ECIJA

INFORME JURÍDICO

VALORACIÓN JURÍDICA DEL SISTEMA DE FIRMA BIOMÉTRICA DIGITALIZADA DENOMINADO 3G MOBILE SIGN

TIPO DE DOCUMENTO			Ámbito general
		X	Confidencial
TÍTULO	Informe Jurídico – Firma Biométrica Digitalizada – 3G Mobile Sign		
TITULAR	Écija Legal & Compliance S.L		
FORMATO	Electrónico – PDF		
PÁGINAS	27		
DENOMINACIÓN PLATAFORMA	3G MOBILE SIGN		
VERSIÓN DEL SOFTWARE	1.0		
VERSIÓN	**FECHA**	**AUTOR - DEPARTAMENTO**	**CARGO**
1	05/11/2014	Alonso Hurtado Bueno María González	Socio – Information Technology Asociado - Information Technology

Fdo. Alonso Hurtado
Socio IT & Compliance
ECIJA Abogados

Fdo. María González
Socia IT
ECIJA Abogados

ÍNDICE

1 INTRODUCCIÓN

En solo unos pocos años el interés por los rasgos biométricos para la verificación o autenticación de personas ha crecido notablemente. En la sociedad actual y hacia donde se está evolucionando es de vital importancia conocer la identidad del usuario y la biometría lo permite a través de características intrínsecas del sujeto.

La permanente evolución de los servicios de la Sociedad de la Información ha dado lugar a la aparición de una nueva rama de la Tecnología denominada Autenticación biométrica, encontrándose dentro de este tipo de tecnología aquellos sistemas automatizados que permiten el reconocimiento de personas a través de sus rasgos inherentes.

Dependiendo de las características estudiadas existen dos grandes grupos de sistemas biométricos: los que se fijan en aspectos físicos y los que se fijan en aspectos vinculados a la conducta. Se conoce como biometría estática a la primera y como biometría dinámica a la segunda. Dentro de estas dos categorías existen distintas características de estudio como puede ser la huella dactilar, el iris, la firma manuscrita, la voz, entre otras.

De entre los múltiples rasgos que pueden ser empleados para realizar la autenticación biométrica de usuarios, 3G Mobile Sign ha optado por los rasgos inherentes que toda persona plasma a la hora de llevar a cabo su firma manuscrita u ológrafa.

La firma manuscrita es una herramienta que el ser humano utiliza y ha utilizado desde la antigüedad para dejar constancia de que algo es suyo. Se trata de un signo de identidad y por ello es tan importante. Además, es usada ampliamente en multitud de escenarios como puede ser en un pago con tarjeta, en un contrato laboral, en un consentimiento médico, entre otros.

La firma manuscrita es uno de los medios de verificación de identidad por excelencia. La seguridad, aceptación y arraigo de la firma como medio de autentificación personal, social y legal, confieren enormes posibilidades de futuro a este trabajo especialmente en ámbitos donde la seguridad sea parte fundamental de su actividad.

Además, la firma tiene grandes implicaciones legales puesto que es considerada un signo propio y singular de cada individuo y por tanto goza de total validez legal.

De este modo, el creciente desarrollo y utilización de potentes terminales como Tablet PC, Smartphone o tabletas fijas, así como la proliferación de redes de comunicaciones de banda ancha, especialmente móviles, permiten la implantación y uso de sistemas automáticos para el reconocimiento y verificación de usuarios mediante rasgos biométricos, como son la velocidad, la presión y la inclinación de la firma, que se encuentran incluidos en todo proceso de firmado ológrafo.

2 OBJETO Y ALCANCE

La compañía 3G Mobile Sign SL ha desarrollado una plataforma online denominada "3G Mobile Sign", que permite obtener, de forma remota, el consentimiento de los usuarios en procesos de contratación cotidianos, tales como hojas de pedido, contratos o albaranes de entrega. Para ello, el sistema emplea el uso de la firma biométrica digitalizada, que los usuarios realizan desde sus dispositivos móviles (Smartphone y tabletas electrónicas).

El objeto del presente informe se centra en la evaluación desde el punto de vista jurídico, y especialmente en relación al valor probatorio de los documentos resultantes, de todos y cada uno de los elementos que componen el sistema de firma biométrica digitalizada.

Concretamente el informe de auditoría comprende la evaluación y verificación del cumplimiento por parte del sistema de firma biométrica digitalizada, de todos los requisitos normativos aplicables al sistema que garantizan que los consentimientos obtenidos mediante el mismo, son plenamente validos desde el punto de vista jurídico y probatorio, causando los efectos jurídicos que en Derecho corresponden.

Queda comprendido en el alcance del presente informe las siguientes acciones:

1) Servicios de auditoría independiente para evaluar el nivel de cumplimiento del sistema de firma biométrica digitalizada diseñado y explotado por parte de 3G Mobile Sign con la normativa indicada en el presente documento.
2) Determinar si el documento electrónico resultante cuenta con valor judicial probatorio, y en su caso, determinar el grado de validez del mismo atendiendo a los requisitos dispuestos por la Ley de Enjuiciamiento Civil y demás normativa de aplicación.
3) Evaluación desde el punto de vista pericial caligráfico del tipo de pruebas generadas por parte del sistema de firma biométrica planteado por parte de 3G Mobile Sign.

En este sentido, el presente informe no tiene como objetivo determinar la valoración que posteriormente pudiera llevar a cabo un tribunal competente o cualquier autoridad con capacidad para ello o en su caso asegurar la validez "plena" de la prueba electrónica derivada de la plataforma propiedad de 3G Mobile Sign en sede judicial o ante autoridad administrativa, sino que su objetivo no es otro que determinar, a juicio del equipo auditor y teniendo en cuenta la normativa y el estado de la técnica existe en el momento de la firma del presente informe, cuál es el grado de eficacia probatoria que presentan las pruebas electrónicas derivadas de la plataforma propiedad de 3G Mobile Sign.

3 LEGISLACIÓN APLICABLE

A los efectos de la realización del presente análisis, se tendrán presentes las obligaciones expresamente recogidas en la siguiente normativa:

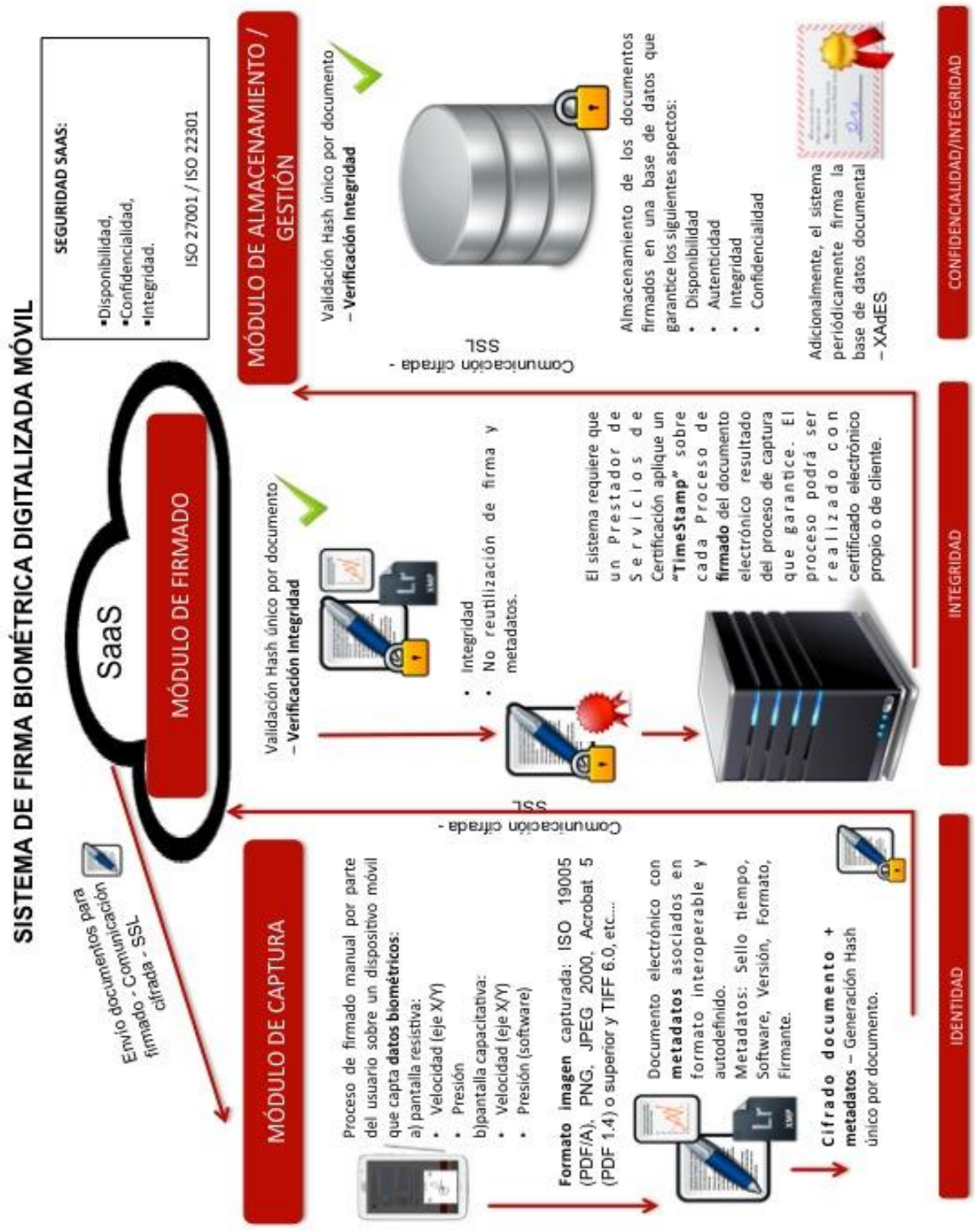
1) Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante LFE)
2) Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
3) Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante, LECi)
4) Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).
5) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante RLOPD).
6) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante LSSI)
7) ISO/IEC 19.795 Information Technology - Biometric performance testing and reporting

4 METODOLOGÍA EMPLEADA

Para la realización del proceso de auditoría, el equipo auditor ha empleado en todo momento una metodología sistemática, basada en una lista de control previamente diseñada, en la que se plantea el análisis de todas y cada una de las cuestiones expresamente referenciadas en la normativa de referencia.

La auditoría del sistema de digitalización ha sido realizada directamente por parte del equipo auditor, llevando a cabo las pruebas correspondientes del sistema y la evaluación de los documentos generados por el mismo, con el fin de garantizar la independencia plena a la hora de evaluar el grado de cumplimiento de la solución objeto de la auditoría.

5 ELEMENTOS DEL SISTEMA DE FIRMA BIOMÉTRICA OBJETO DE ANÁLISIS Y EVALUACIÓN



Evidencia 1. Esquema de Proceso de Captura, Firmado y Almacenamiento de Firmas

6 ANÁLISIS JURÍDICO DE LOS ELEMENTOS DEL SISTEMA

A continuación se lleva a cabo el análisis de cada uno de los tres módulos anteriormente identificados en el esquema del sistema de firma biométrica digitalizada de 3G Mobile Sign, centrándose el análisis en la evaluación del cumplimiento de los requisitos mínimos y en su caso, recomendables, para dotar al sistema y las evidencias electrónicas derivadas del mismo de las máximas garantías legales.

Todo sistema de firma biométrica digitalizada debe lograr garantizar los siguientes tres aspectos:

1) Que el sistema permite obtener durante el proceso de firma los datos y parámetros biométricos necesarios para poder identificar a la persona que efectivamente realizó la firma del documento concreto.
2) Que el sistema cuenta con las medidas tecnológicas y criptográficas necesarias para garantiza la integridad e inalterabilidad de los datos captados, así como la imposibilidad de reutilización de los mismos.
3) Que el sistema cuenta con elementos de almacenamiento de los documentos firmados que garanticen la integridad de la base de datos y el contenido de la misma.

En los apartados a continuación expuestos se lleva a cabo el análisis completo de cada uno de estos elementos, tomando como referencia para cada uno de ellos la normativa anteriormente referenciada.

6.1 MÓDULO DE CAPTURA DE FIRMA (IDENTIDAD)

El primero de los aspectos que será objeto de análisis en el presente informe es el módulo de captura de la firma y los datos biométricos asociados a ésta, siendo precisamente los datos biométricos los que, como si se tratara de una firma ológrafa tradicional que posteriormente puede ser sometida a peritaje en sede judicial, serán empleados para probar la identidad y autoría de la firma efectivamente realizada a través de la plataforma 3G Mobile Sign.

6.1.1 CAPTURA DE DATOS BIOMÉTRICOS

Como regla general, cualquier característica, física o de conducta, puede usarse como elemento biométrico para determinar la identidad de una persona. No obstante, para que ello sea posible contando con las máximas garantías, es necesario que cuenten con las siguientes propiedades:

1) Universalidad: todo el mundo debe poseer esa característica.
2) Unicidad: dos personas cualesquiera deben ser suficientemente diferentes en términos de ese rasgo, es decir, un mismo rasgo para dos personas diferentes nunca puede ser idéntico.
3) Permanencia: el rasgo debe permanecer suficientemente invariable en el tiempo durante un periodo de tiempo aceptable.
4) Evaluabilidad: el rasgo debe poder ser medido cuantitativamente.

Aparte de estas propiedades, desde el punto de vista práctico de un sistema de reconocimiento, hay otro conjunto de propiedades que deben satisfacerse:

1) Rendimiento: hace referencia al error cometido en el reconocimiento de individuos, a la velocidad y recursos necesarios para llevarlo a cabo, así como a los factores externos que afecten a las capacidades de reconocimiento del sistema.
2) Aceptabilidad: los usuarios deben estar dispuestos a emplear ese rasgo en las actividades de su vida cotidiana.
3) Fraude: los sistemas que usen ese rasgo deben ser suficientemente seguros de forma que resulte difícil atacarlos.

Por ello, cualquier sistema que utilice el reconocimiento biométrico debe cumplir con los requisitos de precisión, velocidad y utilización de recursos, debe ser aceptado por la población a la que se dirige y debe ser lo suficientemente robusto a los intentos de fraude y ataques a los que pueda ser sometido.

Antes de entrar a analizar cada uno de los elementos que deben ser tenidos en consideración en un sistema de firma biométrica digitalizada, debe tenerse en cuenta que la finalidad última de un sistema como el analizado, es **la identificación del firmante mediante la relación de un firma ológrafa, realizada de un momento concreto, con una persona concreta.**

La verificación de firma es el proceso mediante el cual, dada una firma que pertenece a un usuario, una decisión se toma sobre si dicha firma ha sido hecha por ese usuario, una firma genuina, o ha sido realizada por otro usuario, una firma falsificada.

Habitualmente, las firmas falsificadas se clasifican en tres grupos:

1) Aleatoria: se realizan sin ningún conocimiento sobre las firma del usuario o de su nombre.
2) Simple: se realizan sabiendo el nombre del usuario pero sin ningún conocimiento sobre su firma.
3) Experta: se realizan con un conocimiento completo sobre el nombre y la firma del usuario.

Del mismo modo, existen diferentes métodos para la verificación de la autenticidad de las firmas, pudiendo diferenciarse entres dos grupos principales:

1) Off-line (estáticos): se basan en procesar una imagen digitalizada en escala de grises de la firma manuscrita en un papel.
2) On-line (dinámicos): tienen en cuenta las características dinámicas de la firma, tales como la presión ejercida, las inclinaciones, posiciones o la velocidad del stylus. Todas las señales proveen, no sólo de información de la firma, sino también información sobre el acto propio de firmar, que se considera relacionado con el usuario específico (una característica de comportamiento).

El sistema planteado por parte de 3G Mobile Sign es un sistema categorizado como On-line o dinámico, en tanto se trata de un sistema que permite la captura, tanto del gráfico de la firma, como de las características biométricas derivadas del propio acto de la firma y emanadas directamente del comportamiento de cada uno de los individuos. Debido a esto, y a la mayor cantidad de información recogida en comparación con los sistemas estáticos, los sistemas de verificación automáticos on-line (dinámicos) obtienen una mayor fiabilidad que los sistemas off-line y en definitiva que los sistemas de cotejo de firmas realizado de forma habitual por los peritos calígrafos en sede judicial.

6.1.1.1 DATOS BIOMÉTRICOS QUE SON CAPTURADOS Y PROCESADOS POR EL SISTEMA

Los datos biométricos que pueden ser capturados por parte del sistema de firma analizado son los indicados a continuación, sin perjuicio de que algunos de ellos no dependen única y exclusivamente del software objeto de este análisis, sino que el dispositivo de captura (Tabletas o Smartphones) empleado para la obtención de las firmas y las características del mismo, son determinantes para poder obtener algunos de los datos indicados a continuación.

No obstante, sin perjuicio de los factores incluidos a continuación, debe tenerse en consideración que los peritos calígrafos, además de los factores comentados a continuación, en función del tipo de firma, tienen en cuenta un gran número de factores adicionales, propios de cada tipo de firma y que la mayoría de sistemas de software existente en el mercado permiten capturar, incluido el software empleado por parte de 3G Mobile Sign.

1) Presión

La presión se puede definir como la fuerza o energía con la que se asienta sobre el receptor, en nuestro caso la tableta gráfica, para producir o ejecutarla escritura y/o firma manuscrita. Esta, no es constante en una escritura y/o firma manuscrita, está íntimamente ligada a los movimientos de extensión, rotación y flexión de la parte del órgano humano utilizado para escribir.

En la identificación de una persona, a través de su escritura / firma manuscrita, la presión es uno de los elementos estructurales de grafismo que siempre está presente, y que resulta esencial para lograr determinar la autoría de una firma. Conforme a la doctrina, para unos, la presión es de fácil observación, para otros, no lo es tanto, y demanda mucha observación y ponderación en su estudio y análisis.

2) Velocidad y Frecuencia de Muestreo

Otro de los factores principales que debe ser captado por parte del sistema de firma biométrica digitalizada es la velocidad con la que el autor de la firma lleva a cabo cada una de las partes de la firma, siendo ésta característica otro elemento esencial para lograr la identificación del firmante.

Para determina la velocidad el sistema debe registrar el plazo de tiempo que se tarda en recorrer la distancia entre dos puntos, tanto en el eje de coordenadas X, como en el eje de coordenadas Y.

$$\textbf{Velocidad eje X} = \frac{\text{Distancia entre el punto 1 y 2}}{\text{Tiempo de recorrido}}$$

$$\textbf{Velocidad eje Y} = \frac{\text{Distancia entre el punto 1 y 2}}{\text{Tiempo de recorrido}}$$

Del mismo modo, a efectos de determinar la velocidad, es necesario concretar cuál es la velocidad de muestreo del dispositivo empleado para realizar la captura, dado que a menor velocidad de muestreo, menor será la exactitud con la que posteriormente podremos determinar la velocidad concreta con la que se realizó la firma.

La frecuencia de muestreo se puede definir como el número de muestras por unidad de tiempo que se toman de una señal continua para producir una señal discreta, durante el proceso necesario para convertirla de analógica en digital. Como todas las frecuencias, generalmente se expresa en hercios (Hz, ciclos por segundo) o múltiplos suyos, como el kilohercio (kHz), aunque pueden utilizarse otras magnitudes.

3) Inclinación

Por último, otro de los factores principales que deben ser tenidos en consideración para determinar la identidad de la autoría de una firma manuscrita, es la inclinación que el usuario emplea para realizar el proceso de escritura.

En este sentido, el software empleado por parte de 3G Mobile Sign permite la captura de la inclinación, sin perjuicio de que para que la captura de estos datos deba realizarse con un Stylus específico que cuente con un osciloscopio interno, que permita determinar el grado de inclinación que aplica el firmante en cada proceso de firma.

6.1.1.2 LA IMPORTANCIA DEL DISPOSITIVO DE CAPTURA

Como hemos indicado, el sistema planteado por 3G Mobile Sign es un sistema orientado principalmente a la movilidad, en la que es necesaria la utilización de dispositivos externos de captura de las firmas (Tabletas o Smartphones) y que son aportados por parte de los usuarios del sistema.

A pesar de que el análisis específico de estos dispositivos no están incluidos dentro del alcance del presente informe, se considera importante por parte del equipo auditor determinar cuáles son los aspectos y características propias de los dispositivos de captura que deben ser tenidos en consideración, dado que afectan de forma directa a la capacidad de captación y procesamiento de los datos biométricos anteriormente analizados y considerados esenciales para lograr un nivel de identificación entre la firma ológrafa y su autor.

El sistema planteado por parte de 3G Mobile Sign, tras las pruebas realizadas por parte del equipo auditor, permite la utilización de cualquier tipo de dispositivo móvil de captura (ya sea Smartphone, Tablet móvil o Tablet fija) siempre que el método de firmado, sea realizado mediante un lápiz o Stylus especifico para esta función.

Concretamente, pueden diferenciarse dos tipos de dispositivos / tabletas en función del tipo de pantalla:

1) **Tabletas con pantalla resistiva:** este tipo de pantallas está formada por varias capas, las más importantes son dos finas capas de material conductor entre las cuales hay una pequeña separación. Cuando algún objeto toca la superficie de la capa exterior, las dos capas conductoras entran en contacto en un punto concreto. De esta forma se produce un cambio en la corriente eléctrica que permite a un controlador calcular la posición del punto en el que se ha tocado la pantalla midiendo la resistencia, lo que permite capturar la presión y la velocidad en los ejes X e Y. (Ej.: BQ Verne, BQ Darwin, Epad ZT-180).

2) **Tabletas con pantalla capacitiva:** este tipo de pantallas necesitan ser manejadas mediante el dedo o un objeto que disponga de capacitancia. Pueden detectar varias pulsaciones simultáneas o gestos. Las pulsaciones o gestos no requieren presión, basta con deslizar el dedo para controlar la pantalla del dispositivo. No permiten medir la presión, pero sí el grosor, a partir del cual es posible obtener información relativa a la presión.

Es importante tener en cuenta que en el mercado de dispositivos existente en el momento de la realización del presente informe, la mayoría de dispositivos existentes cuentan con pantallas que son resistivas y capacitativas, aunando en un mismo dispositivo las características propias de cada tipo de pantalla. Como ejemplo de las pantallas de este tipo, cabe destacar los dispositivos de la gama de Samsung Galaxy Note en sus diferentes versiones o la mayoría de pantallas del fabricante Wacom.

Como se ha indicado en el apartado anterior, para lograr un nivel de identificación del autor de la firma adecuado y por tanto un nivel de eficacia probatoria de la prueba electrónica derivada del sistema objeto de auditoría, es necesario que el dispositivo de captura y posteriormente el software y algoritmos empleados por el mismo, permitan obtener y procesar la evolución temporal durante el proceso de firma de al menos las siguientes funciones:

1) **Velocidad:** la coordenada X y la coordenada Y. La velocidad se calcula como la distancia recorrida entre 2 puntos determinados dividido por el tiempo transcurrido y.
2) **Presión:** ejercida por el usuario sobre la pantalla.

En relación a la orientación del Stylus o lo que es lo mismo, los factores de inclinación y azimut[1] son factores que aportan un valor identificativo adicional y que permitirían aumentar, aún más, el nivel de identificación de los usuarios firmantes. Ahora bien, en el momento actual no existe ningún tipo de dispositivo móvil que permita la captación de este tipo de factor, sin contar para ello con dispositivos Stylus o lápices específicos que cuenten con el correspondiente osciloscopio capaz de capturar ese dato adicional.

[1] Ángulo medido en el sentido de las agujas del reloj desde el eje "y", respecto a la proyección perpendicular de la pluma sobre el plano de escritura.

A pesar de ello, los factores anteriormente identificados, son los factores considerados como principales para lograr un nivel de identificación adecuado y válido en un procedimiento judicial para que un perito calígrafo pueda determinar con un alto grado de exactitud la identidad del firmante y por tanto lograr que la prueba electrónica cuente con eficacia suficiente, sin perjuicio de que los peritos calígrafos tienen en cuenta en sus análisis un conjunto adicional de factores, tales como la forma y configuración de los puntos de ataque, inicios y finales de los impulsos gráficos, configuraciones espaciales de determinados sectores de la firma, calidad de los desenlaces, características de los signos accesorios de puntuación, tensión o energía con que se improntan los movimientos en flexión y extensión, diseño de elipses y grado de rapidez de los cambios de dirección en curva o temblores o anomalías en sectores o trayectorias determinadas del trazado, en otros muchos factores adicionales.

Es por ello necesario destacar, que para que el sistema propuesto por parte de 3G Mobile Sign logre el grado de identificación adecuado, para que en sede judicial un perito calígrafo logre la asociación de una persona concreta con la firma realizada en la tableta con un nivel de garantía que sea equivalente o superior al empleado cuando se trata de firmas realizadas sobre papel y por tanto la prueba electrónica cuente con eficacia probatoria suficiente, es necesario que el cliente final emplee dispositivos de captura que cuenten con pantalla resistiva, en la medida en que permiten capturar la presión realizada sobre la pantalla.

En este sentido, y según ha podido comprobar el equipo auditor, 3G Mobile Sign ha procedido a incluir esta advertencia en las condiciones de uso de la plataforma, de tal forma que todos los clientes y usuarios que instalen e utilicen la plataforma conocerán que la validez y eficacia jurídica de los documentos electrónicos firmados a través de la plataforma, pueden verse afectada en función del tipo de dispositivo de captura empleado, siendo recomendable emplear dispositivos que como mínimo capturen la velocidad y la presión, así como la mayoría de factores indicados con anterioridad.

Con independencia del tipo de dispositivo, marca y modelo que se seleccione por el usuario final, debe tenerse en cuenta que, en la medida en que 3G Mobile Sign no puede controlar el tipo de dispositivo que va a ser empleado por el cliente final para introducir la firma, no puede determinarse de ante mano los datos biométricos concretos que pueden ser capturados por el sistema en cada caso. Sin perjuicio de ello, el presente análisis ha sido realizado empleado un dispositivo tableta móvil, con pantalla resistiva, y capaz de capturar la velocidad y la presión del proceso de firma.

6.1.1.3 INCLUSIÓN DE METADATOS EN EL DOCUMENTO GENERADO

El sistema de firma electrónica móvil empleado por 3G Mobile Sign se encuentra integrado, entre otros elementos, por un software especifico de captura de firma biométrica en dispositivos fijos y móviles provisto por la compañía Smartaccess S.L, fabricante de la tecnología de 3G Mobile Sign.

Es este software el encargado de incluir los metadatos requeridos, incluidos los datos biométricos, en el documento generado, inclusión que se hace de forma totalmente automatizada e instantánea en el documento, sin que exista ningún tipo de manipulación previa tal y como ha podido comprobar ECIJA y queda debidamente evidenciado en el presente informe.

Los metadatos incluidos en el documento generado, son incluidos en un formato interoperable y autodocumentado, de forma que se permita el acceso a los mismos desde cualquier sistema.

Todos estos datos quedan vinculados de forma única a la firma y al documento firmado por el usuario, de forma que no es posible la reutilización de la firma obtenida en otro documento diferente al contrato asociado al proceso de contratación efectuado por el usuario final.

Estos aspectos quedan acreditados y certificados por el titular del software empleado, Smartaccess, que se incorpora al presente Informe como Anexo I.

6.1.1.4 NEUTRALIDAD TECNOLÓGICA - LA IMPORTANCIA DE LA ESTANDARIZACIÓN

La solución de firma biométrica móvil 3G Mobile Sign, tal y como ha podido comprobar el equipo auditor, se basa en tecnología estándar, que emplea algoritmos matemáticos para el cálculo y captura de los datos biométricos que permiten, de forma completamente independiente del dispositivo de captura capturar y reproducir los datos biométricos con independencia del tipo de dispositivo empleado.

Todo ello es posible, gracias a que los algoritmos matemáticos empleados por el sistema han sido desarrollados tomando como referencia el estándar internacional ISO/IEC 19.795 "Information Technology - Biometric performance testing and reporting".

En este sentido, los datos biométricos, incorporados a los documentos generados y tratados por el sistema de firma biométrica móvil, tienen un formato autodocumentado e interoperable, quedando acreditado y garantizada la neutralidad tecnológica y la estandarización de la solución a través del certificado emitido por Smartaccess e incorporado la presente informe como Anexo I.

Del mismo modo, es importante tener en consideración que los ficheros generados a través del sistema se encuentran en formatos autodocumentados, autosuficientes e interoperables, lo que garantiza que el cliente final y en su caso, los juzgados y tribunales, en caso de ser necesario reproducir dichos ficheros no dependerán de ninguna tecnología de software concreta o específica, sino que por sí mismo podrán ser ejecutados. Concretamente los formatos empleados por el sistema son PDF, PDF/A, XPS y XML.

6.1.2 GARANTÍAS DE SEGURIDAD DURANTE EL PROCESO DE CAPTURA

En la medida en que los datos biométricos capturados durante cada proceso de firma son datos esenciales para determinar la autoría y la identidad del firmante, es esencial que los datos biométricos capturados durante el proceso de firma sean plenamente íntegros.

En este sentido y tal y como se explica ampliamente en el próximo apartado del presente informe, es necesario plantearse en el análisis de los elementos que componen el módulo de captura, cómo garantiza al sistema la integridad de los datos, en caso de que no sea posible conectarse con el sistema de sellado de tiempo o Time Stamp externo (por ejemplo por falta de conectividad de la red móvil).

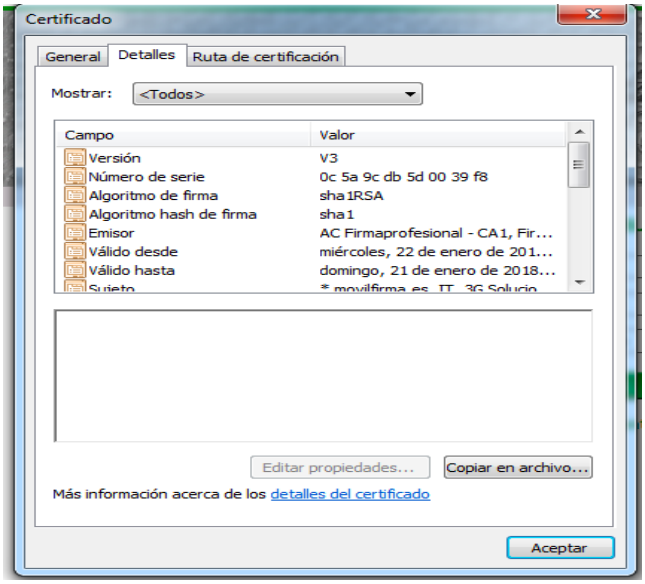
Tal y como ha podido comprobar el equipo auditor, el software de captura de firma integrado en el sistema de firma biométrica digitalizada objeto de, garantiza la integridad de los datos capturados a pesar de que pueda haber problemas de conectividad, de este modo, y tal como se acredita y certifica en el documento emitido por el proveedor y adjunto al presente Informe como Anexo I, el software permite la inserción automática e inmediata en el documento, sin que pueda existir una manipulación previa o posterior como metadatos del propio documento.

Del mismo modo, el equipo auditor se ha centrado en comprobar si el sistema, una vez se captura la firma y los datos biométricos asociados al proceso, dichos datos son automáticamente introducidos como metadatos en el documento electrónico correspondiente, realizándose dicho proceso de forma completamente automática, sin intervención humana alguna y de tal forma que en ningún momento el documento y/o los metadatos asociados al mismos sean almacenados en memoria del dispositivo, sin que previamente hayan sido sometidos a la aplicación del correspondiente algoritmo matemático para calcular el Hash correspondiente.

Concretamente, el sistema objeto de análisis una vez finalizado el proceso de captura aplica sobre el documento un algoritmo matemático SHA-1 para obtener el Hash del documento, tal y como se evidencia a continuación.

```
String shash = String.Empty;

try{
    shash = Utils.getHash(document);
}catch(Exception ex){
    Utils.logInfo("changeDocumentState error obteniendo hash " + ex.Message);
}


string query = "UPDATE ssdocumentos SET fidestado = {0}, sruta = '{1}', ifirmaactual = ifirmaactual+1, dfechamodificacion = getdate(), shash = '{4}'"
    + " WHERE iiddocumento = {2} AND fidusuarioasignado = {3}";

string HistoryQuery = "INSERT INTO ssfirmas (fiddocumento, fidusuario, fidempresa, dfechafirma, fidorden, sruta, fidestado, fidtipofirmafacturacion)"
    + " VALUES ({0}, {1}, {2}, getdate(), {3}, '{4}', {5}, {6})";

string EmpresaQuery = "UPDATE ssempresas SET {0} WHERE iidempresa = {1}";

if (sd.IsTheLast)
{
    //Es la ultima
    query = string.Format(query, Utils.ESTADO_FIRMADO, fullFilePath, idDoc, uData.UserId.ToString(), shash);
    Utils.logInfo("changeDocumentState query:" + query);
    HistoryQuery = string.Format(HistoryQuery, idDoc, uData.UserId.ToString(), uData.EmpId.ToString()
        , sd.CurrentSignature.ToString(), fullFilePath, Utils.ESTADO FIRMADO, fidtipofirmafacturacion);
```

Evidencia 2. Código fuente - Cálculo del hash sobre el documento y los metadatos asociados



Evidencia 3. Propiedades certificado electrónico – Algoritmo de cifrado SHA1

Por último, el equipo auditor ha revisado el procedimiento de captura para determinar si el proceso es completamente automático y sin intervención humana de ningún tipo (más allá de la propia para realizar el acto de firma), comprobándose que en efecto, el proceso es completamente automático, no existiendo manipulación por parte del operador y/o usuario, llevándose a cabo el proceso lógico incluido como Evidencia 1 del presente informe de forma plenamente automatizada.

6.2 MÓDULO DE FIRMADO ELECTRÓNICO (INTEGRIDAD)

Una vez obtenida la firma manuscrita, junto a todos los datos biométricos, el sistema objeto de análisis tal y como ha podido comprobar el equipo auditor, propone como medida de protección un doble sistema de seguridad encaminado a lograr garantizar la integridad de toda la información asociada a la firma en sí y a la propia firma.

Por un lado, tanto la imagen gráfica de la firma, como los datos biométricos asociados a ésta e incluidos como metadatos de la firma, son debidamente firmados electrónicamente mediante un certificado de firma electrónica reconocida, con la única finalidad de garantizar la plena integridad y no modificación de los datos.

Dicha firma mediante certificado electrónico reconocido es directamente aplicada, de forma completamente automática, en el mismo momento que el usuario finaliza la firma manuscrita, realizándose una petición al servidor donde se encuentra alojado el sistema, y respondiendo éste de forma completamente automática e inmediata, siendo aplicada la firma mediante certificado reconocido sobre el documento, la firma manuscrita y todo los metadatos.

En segundo lugar, el sistema objeto de análisis de forma completamente automática lleva a cabo una petición a un Prestador de Servicios de Certificación (PSC) para que aplique un sellado de tiempo electrónico o "Time Stamp" sobre los documentos firmados por los usuarios, lo que garantizará el momento exacto en el que se llevó a cabo la firma del documento en cuestión[2].

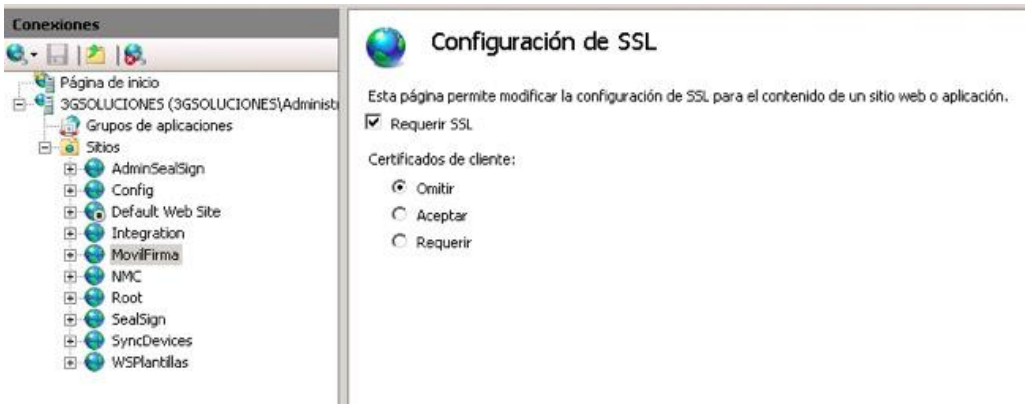
6.2.1 GARANTÍAS DE SEGURIDAD DE LAS COMUNICACIONES CON EL SERVIDOR CENTRAL

Un sistema como el planteado por parte de 3G Mobile Sign, en el que existe una comunicación a través de Internet entre el dispositivo desde el que se captura la firma y los datos biométricos y el servidor externo propiedad de 3G Mobile Sign, en el que se recibe el documento y éste es sometido al proceso de firmado mediante certificado de firma electrónica reconocido instalado en el servidor de 3G Mobile Sign.

En la medida en que existe comunicación a través de una red pública (Internet) entre el dispositivo de captura y el servidor donde se firma electrónicamente el documento, a juicio del equipo auditor es esencial determinar el grado de seguridad existente para garantizar, principalmente, la integridad del documento con la firma y los metadatos asociados antes de aplicarse sobre el mismo el certificado de firma electrónica reconocida.

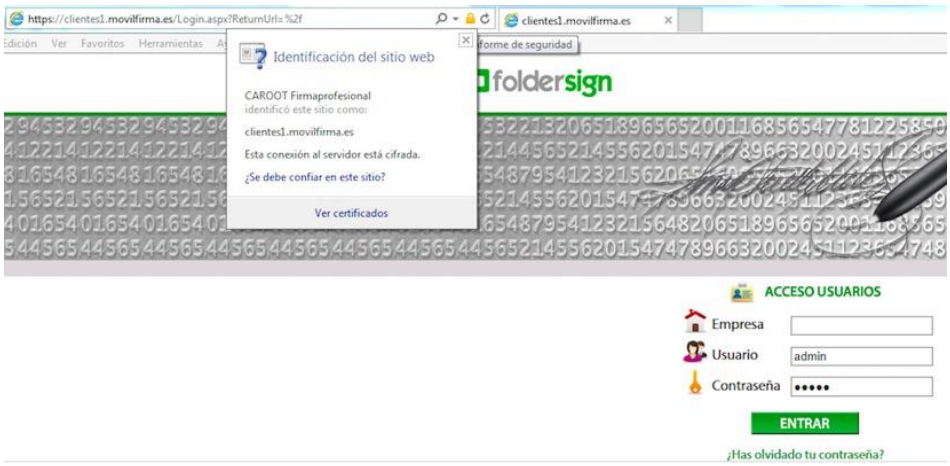
Para cumplir este objetivo es necesario que la plataforma cuente con un sistema que garantice la securización de las comunicaciones entre el dispositivo de captura y el servidor de 3G Mobile Sign, siendo estas comunicaciones ejecutadas a través de canales seguros y de forma cifrada, tal y como se analiza en el presente apartado.

Así, la configuración del sistema de firma biométrica móvil se encuentra establecida de forma que las comunicaciones se realicen a través del protocolo de comunicación SSL, de 2048 bits lo que garantiza que todas las comunicaciones entre los usuarios del sistema y las tabletas empleadas por los usuarios cumplen íntegramente con los requisitos de seguridad necesarios para garantizar la integridad de la información.

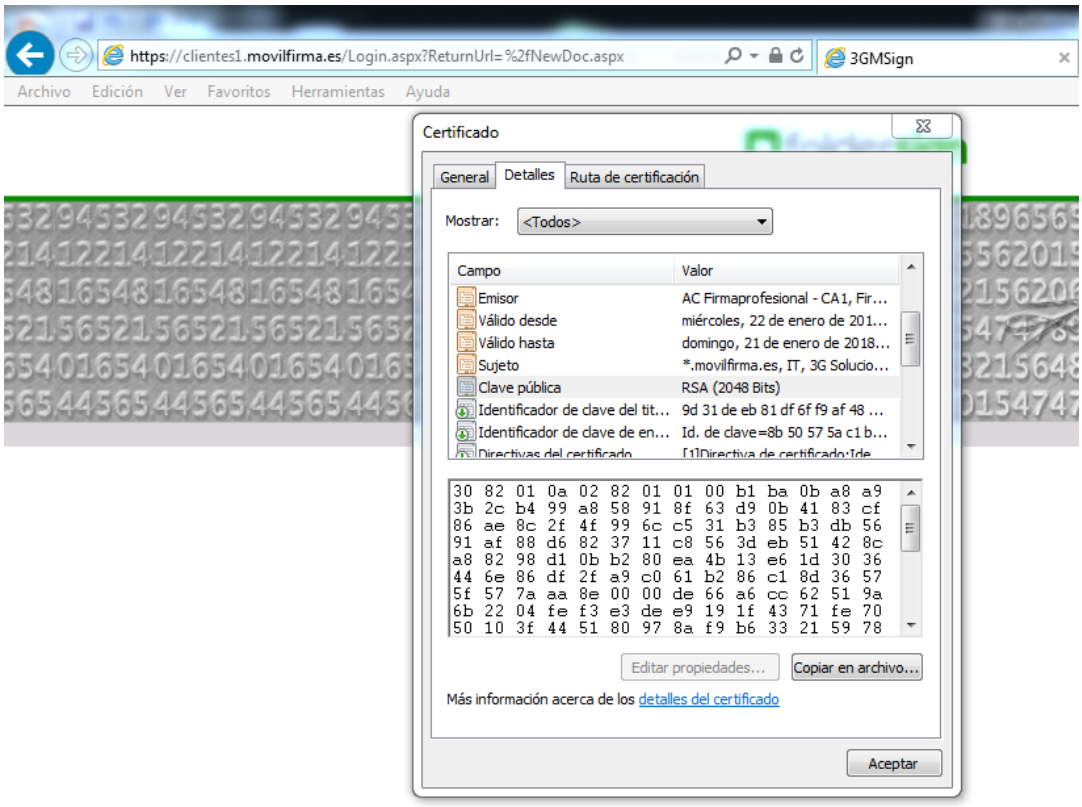


[2] El sellado de tiempo tomará en todo caso como referencia la hora oficial española establecida por el Real Instituto y Observatorio de la Armada Española (ROA) de conformidad con lo dispuesto en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada como laboratorio depositario del Patrón Nacional de Tiempo y laboratorio asociado al Centro Español de Metrología.

Evidencia 4. Activación de protocolo SSL en el servidor web de la plataforma.



Evidencia 5. Interface del sistema de firma bajo el protocolo de comunicación HTTPS



Evidencia 6. Datos del Certificado de Cifrado de Comunicación HTTPS

En este sentido, sería recomendable que 3G Mobile Sign empleara como certificado electrónico para el cifrado de las comunicaciones, un certificado que además de garantizar la integridad de las comunicaciones, garantizara la identidad del titular del sitio web.

Una vez comprobado que el sistema garantiza que el protocolo de comunicaciones entre el usuario final y el dispositivo de captura y el servidor de 3G Mobile Sign cumple con los requisitos de seguridad en lo que respecta al canal de comunicación, el equipo auditor considera esencial determinar si el sistema emplea algún tipo de sistema para garantizar que, además del canal de comunicación, se cifra el contenido transmitido (el documento firmado y los metadatos asociados al mismo).

Del mismo modo, el equipo auditor ha analizado el código fuente del sistema de firma biométrica con el objetivo de verificar si el mismo incluye funcionalidades de cifrado, y tal y como se evidencia a continuación, en el código fuente se puede observar la funcionalidad de cifrado que el propio sistema de firma biométrica activa previamente a realizar la comunicación, siendo comprobado que el documento no ha sufrido modificación alguna, una vez recibido el documento en el servidor.

```
public static String encrypt(String s) throws UnsupportedEncodingException {
    String StringPublicKey = "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnNHwFuyC
                             "pVihKqgK0YM0Das7gLcdP0t3mkANPC0hLXpXRqGXBO6AsGrOM
                             "QwGNmK0TdILWBbBPYRI/PZp6Z5TD5RlAwuEJhH1sazaKNo6yC
    String resultado = s;
    PublicKey publicKey = null;
    try {
        publicKey = toPubKey(StringPublicKey);
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
    } catch (NoSuchProviderException e) {
        e.printStackTrace();
    } catch (InvalidKeySpecException e) {
        e.printStackTrace();
    } catch (IOException e) {
        e.printStackTrace();
    }

    try {
        Cipher cipher = Cipher.getInstance("RSA");
        cipher.init(Cipher.ENCRYPT_MODE, publicKey);
        byte[] cipherData = cipher.doFinal(s.getBytes());

        resultado = Base64.encodeToString(cipherData, Base64.NO_WRAP);
    } catch (InvalidKeyException e) {
        e.printStackTrace();
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
    } catch (NoSuchPaddingException e) {
        e.printStackTrace();
    } catch (IllegalBlockSizeException e) {
        e.printStackTrace();
    } catch (BadPaddingException e) {
        e.printStackTrace();
    }
    return resultado;
```

```
public String getCodigo() {
    return codigo;
}

public String getEncryptedPass() {
    String encPass = null;
    try {
        encPass = Utils.encrypt(Global.getPreferencias().getPass());
    } catch (UnsupportedEncodingException e) {
        e.printStackTrace();
    }
    return encPass;
}
```

Evidencia 7. Código fuente - Funcionalidad de cifrado del documento y metadatos

6.2.2 FIRMADO DEL DOCUMENTO ELECTRÓNICO MEDIANTE CERTIFICADO RECONOCIDO

El sistema de firmado móvil 3G Mobile Sign requiere para el correcto funcionamiento del sistema, la instalación en el servidor de un certificado de firma electrónica reconocido, siendo posible emplear certificados propios de 3G Mobile Sign, o bien certificados titularidad de cada uno de los clientes que contraten el servicio.

En caso de que el cliente decida emplear para firmar electrónicamente su propio certificado de firma electrónica reconocido, se ha comprobado que 3G Mobile Sign lleva a cabo la firma de un contrato de cesión temporal, depósito y gestión del certificado de firma. Para ello es necesario que, o bien el cliente final introduzca la clave privada del mismo, o bien ésta sea facilitada por éste a 3G Mobile Sign, con el fin de que éste la introduzca y gestione.

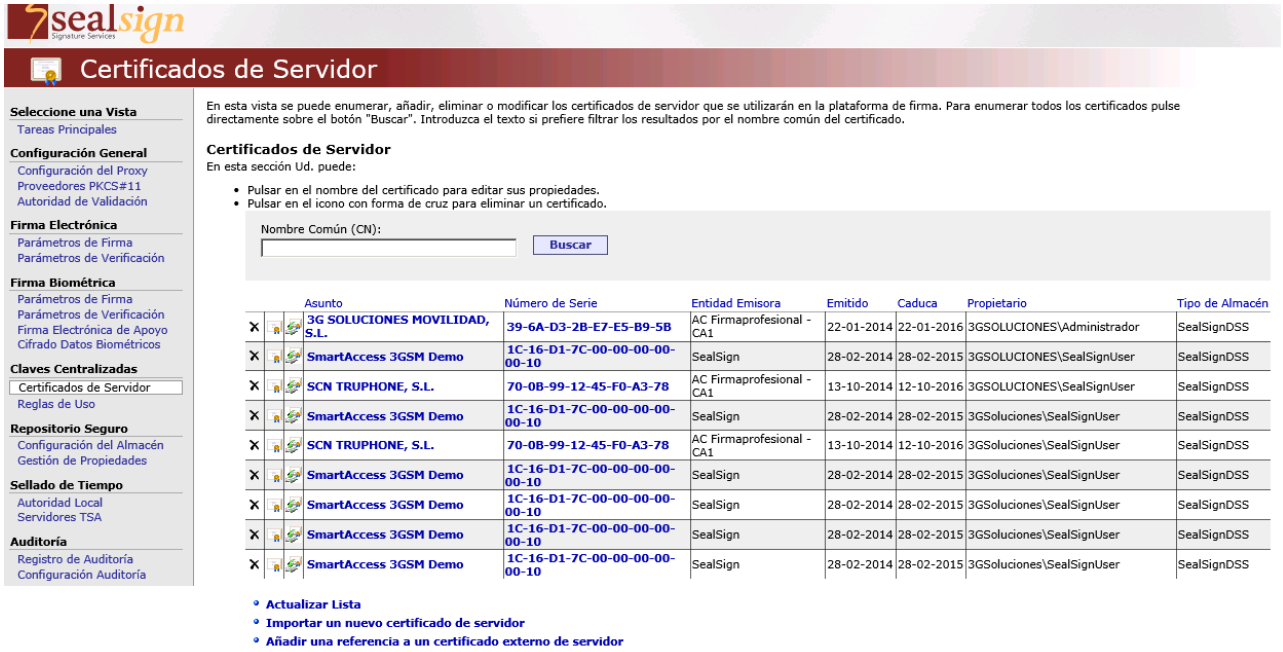
Tal y como ha podido comprobar el equipo auditor, el conjunto de certificados electrónicos empleados por la plataforma, son cargados en el servidor central de 3G Mobile Sign, donde son almacenados y donde el

sistema acude a realizar las consultas oportunas para llevar a cabo el proceso de firma de los documentos.

Evidencia 8. Almacén de Certificados de Firma Electrónica

En el momento de la realización de la auditoría, la plataforma objeto de análisis permite que el certificado empleado para firmar electrónicamente pueda ser un certificado propio de 3G Mobile Sign, un certificado propio del cliente final, que 3G Mobile Sign se encargará de instalar en la plataforma o bien un certificado propio del cliente final, que el propio cliente a través de la interface del sistema se encargará de instalar en la plataforma a través de la interface habilitada para ello. En caso de optar por esta tercera opción, en 3G Mobile Sign tendrá posibilidad de intervenir en el proceso de carga y gestión del certificado, en tanto no conocerá la clave privada del mismo necesaria para su instalación y/o exportación, tal y como se evidencia a continuación:

Evidencia 9. Carga de Certificados por parte del Cliente



Evidencia 10. Almacén de Certificados cargados por los clientes

```
public void setCertificate(Byte[] ficheroCertificado, String contrasena, String nombreDescriptivo)
{
    using (new Impersonator(System.Configuration.ConfigurationManager.AppSettings["SS_Impersonate_User"].ToString(), System.Configuration.ConfigurationManager.AppSettings["SS_Impersonate_Domain"].ToString(),
System.Configuration.ConfigurationManager.AppSettings["SS_Impersonate_Password"].ToString()))
    {
        WSAdminService.AdminServiceClient wsAdminServiceClient = new WSAdminService.AdminServiceClient();
        try
        {
            String owner = System.Configuration.ConfigurationManager.AppSettings["SS_Impersonate_Domain"] + @"\" + System.Configuration.ConfigurationManager.AppSettings["SS_Impersonate_User"];
            this.idCertificado = wsAdminServiceClient.ImportExtendedCertificateReference(ficheroCertificado, owner, false, true, contrasena, string.Empty, false, nombreDescriptivo);
        }
        catch (Exception ex)
        {
            throw new Exception("Error estableciendo certificado", ex.InnerException);
        }
        finally
        {
            wsAdminServiceClient.Close();
        }
    }
}
```

Evidencia 11. Código fuente – Carga de certificado de firma electrónica

```
public WSAdminService.ExtendedCertificateReference getCertificate()
{
    using (new Impersonator(System.Configuration.ConfigurationManager.AppSettings["SS_Impersonate_User"].ToString(), System.Configuration.ConfigurationManager.AppSettings["SS_Impersonate_Domain"].ToString(),
System.Configuration.ConfigurationManager.AppSettings["SS_Impersonate_Password"].ToString()))
    {
        WSAdminService.AdminServiceClient wsAdminServiceClient = new WSAdminService.AdminServiceClient();
        try
        {
            WSAdminService.ExtendedCertificateReference certificado = new WSAdminService.ExtendedCertificateReference();
            certificado = wsAdminServiceClient.GetExtendedCertificateReference(this.idCertificado, true);
            return certificado;
        }
        catch (Exception ex)
        {
            Utilidades.Log.log("ExtendedCertificateReference error " + ex.Message);
            throw new Exception("Error obteniendo certificado", ex.InnerException);
        }
        finally
        {
            try
            {
                wsAdminServiceClient.Close();
            }
            catch (Exception ex) {

            }
        }
    }
}
```

Evidencia 12. Código fuente – Consulta y utilización de certificado de forma automatizada por parte de la plataforma

A pesar de que el almacenamiento de los certificados es adecuado desde el punto de vista técnico, en tanto las claves privadas de los mismos no son conocidas más que por los titulares de éstos, desde el punto de vista del equipo auditor y con el fin de garantizar la securización plena del sistema, sería

recomendable que el sistema almacenara los certificados en un dispositivo seguro de almacenamiento centralizado de certificados, conocidos como HSM – Hardware Security Module.

6.2.3 GARANTÍAS DE NO REUTILIZACIÓN DE LA FIRMA

En un proceso de contratación realizado a través de medios electrónicos una de las principales cuestiones que pueden entrañar dudas es si la firma plasmada por parte del usuario final, así como los datos biométricos asociados a la misma, puede o no ser reutilizada posteriormente en otros procesos de firmado electrónico.

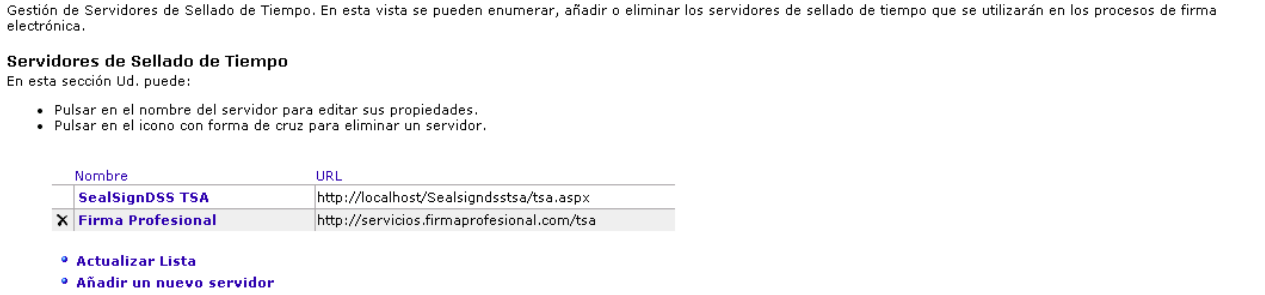
El hecho de que pudiera ser posible la reutilización de la firma y los metadatos asociados en un documento diferente, además de introducir un importante grado de desconfianza en el sistema, supone un riesgo desde el punto de vista jurídico que en ningún caso un sistema como el planteado puede permitirse.

El sistema objeto de análisis emplea para garantizar que la imagen gráfica de la firma, los datos biométricos y el propio documento firmado no puede ser reutilizado en ningún otro proceso de firmado, empelando para ello criptografía basada en infraestructura PKI aplicada sobre todos los elementos, concretamente el firmado electrónico, mediante certificado de firma electrónica reconocida, así como la aplicación de sellados de tiempo realizados por un Prestador de Servicios de Certificación (PSC) Reconocido o cualificado.

6.2.4 LA IMPORTANCIA DE LA APLICACIÓN DE SELLADOS DE TIEMPO RECONOCIDOS

Un aspecto esencial, aunque optativo, en los sistemas de firma biométrica, y en concreto, en el sistema de 3G Mobile Sign, donde interviene un elemento / dispositivo móvil, es la posibilidad de incorporar sellados de tiempo reconocidos, que permitan garantizar de forma fehaciente, el momento exacto en el que se produjo una determinada firma, y en consecuencia, el documento contractual generado, empieza a desplegar efectos.

En este sentido, el sistema 3G Mobile Sign, posibilita la configuración de incluir sellados de tiempo reconocidos, tal y como se evidencia a continuación, siendo éstos sellados de tiempo realizados por un Prestador de Servicios de Certificación (PSC) Reconocido o Cualificado.


Gestión de Servidores de Sellado de Tiempo. En esta vista se pueden enumerar, añadir o eliminar los servidores de sellado de tiempo que se utilizarán en los procesos de firma electrónica.

Servidores de Sellado de Tiempo

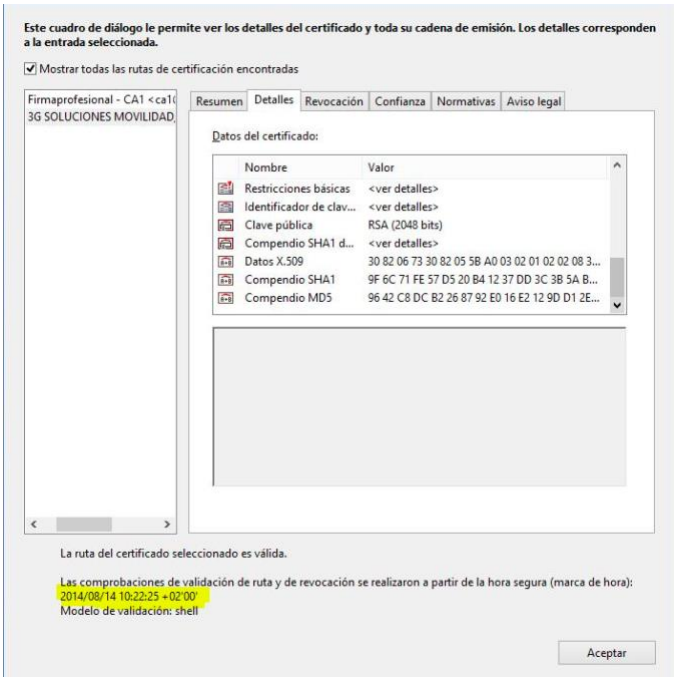
En esta sección Ud. puede:

- Pulsar en el nombre del servidor para editar sus propiedades.
- Pulsar en el icono con forma de cruz para eliminar un servidor.

	Nombre	URL
	SealSignDSS TSA	http://localhost/Sealsigndsstsa/tsa.aspx
✕	Firma Profesional	http://servicios.firmaprofesional.com/tsa

- Actualizar Lista
- Añadir un nuevo servidor

Evidencia 13. Configuración sellado de tiempo en sistema 3G Mobile Sign.



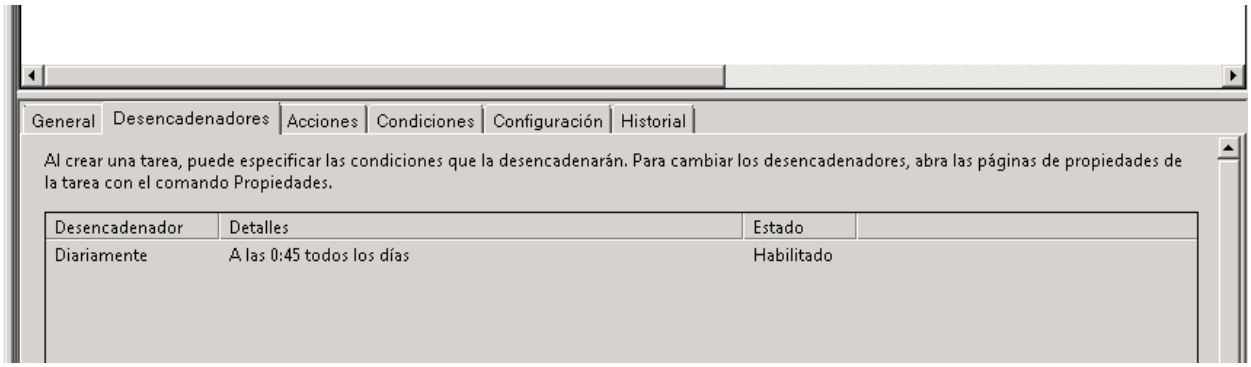
Evidencia 14. Sellado de Tiempo incluido como metadato en el documento firmado

6.3 MÓDULO DE ALMACENAMIENTO Y GESTIÓN DOCUMENTAL

6.3.1 GARANTÍAS DE INTEGRIDAD DE LA BASE DE DATOS DOCUMENTAL

1) Firmado periódico de la base de datos

Sobre la base de datos de gestión documental se realizan copias de seguridad periódicas al objeto de garantizar su disponibilidad. En este sentido, y tal y como se evidencia a continuación, las copias de seguridad se encuentran programadas, guardando una copia de cada uno de los backup realizados:

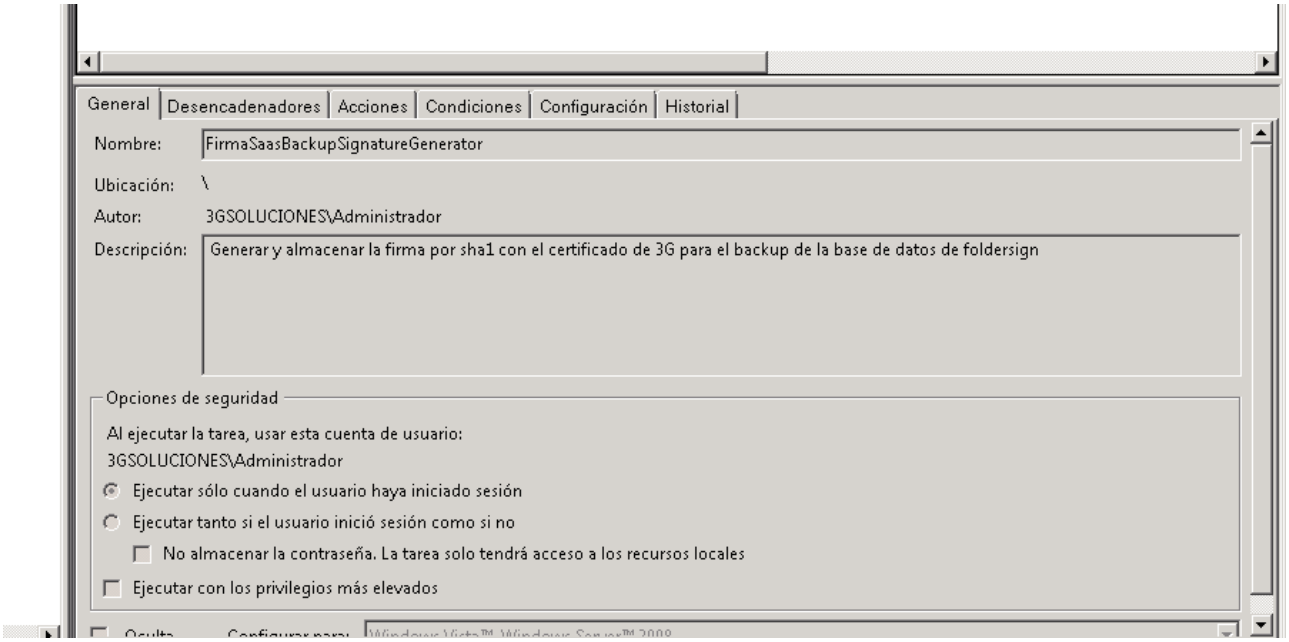


Evidencia 15. Programación de las copias de seguridad periódicas realizadas sobre la base de datos documental

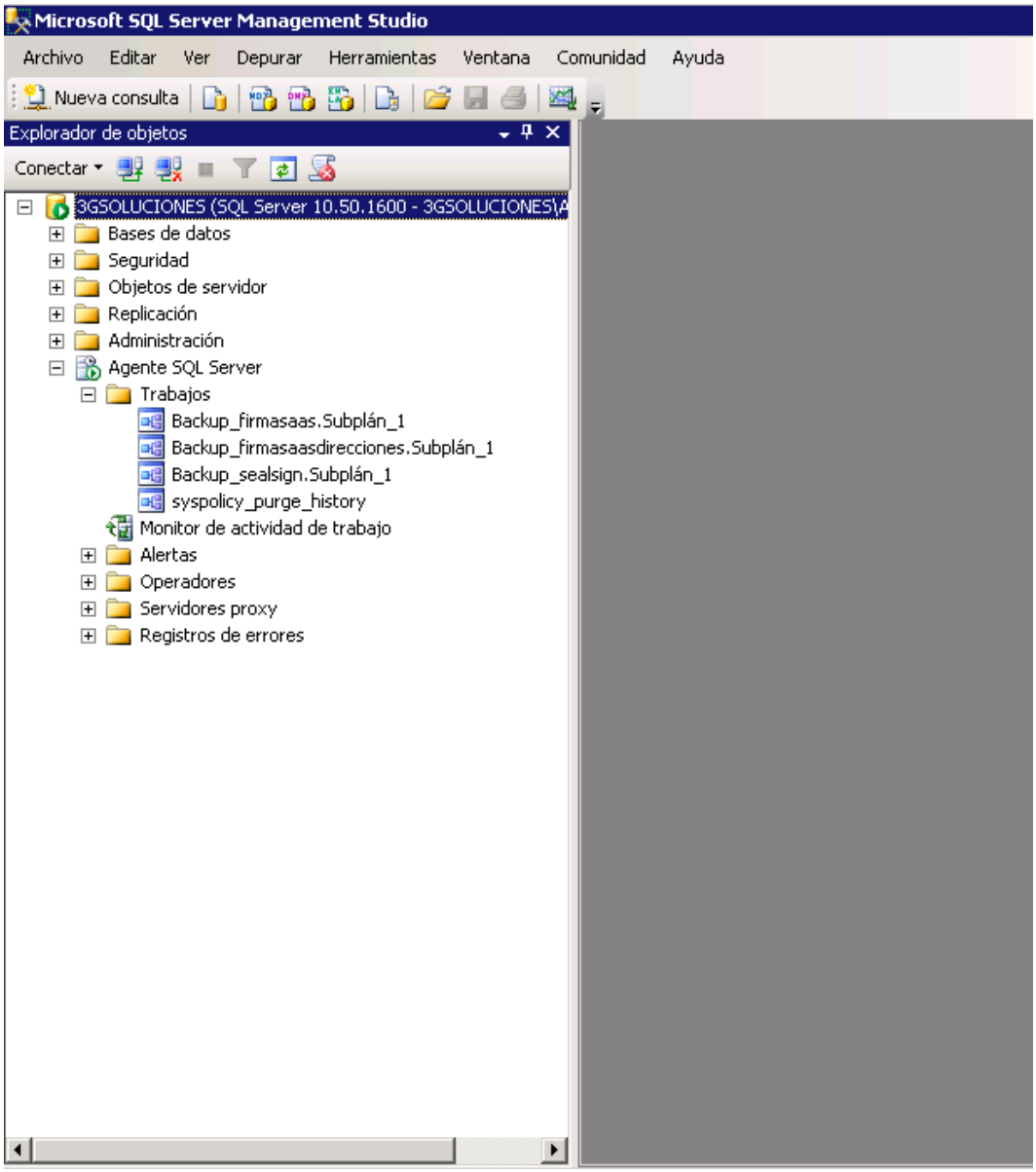
Nombre	Fecha de modificación	Tipo	Tamaño
firmasaas_backup_2014_05_25_003003_9243589.bak.gz	25/05/2014 0:30	Archivo WinRAR	300 KB
firmasaas_backup_2014_05_26_003003_9681587.bak.gz	26/05/2014 0:30	Archivo WinRAR	299 KB
firmasaas_backup_2014_05_27_003003_5393521.bak.gz	27/05/2014 0:30	Archivo WinRAR	300 KB
firmasaas_backup_2014_05_28_003003_5111478.bak.gz	28/05/2014 0:30	Archivo WinRAR	302 KB
firmasaas_backup_2014_05_29_003003_6489530.bak.gz	29/05/2014 0:30	Archivo WinRAR	302 KB
firmasaas_backup_2014_05_30_003003_7157542.bak.gz	30/05/2014 0:30	Archivo WinRAR	305 KB
firmasaas_backup_2014_05_31_003003_6255463.bak.gz	31/05/2014 0:30	Archivo WinRAR	305 KB
firmasaas_backup_2014_06_01_003003_8613571.bak.gz	01/06/2014 0:30	Archivo WinRAR	303 KB
firmasaas_backup_2014_06_02_003003_7541483.bak.gz	02/06/2014 0:30	Archivo WinRAR	303 KB
firmasaas_backup_2014_06_03_003003_3083384.bak.gz	03/06/2014 0:30	Archivo WinRAR	307 KB
firmasaas_backup_2014_06_04_003003_4351430.bak.gz	04/06/2014 0:30	Archivo WinRAR	308 KB
firmasaas_backup_2014_06_05_003003_4779428.bak.gz	05/06/2014 0:30	Archivo WinRAR	311 KB
firmasaas_backup_2014_06_06_003003_5517443.bak.gz	06/06/2014 0:30	Archivo WinRAR	318 KB
firmasaas_backup_2014_06_07_003003_6245458.bak.gz	07/06/2014 0:30	Archivo WinRAR	319 KB
firmasaas_backup_2014_06_08_003003_6703457.bak.gz	08/06/2014 0:30	Archivo WinRAR	319 KB
firmasaas_backup_2014_06_09_003003_6801436.bak.gz	09/06/2014 0:30	Archivo WinRAR	319 KB
firmasaas_backup_2014_06_10_003003_8169488.bak.gz	10/06/2014 0:30	Archivo WinRAR	320 KB
firmasaas_backup_2014_06_11_003003_8467478.bak.gz	11/06/2014 0:30	Archivo WinRAR	322 KB
firmasaas_backup_2014_06_12_003002_9824957.bak.gz	12/06/2014 0:30	Archivo WinRAR	322 KB
firmasaas_backup_2014_06_13_003003_1813044.bak.gz	13/06/2014 0:30	Archivo WinRAR	323 KB
firmasaas_backup_2014_06_14_003003_1010972.bak.gz	14/06/2014 0:30	Archivo WinRAR	322 KB
firmasaas_backup_2014_06_15_003003_1979000.bak.gz	15/06/2014 0:30	Archivo WinRAR	322 KB
firmasaas_backup_2014_06_16_003003_2306992.bak.gz	16/06/2014 0:30	Archivo WinRAR	323 KB
firmasaas_backup_2014_06_17_003003_8984609.bak.gz	17/06/2014 0:30	Archivo WinRAR	324 KB
firmasaas_backup_2014_06_18_003004_1768966.bak.gz	18/06/2014 0:30	Archivo WinRAR	323 KB
firmasaas_backup_2014_06_19_003003_7266682.bak.gz	19/06/2014 0:30	Archivo WinRAR	326 KB

Evidencia 16. Backup disponibles de la base de datos documental

Del mismo modo, y para garantizar la integridad de la base de datos documental, el sistema objeto de evaluación se encuentra programado para llevar a cabo firmados periódicos de la base de datos documental. En este sentido, a continuación se incorporan las evidencias relativas a la programación del firmado periódico de la base de datos, así como el listado de backup firmados:



Evidencia 17. Sistema automático firmado periódico base de datos documental



Evidencia 18. Bases de datos firmadas periódicamente.

6.4 LA FIRMA BIOMÉTRICA DIGITALIZADA COMO FIRMA ELECTRÓNICA AVANZADA

De conformidad con lo dispuesto en el artículo 3.2 de la Ley 59/2003 de Firma Electrónica, la firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Atendiendo a la descripción del sistema de firma biométrica digital realizada a lo largo del presente informe, podemos comprobar cómo, el mismo permite cumplir con los requisitos expresamente exigidos para que la firma biométrica generada pueda ser considerada una firma electrónica avanzada, dado que:

1) **Permite identificar al firmante**, en tanto se trata de una firma manuscrita asociada directamente al titular de la firma.
2) **Permite detectar cualquier cambio ulterior de los datos firmados**, en tanto el documento firmado, así como el grafo de la firma y los propios datos biométricos asociados a la firma manuscrita son debidamente cifrados mediante un certificado de firma electrónica reconocida.

3) **Que se encuentre vinculada de manera única al firmante**, en tanto los datos biométricos asociados a una firma manuscrita se encuentra directa y únicamente asociados a una persona concreta, siendo acreditado mediante prueba perito caligráfica posterior en sede judicial.
4) **Que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control**, en tanto es directamente el propio firmante el que crea la firma mediante la realización del trazado correspondiente en la pantalla del dispositivo.

Por todo ello, entendemos que la firma resultado del sistema objeto de análisis podría quedar englobada dentro del concepto de **firma electrónica avanzada**, generando así los siguientes efectos:

a) *"Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil3", según establece el art. 3.8 de la LFE.*
b) *"No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica", según se establece en el artículo 3.9 LFE.*

Queda acreditado por tanto, que la firma biométrica, cuando reúne los requisitos establecidos por la Ley de Firma Electrónica y adquiere la consideración de firma electrónica avanzada, genera todos sus efectos, también en vía judicial, conforme se ha visto anteriormente.

6.5 LA FIRMA BIOMÉTRICA DIGITALIZADA Y SU VALIDEZ PROCESAL

Con independencia de que no existe una definición legal de la misma, la evidencia o prueba electrónica puede definirse como el soporte susceptible de almacenar información digital con la finalidad de acreditar hechos ante los Tribunales.

Desde el punto de vista procesal, como norma general, la evidencia electrónica puede tener carácter de prueba documental (por ejemplo, el mero almacenamiento de una fotografía en soporte digital) o pericial (por ejemplo, un informe en el que se analice el contenido de un equipo informático). Para asegurar la admisibilidad de la prueba electrónica en un proceso judicial, han de cumplirse los siguientes requisitos:

1) **Licitud:** La prueba electrónica ha de obtenerse de forma lícita, sin vulnerar el derecho a la intimidad y el secreto de las comunicaciones que garantiza el art. 18 de la Constitución Española. En el caso de que sea necesario realizar una injerencia en dichos derechos para la obtención de una evidencia electrónica, sería necesaria una Resolución Judicial expresa y motivada que lo autorizara, fundada en la existencia de sospechas de la comisión de un delito.

   En todo caso, hay que tener presente el art. 197 del Código Penal, que regula el delito de revelación de secretos, castigando con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses, al que se apodere de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales de un tercero, o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, sin consentimiento.

2) **Autenticidad:** debe garantizarse que la prueba es auténtica, es decir, que lo que se analiza es exactamente lo ocupado en la actuación, lo que requiere que se haya realizado adecuadamente la cadena de custodia.

[3] *"2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.*
Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica".

3) **Integridad:** dada la extremada mutabilidad de las pruebas electrónicas, es necesario preservar la integridad de los medios de almacenamiento originales (PC, PDA, Pendrive, etc.), no alterando su contenido, siendo por tanto esencial emplear sistemas que garanticen que no es posible la modificación del contenido.

4) **Claridad:** el componente tecnológico de la prueba electrónica hace que los expertos deban presentarla ante los Tribunales de forma clara y comprensible, para que personas legas en informática puedan comprenderla.

6.5.1 ADMISIBILIDAD Y VALIDEZ PROBATORIA EN SEDE JUDICIAL

La Ley de Enjuiciamiento Civil, aplicable al proceso civil y, de forma supletoria, a los procedimientos del resto de Jurisdicciones de conformidad con lo dispuesto en el art. 4 de la Ley de Enjuiciamiento Civil, establece que se admitirán, como medios de prueba, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.

Asimismo, el documento electrónico, de conformidad con lo dispuesto en el artículo 3-6 de la Ley 59/2003 de Firma Electrónica podrá ser soporte de documentos públicos o privados, de forma que, reuniendo los requisitos legales y tecnológicos establecidos para ello, se admite su valor equivalente al de la firma manuscrita.

De esta forma, su valor probatorio dependerá de la acreditación del tipo de firma electrónica empleada, del certificado empleado y del cumplimiento de los requisitos legales exigibles al tipo de documento al que le presta soporte.

En particular, en los procesos penales, el art. 26 del Código Penal admite la prueba electrónica, al establecer que se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

De esta manera, al amparo de lo dispuesto en los arts. 281 y siguientes de la Ley de Enjuiciamiento Civil, dado que este tipo de prueba (i) está expresamente prevista en la Ley, (ii) es necesaria para la resolución del litigio y (iii) cumple los requisitos previstos legalmente para proceder a su práctica; la inadmisión de la misma vulneraría el Derecho a la Tutela Judicial Efectiva consagrado por el art. 24 de la Constitución Española, ya que supondría negar el derecho a que queden acreditados extremos que podrían influir decisivamente en la sentencia que resuelva el procedimiento.

En este sentido se ha pronunciado, de forma general, la Sentencia del Tribunal Constitucional 82/2006, Sala 2ª, de 13 marzo, garantizando a las partes el derecho a impulsar una actividad probatoria acorde con sus intereses, evitando la indefensión que se produciría si la actividad probatoria que no fue admitida o practicada fuera decisiva en términos de defensa, esto es, que hubiera podido tener una influencia decisiva en la resolución del pleito, al ser susceptible de alterar el Fallo.

Por tanto y a tenor literal de la información anteriormente indicada, la firma biométrica digital tendrá valor probatorio en juicio debiendo ser admitida a trámite por el tribunal, para su posterior valoración y comprobación del cumplimiento de los requisitos anteriormente indicados en sede judicial.

El sistema planteado permite a los usuarios, en tiempo real, poder comparar la firma efectivamente realizada por parte de un usuario, con el patrón de otra firma obtenida de éste, permitiendo al algoritmo matemático que integra la herramienta poder evaluar los puntos de coincidencia con el sistema.

Así, cuando se pretenda considerar la firma biométrica en un procedimiento judicial, las pautas y necesidades para su aportación en el contexto de un dictamen de peritos se dan en dos escenarios:

1) **Comprobación de firmas.** Se trata en este caso de verificar que la Firma biométrica incorporada a un documento es la que en su momento se realizo (autenticidad) y que no ha sido alterada (integridad). En este caso, el proceso habría de ser:
   - **a)** Acceso al sistema de custodia de los datos relativos a la firma biométrica almacenada en el momento de su generación.
   - **b)** Considerando que la integridad de tales datos es garantizada desde el momento de su generación mediante certificados de firma electrónica, en este momento se deberán utilizar los medios que nos permiten acceder a los datos sin poner en riesgo tal integridad. Así por ejemplo, en el caso de haber utilizado firma electrónica, en este momento se utilizará la clave pública del firmante para acceder a los datos de la firma biométrica.
   - **c)** Comprobación técnica de la correspondencia entre la firma biométrica almacenada y aquella que se pretende como la misma, con el fin de verificar tal afirmación.

   Se trata de conocer si los datos de la firma biométrica "original" se encuentren, idénticos en la que se pretende como igual, sin que hayan de considerarse otros factores exógenos o endógenos a la firma ni a su proceso de creación. Dicha determinación, que se trata de una tarea eminentemente técnica, será realizada por un perito experto en la materia.

2) **Comparación de firmas.** Se trata de verificar la autoría de una Firma biométrica mediante su comparación con otra/s firma/s biométrica/s (muestra/s) del mismo autor. En este caso, el proceso habría de ser:
   - **a)** Acceso al sistema de custodia de los datos relativos a la firma biométrica almacenada en el momento de su generación.
   - **b)** Comprobación de la integridad de los datos
   - **c)** Cotejo de firmas tendente a averiguar la autoría de las mismas.

   En este punto, de forma similar a lo que sucede con relación a la firma manuscrita realizada en papel con tinta, existiría una firma indubitada (la almacenada en el sistema de custodia de datos de firmas biométricas) y la dubitada, que sería objeto de cotejo.

   Podrán utilizarse diferentes técnicas, pero en todo caso (al contrario que el supuestos anterior) parece conveniente la actuación de un perito calígrafo que a su vez tenga los conocimientos, herramientas y experiencia adecuada con relación a la Firma biométrica.

Entre otras, estas serán las comprobaciones que en sede judicial serán llevadas a cabo sobre la prueba electrónica resultante del proceso de firma biométrica digital.

7 CONCLUSIONES

Tomando en consideración lo expuesto en el presente Informe, se pueden extraer las siguientes conclusiones:

1) Se entiende por Firma biométrica la información que escribe una persona de su propia mano a través de un dispositivo electrónico, en un documento con el fin bien de dar autenticidad al documento firmado o expresar que aprueba el contenido del mismo, y a la que se añade el resultado de medir fenómenos o procesos biológicos asociados al proceso de generación de la firma o rúbrica.

2) La Firma biométrica tiene como finalidades por tanto:
   - Que se pueda demostrar que el autor de la firma es quien dice haberla hecho (autenticidad),
   - Y que sirva como método o forma de mostrar la aprobación sobre lo firmado (consentimiento).

3) En el proceso de generación y captación (para su posterior almacenamiento) de la Firma biométrica, los objetivos fundamentales a alcanzar son:

   - Obtener garantías de que la firma biométrica generada no se puede reproducir, en su totalidad o de manera parcial, con el fin de evitar el riesgo de su utilización con fines fraudulentos o no.
   - Obtener garantías de integridad y no alteración de los datos biométricos, ni por su autor, ni por ningún tercero, con fines fraudulentos o no, con el objetivo de que puedan utilizarse en sede judicial. A tal fin, lo más recomendable es firmar los datos biométricos con Firma electrónica Reconocida o al menos con Firma electrónica avanzada.

4) Las garantías requeridas para generar los efectos legales de acreditar la identidad de una persona, garantizando la autenticidad de su firma, y la integridad de los datos biométricos (o metadatos) son obtenidas en el sistema de firma biométrica analizado en el presente informe a través de:

   - Obtención de la imagen gráfica de la firma biométrica, así como de los metadatos o datos biométricos asociados y que permiten acreditar la autenticidad de la misma. Concretamente, es necesario disponer de la velocidad y la presión, como mínimo.
   - Envío y comunicación firma biométrica obtenida y metadatos de manera cifrada utilizando al efecto los correspondientes certificados electrónicos.
   - El sistema de firma biométrica cuenta con un servicio de sellado de tiempo. En este caso, el documento se almacena con la firma biométrica, los metadatos, y el sellado de tiempo, que garantiza además la temporalidad del documento, desde el momento exacto en el que fue firmado y hacia el futuro.

5) La garantía de eficacia se ve reforzada además con el servicio legal integrante del sistema de firma biométrica objeto del presente Informe. El servicio legal se encargará de:
   - Validar
   - Auditar
   - Asistir legalmente todo el procedimiento del sistema de firma biométrica.

6) La firma biométrica digital, siempre que cumpla con todos los requisitos descritos a lo largo del presente informe, podría quedar englobada dentro del concepto de firma electrónica avanzada de conformidad con lo dispuesto en la Ley de Firma Electrónica.

7) El almacenamiento de los datos de Firma biométrica podrá realizarse por medios propios o de un tercero, tal y como se recoge y valida por la normativa de aplicación. Dichos terceros deberán respetar las medidas de seguridad establecidas por el RLOPD, cuestión que queda debidamente regulada en las condiciones de contratación previstas por 3G Mobile Sign.

8) La aportación en juicio de la Firma biométrica se regirá por las reglas generales de la Prueba, y normalmente requerirá de la generación de un Dictamen pericial, que en el caso objeto de este informe deberá ser emitido, tanto por un perito calígrafo, como por parte de un perito informático especialista en seguridad.

9) Así, el cumplimiento y consecución de los objetivos y fines de la firma biométrica, dependerá de la fortaleza del sistema integral, procedimientos, metodologías y algoritmos de obtención, análisis, comunicación y tratamiento de la firma biométrica, de la capacidad para limitar errores o falsos positivos y de la pericia, herramientas, metodología y expertise del perito encargado de su cotejo (en caso de juicio).

   Estos aspectos quedan garantizados y cumplidos por el sistema de firma biométrica expuesto, al integrar todos los requisitos y ámbitos de protección requeridos por las normativas de aplicación, y contar además con un proceso de continua validación, auditoria y asistencia legal al procedimiento

de obtención del consentimiento informado a través de firma biométrica analizado en el presente Informe.

8 ANEXO I – CERTIFICADO DE CUMPLIMIENTO DEL FABRICANTE

SMARTACCESS

En Madrid, a 30 de septiembre de 2014

D. Rames Sarwat Schaker, con DNI 05.275.000-L. en su condición de Administrador Único y en nombre y representación de SMARTACCESS S.L, con CIF B-84620111, domicilio social en Paseo de la Castellana 129, 28046 Madrid e inscrita en el Registro Mercantil de Madrid, al Tomo 22.392, Folio 113 Sección 8 Hoja M-399917,

DECLARA RESPONSABLEMENTE

1) Que en la actualidad, como fabricante de software, cuenta con un acuerdo con la compañía 3G Soluciones Móviles S.L (en adelante Foldersign) para la provisión a ésta de software de captura de firma biométrica en dispositivos fijos y móviles, en base al que Foldersign ha integrado dicho software dentro de su servicio online accesible desde www.foldersign.com.

2) Que como fabricante del software de firma biométrica reconoce la importancia que tiene para un sistema como Foldersign que los documentos y evidencias electrónicas generadas a partir del software cuenten con las máximas garantías probatorias, así como con las máximas garantías desde el punto de vista de la seguridad y legalidad.

3) Que tiene conocimiento de que Foldersign ha sometido su servicio completo, accesible desde www.foldersign.com, a un proceso de auditoría jurídico tecnológica, en la que se ha analizado entre otros aspectos el grado de validez y reconocimiento jurídico, como prueba electrónica, de las evidencias electrónicas con documentos firmados mediante firma biométrica.

4) Que dado que el software provisto por SmartAccess y empleado por parte de Foldersign es el encargado de generar la captura de los datos biométricos asociados a la firma, así como el aseguramiento de la integridad de la evidencia electrónica, garantiza mediante la firma de la presente declaración que el software cumple plenamente con los requisitos indicados a continuación:

   - Que el software permite capturar los documentos firmados en un formato interoperable, autosuficiente y autodocumentado, tales como PDF, PDF/A, XPS y XML.
   - Que el software garantiza que en todo caso se obtiene durante la realización de las firmas por parte de los usuarios y siempre que el dispositivo de captura (tableta, fija o móvil así lo permita) capturar los siguientes datos: trazado de la firma, velocidad y presión ejercida por el firmante, como datos biométricos
   - Que dichos datos capturados durante el proceso de firma, son introducidos automáticamente y de forma instantánea en el documento, y sin ningún tipo de manipulación previa, como metadatos en formato autodocumentado e interoperable, en el propio documento electrónico firmado.
   - Que dichos datos biométricos quedan vinculados de forma única la firma y los metadatos al documento firmado por el usuario.
   - Que el software permite la incorporación de metadatos adicionales, tales como la geolocalización, versión del software de captura o modelo de la tableta de captura.
   - Que el software no requiere para su funcionamiento la aplicación de no se producen almacenamientos intermedios, antes de que quede garantizada la integridad e invariabilidad del documento electrónico y sus metadatos asociados.
   - Que no es posible reutilizar la firma obtenida en otro documento diferente al contrato asociado al proceso de contratación efectuado por el usuario final
   - Que el software calcula el hash del contrato de forma automática, empleando para ello algoritmos de cálculo cuya seguridad e integridad se encuentra garantizada.
   - Que dichos algoritmos son actualizados en función del estado de la técnica, con el fin de garantizar que los algoritmos empleados son seguros en el momento de su utilización.
   - Que el software, tras el calculo del hash, lleva a cabo de forma completamente automática y en todo caso la comprobación de la identidad del mismo, garantizándose así la integridad del documento.
   - Que el software permite invocar un sellado de tiempo, de forma completamente automática, sobre cada uno de los documentos electrónicos y sus metadatos generados por el software.

Fdo. Rames Sarwat Shaker

SMARTACCESS S.L, con CIF B-84620111 - Paseo de la Castellana 129, 28046 Madrid e inscrita en el Registro Mercantil de Madrid, al Tomo 22.392, Folio 113 Sección 8 Hoja M-399917 - www.smartaccess.com