ha estado insistiendo en ellas al menos desde mediados de los años noventa del siglo veinte, estando en la

[37] Confróntese, por ejemplo, *ISO/TR 18492:2005*, cit.

[38] Acerca del concepto de canonicalización, confróntese, por ejemplo, Lynch, Clifford: "Canonicalization: A Fundamental Tool to Facilitate Preservation and Management of Digital Information". En: *D-Lib Magazine*. Vol 5, n. 9 (September 1999). URL: http://www.dlib.org/dlib/september99/09lynch.html (Consulta: 27-10-2007). Información acerca de XML canónico puede obtenerse en: *Canonical XML. Version 1.0*. URL: http://www.w3.org/TR/2001/REC-xml-c14n-20010315 (Consulta: 27-10-2007).

[39] Confróntese: National Archives of Australia: *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication or Encryption*. Canberra: National Archives of Australia, 2004; *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*. Canberra: National Archives of Australia, 2004.

base de resultados de proyectos como los citados Pittsburgh e InterPARES, si bien Pittsburgh sí definió, en su momento, tanto los requisitos funcionales para la conservación de la evidencia como los metadatos derivados de tales requisitos[40]; mientras que InterPAREs discriminó, como medios de provisión de evidencia, requisitos de cota que incluían metadatos para garantizar la identidad del documento, y requisitos de base *post hoc* entre los que se incluía la descripción archivística[41]. De hecho, los procesos de asignación de metadatos, con o sin este nombre, han sido el medio por el que se ha garantizado durante siglos la autenticidad de los documentos analógicos[42]. En lo que concierne a las firmas digitales, ya se han examinado en secciones anteriores algunas propuestas que sugieren que, siendo imposible conservar éstas con significado, debieran al menos conservarse los metadatos que indiquen, en las debidas condiciones de confiabilidad, que la firma alguna vez estuvo allí. De este modo, la responsabilidad de la autenticación e integridad de datos asignada a la firma digital, y su certificado asociado, en el momento de la transmisión, se trasladaría, en términos de largo plazo, al proceso de asignación de metadatos. Esto, por supuesto, plantea un cierto número de problemas, algunos de los cuales se corresponden exactamente con los que hemos venido criticando de otras soluciones. En primer lugar, los metadatos no garantizan la tercera función que por convención se asigna a la firma digital, y que es la de hacer imposible la repudiación del documento[43]. Sin embargo, como se ha sugerido anteriormente, una firma digital no evita la repudiación, como no la evitaba una firma analógica. Siempre han existido afirmaciones de que una cierta persona no firmó algo y afirmaciones de que sí lo hizo. La firma digital garantiza simplemente que alguien que estaba en posesión de la clave, quizá porque la robó –lo cual derivaría en el grave problema de conservar las identidades digitales- realizó una transmisión de datos. Con la información disponible, la repudiación de la firma, analógica o digital, tiene que someterse a escrutinio humano externo, probable, aunque no necesariamente, ante un tribunal[44]. Es decir, tanto en el entorno analógico como en el digital, y tanto para los procesos de asignación de

[40] Confróntese *Functional Requirements for Evidence in Recordkeeping*, cit.

[41] Confróntese "Apéndice 2: Requisitos para ponderar y mantener la autenticidad de los documentos electrónicos". En: Duranti, Luciana, (ed.): *La conservación a largo plazo de documentos electrónicos auténticos*, cit. P. 259-276.

[42] Boudrez, cit. P. 5.

[43] Boudrez, cit. P. 3; Currall, cit. P. 499.

[44] McCullagh, Adrian, Caelli, William, cit.

metadatos como para cualquier otra técnica, los mecanismos sociales de asignación de confianza siguen jugando un papel crucial.

En segundo lugar, una actividad continuada de asignación de metadatos, a efectos de garantizar la autenticidad del documento, caería él mismo, por una parte, en el proceso *ad infinitum* que se ha criticado de otras propuestas; y, por otra, en la inadmisibilidad jurídica que también se ha criticado. En cuanto al primer problema, y dado el actual estado de las tecnologías, tales procesos *ad infinitum* parecen inevitables, y el problema no reside en su carácter infinito, sino en la clara delineación de aquello que se debe conservar y aquello que puede desecharse formalmente, por costoso, ineficaz, complejo, o cualquier otro motivo. Por ejemplo, emular el software o el sistema operativo, teniendo en cuenta que el sistema que los emula caducará a su vez y tendrá que ser emulado, junto con el software y el sistema operativo originales emulados, una y otra vez, parece una medida costosa e innecesaria; sin embargo, conservar el contenido del documento, junto con su contexto de creación, gestión y uso, puede que resulte pertinente. En cuanto al segundo, la admisibilidad jurídica es, una vez más, indecidible sin escrutinio humano externo, y el problema no reside tanto en el hecho de que un tribunal acepte como prueba los metadatos asociados a una firma, cuanto en la escasa atención que en nuestra tradición se está prestando a la opinión del archivero a la hora de legislar. En otros términos, que un tribunal acepte un documento refirmado o un documento encapsulado junto con sus metadatos es indiferente en términos objetivos, puesto que la confiabilidad que se asignará al mismo, como hemos adelantado, depende, no sólo de las técnicas utilizadas, sino también de los mecanismos sociales de confianza que una comunidad dada esté dispuesta a aplicar a tal documento. Por ejemplo, en la tradición escandinava es viable desprenderse de la firma puesto que su sólido sistema de registro recoge metadatos que pueden admitirse en corte. Nuestra tradición, con un sistema de registro mucho más débil, debiera plantearse la posibilidad de conservar, no sólo los metadatos, sino también la firma, con independencia de que ésta devenga ilegible en un plazo no determinado.

En tercer lugar, y como problema mucho más preocupante, aunque en los últimos años se han dictado normas y buenas prácticas relativas a los metadatos de gestión de documentos, y éstos incluirían aquellos necesarios para asignar significado a una

firma digital, las organizaciones siguen utilizando aplicaciones y generando documentos al margen de esas normas y buenas prácticas[45]. Básicamente, si los metadatos de origen no son reutilizables a efectos archivísticos, y si, específicamente dentro de nuestra tradición, los archiveros no reciben la consideración de tercera parte fiable capaz de indicar qué metadatos deben crearse y en qué momento de la vida del documento y de su firma asociada, entonces toda la propuesta de utilización de metadatos como medio para garantizar a largo plazo la autenticidad de documentos firmados digitalmente deviene inviable. Alternativamente, series de metadatos creadas en malas condiciones debieran ser consideradas por los archiveros a efectos de reutilización, encontrando mecanismos de interoperabilidad que satisficieran los requisitos sociales, jurídicos, o de cualquier otro tipo, de confiabilidad, de una comunidad dada[46].

Supuesto que estos problemas sean salvables, no obstante, el modelo que, a nuestro juicio, sigue aportando la mejor solución, a efectos de conservación del significado de las firmas digitales, es el de objeto de metadatos encapsulado, teorizado, como se indicaba, por David Bearman y el equipo de Pittsburgh, y llevado, en cierta medida, a la práctica por el mencionado proyecto VERS, cuya segunda versión de la norma fue publicada en 2003, y que no conserva todos los componentes del objeto (es decir, podría conservarse o no la firma), sino aquellos relevantes, como objetos de metadatos encapsulados (objetos VEO), a los que aplica firmas digitales, y a los que en la primera versión se hacía mención como siendo similares a las capas de una cebolla. A este fin hace uso de técnicas de canonicalización y de XML[47]. No obstante, si bien se diría que la "filosofía" es

[45] Confróntense, por ejemplo, Hurley, Chris: "What, If Anything, Is Records Management?". En: *RMAA Conference, Canberra, September 2004*. URL: http://www.sims.monash.edu.au/research/rcrg/publications/ch-what.pdf (Consulta: 27-10-2007); Nesmith, Tom: "Seeing Archives: Postmodernism and the Changing Intellectual Place of Archives". En: *The American Archivist*. N. 1, Vol. 65 (Spring/Summer 2002). P. 24-41.

[46] A este respecto resultaría interesante revisar los resultados del recientemente finalizado proyecto del Records Continuum Research Group *Clever Recordkeeping Metadata*. URL: http://www.infotech.monash.edu.au/research/groups/rcrg/crkm/ (Consulta: 8-11-2007).

[47] *Specification 3: VERS Standard Electronic Record Format*, cit. Para una definición de canonicalización confróntese Lynch, Clifford: "Canonicalization", cit. De acuerdo con el autor: "Asumamos que podemos definir una forma canónica para una clase de objetos digitales que, en alguna medida, captura las características esenciales de ese tipo de objeto de manera altamente determinada. Esta forma puede ser bastante voluminosa y no necesariamente razonable para almacenar, transmitir o manipular objetos. Es

correcta, la solución VERS sigue siendo fuertemente dependiente de la tecnología y resultado de una implantación específica. Un procedimiento similar que "describiera" el objeto y conservara inextricablemente vinculado este objeto y su "descripción" parecería igualmente viable a efectos archivísticos. Por supuesto, estos objetos encapsulados estarían ellos mismos sometidos a procesos de migración, de "redescripción" y de nueva encapsulación, siendo por lo demás tan multidimensionales como Chris Hurley ha teorizado recientemente al exponer irónicamente su concepto de HERO (Hurley's Enduring Recordkeeping Object) en el texto más arriba citado[48].

Conclusiones

En la presente exposición se han explorado las diferentes definiciones asociadas al uso de la firma digital a efectos de garantía de autenticidad a largo plazo de los documentos a los que está asociada, así como la funcionalidad de la firma digital en cuanto garante de la autenticidad sólo a corto plazo. A partir de la asunción, creemos que fundada, de que las firmas digitales no han sido concebidas para garantizar la autenticidad de los documentos a largo plazo, se ha examinado literatura que propone diversas soluciones. De este examen debiera poder derivarse, en primer lugar, que la respuesta al problema de la conservación a largo plazo del significado de las firmas digitales no es sólo dependiente de la tecnología, sino que descansa también en mecanismos de confianza socialmente asignados, reflejados frecuente, pero no necesariamente, en el comportamiento del legislador.

---

una forma idealizada del objeto, con independencia de su eficacia. Además, las representaciones específicas del objeto pueden ser más ricas que la forma canónica. Puede haber una jerarquía de formas canónicas, algunas de las cuales son capaces de representar muchos más detalles o una semántica más rica que otras... Todos los formatos reales utilizados para almacenar un objeto de un tipo dado deben ser traducibles a la forma canónica. También resulta crítico que, aunque puede haber múltiples modos de representar un objeto específico de un tipo dado en un formato de almacenamiento para trabajo, todos debieran traducirse a una cadena de bits idéntica en la forma canónica. Los formatos de almacenamiento populares pueden incluir listas de parámetros que no son dependientes del orden (por ejemplo, pares clave-valor). Una forma canónica debe forzar una ordenación específica de estos parámetros. De manera similar, un formato de almacenamiento dado puede incorporar valores por defecto para parámetros no especificados. El formato canónico debiera ser idéntico si estos valores por defecto se obtienen omitiendo parámetros o especificando explícitamente los parámetros en cuestión y sus valores por defecto." Acerca del trabajo del W3C e IETF para el desarrollo de firmas XML, confróntese: *XML Signature WG*. URL: http://www.w3.org/Signature/ (Consulta: 8-11-2007).

[48] Hurley, Chris: *Relationships in Records*, cit.

En segundo lugar, debiera poder derivarse que la solución al problema no pasa por la relación tecnología/legislación, sino que requiere la intervención de una tercera parte, el archivo, hasta el momento ausente, en la práctica, de las medidas emprendidas, si es que se han emprendido, para resolver el problema. Además, debiera poder derivarse que es preciso un mayor grado de investigación, tanto en lo que se refiere a los mecanismos para el diseño y uso de firmas digitales, como en lo que se refiere al potencial de reutilización de metadatos procedentes de aplicaciones de negocio. Por último, debiera poder derivarse que, a efectos archivísticos, la mera garantía de que los datos se han conservado no es suficiente, si la conservación de estos datos no viene acompañada por la de su contexto de creación, gestión y uso, la de su o sus estructura(s) cambiante(s), su(s) forma(s) y su comportamiento.