ECIJA

INFORME JURÍDICO

EVALUACION DEL CUMPLIMIENTO Y EFICACIA DEL SISTEMA ONE TIME PASSWORD

3G MOBILE GROUP

3 de marzo de 2020

ÍNDICE

TIPO DE DOCUMENTO				Ámbito general
			X	Confidencial
TÍTULO	Informe jurídico OTP			
DESTINATARIO	3G SOLUCIONES MOVILIDAD S.L			
FORMATO	PDF			
PÁGINAS	23			
VERSIÓN	**FECHA**	**EVALUADOR**		
1.0	02/03/2020	ECIJA LEGAL S.L.U.		

Fdo. Alonso Hurtado
.....

Firmado por HURTADO BUENO FRANCISCO ALONSO - 52699229L el día 03/03/2020

Fdo. Mar Ibáñez
.....

Firmado digitalmente por NOMBRE IBAÑEZ MARTI MARIA DEL MAR - NIF 19898509J
Fecha: 2020.03.03 11:37:47 +01'00'

1 INTRODUCCIÓN

En los últimos años, se ha demostrado que la utilización de contraseñas estáticas es un mecanismo insuficiente para la autenticación en internet, puesto que, con el avance actual de la tecnología, son susceptibles de sufrir ataques y ser descubiertas muy fácilmente.

Una forma de securizar la autenticación es mediante la utilización de tecnología de autenticación de doble factor. En la actualidad, esta tecnología está siendo ampliamente implantada, una vez se han superado sus problemas iniciales de falta de interoperabilidad entre los proveedores, o la posible necesidad de que el firmante disponga de un dispositivo que sólo se utilice para la autenticación.

El sistema One Time Password (OTP) propone un algoritmo de contraseña de un solo uso. Este sistema puede ser implementado en cualquier aplicación y en cualquier hardware para permitir la autenticación y firma electrónica de personas o máquinas. Es un sistema de gran usabilidad, frente a las técnicas de claves asimétricas (certificados digitales) o uso de biometrías.

Hay que tener en cuenta que el algoritmo OTP por sí solo no prevé la privacidad de los datos, puesto que no implica la encriptación de las comunicaciones sobre los que vaya a ser utilizado, por lo que se utilizarán otros mecanismos adicionales que aseguren su confidencialidad, como el uso de claves de cifrado para encriptar la comunicación.

3G Mobile Group (en adelante 3G) es una entidad incluida en el registro público del Ministerio de Economía y Empresa (actual órgano competente en materia de servicios electrónicos de confianza) como Proveedor de Servicios de Confianza no Cualificados. 3G Mobile Group desarrolla servicios electrónicos y aplicaciones que ayudan a la transformación digital de las empresas, disponiendo, entre otras, de una plataforma propia de aplicaciones móviles.

La plataforma de 3G permite, entre varios métodos de firma, la firma mediante códigos OTP.

El presente informe tiene por objetivo determinar el grado de cumplimiento normativo y de seguridad que ofrece la firma con OTP utilizada por la Plataforma de firma de 3G.

2 OBJETO Y ALCANCE.

En el objeto del presente informe queda comprendida la evaluación jurídica y su eficacia probatoria ante juicio en lo referente la utilización del código OTP de la plataforma de firma de 3G para la firma de documentos. Queda comprendido en el alcance del presente informe las siguientes acciones:

1) Evaluar el nivel de cumplimiento normativo de la plataforma de firma de 3G para la firma de documentos mediante OTP.

2) Evaluar si el documento electrónico resultante contaría con valor judicial probatorio, y en su caso, determinar el grado de validez de este, atendiendo a los requisitos dispuestos por la Ley de Enjuiciamiento Civil y demás normativa de aplicación.

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 las evidencias electrónicas generadas por 3G en sede judicial o ante autoridad administrativa.

De esta forma, su objetivo no es otro que analizar, a juicio del equipo informante y teniendo en cuenta la normativa y el estado de la técnica existente en el momento de la firma del presente informe, cuál sería el grado de eficacia probatoria que presentarían las pruebas electrónicas generadas y que podrían ser hipotéticamente utilizadas por 3G en caso de reclamación o litigio si el sistema diseñado es finalmente implementado en las condiciones recomendadas.

3 LEGISLACIÓN APLICABLE.

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

1) Reglamento (UE) 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 el que se deroga la Directiva 1999/93/CE (EIDAS)
2) Reglamento de Ejecución (UE) 2015/1502, de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento eIDAS
3) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
4) Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
5) Ley 59/2003, de 19 de diciembre, de firma electrónica (en aquellos aspectos que complemente al EIDAS)
6) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de carácter personal y garantía de los derechos digitales (LOPDGDD).
7) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI)

Del mismo modo, se ha tenido en consideración para el análisis los estándares ETSI y en su caso CEN relacionados con las tecnologías implicadas en el proceso, tanto de identificación como de firma electrónica, así como las RFC relativas a One Time Password (OTP).

4 METODOLOGÍA EMPLEADA.

Para la realización del proceso de evaluación del cumplimiento, ECIJA ha empleado en todo momento una metodología sistemática, basada en una lista de control previamente

diseñada, en la que se plantea el análisis de las cuestiones expresamente referenciadas en la normativa de referencia.

Las valoraciones contenidas en el presente informe se basan en las manifestaciones realizadas por 3G, y sus conclusiones están supeditadas a una posterior obtención de evidencias de la información facilitada.

5 METODOS PARA GENERACIÓN DE CLAVE.

Partiendo de las evidencias aportadas por 3G así como la lista de control contestada por la entidad, para acceder al documento el firmante previamente se debe identificar en la plataforma de 3G, por lo que la firma con OTP se emplea como doble factor de autenticación.

Los datos que han servido para identificar al firmante se obtendrán a partir de la información presentada por el mismo, por lo que la responsabilidad de la veracidad de los datos es del propio firmante.

Por ello, se refleja expresamente que queda fuera del presente informe la previa identificación del firmante y la comprobación de la veracidad de los datos aportados por el mismo. La evaluación del sistema se realiza a partir del envío del OTP al firmante para la firma del documento.

El hecho de utilizar el terminal móvil como dispositivo para la recepción del OTP ha facilitado la expansión del uso de esta tecnología. Efectivamente, el teléfono móvil es un dispositivo con el que en la actualidad cuenta la mayor parte de la población, por lo que resulta muy sencillo y se evita el gasto que puede suponer la adquisición de un dispositivo ad-hoc para la utilización de este tipo de sistema One Time Password (OTP)

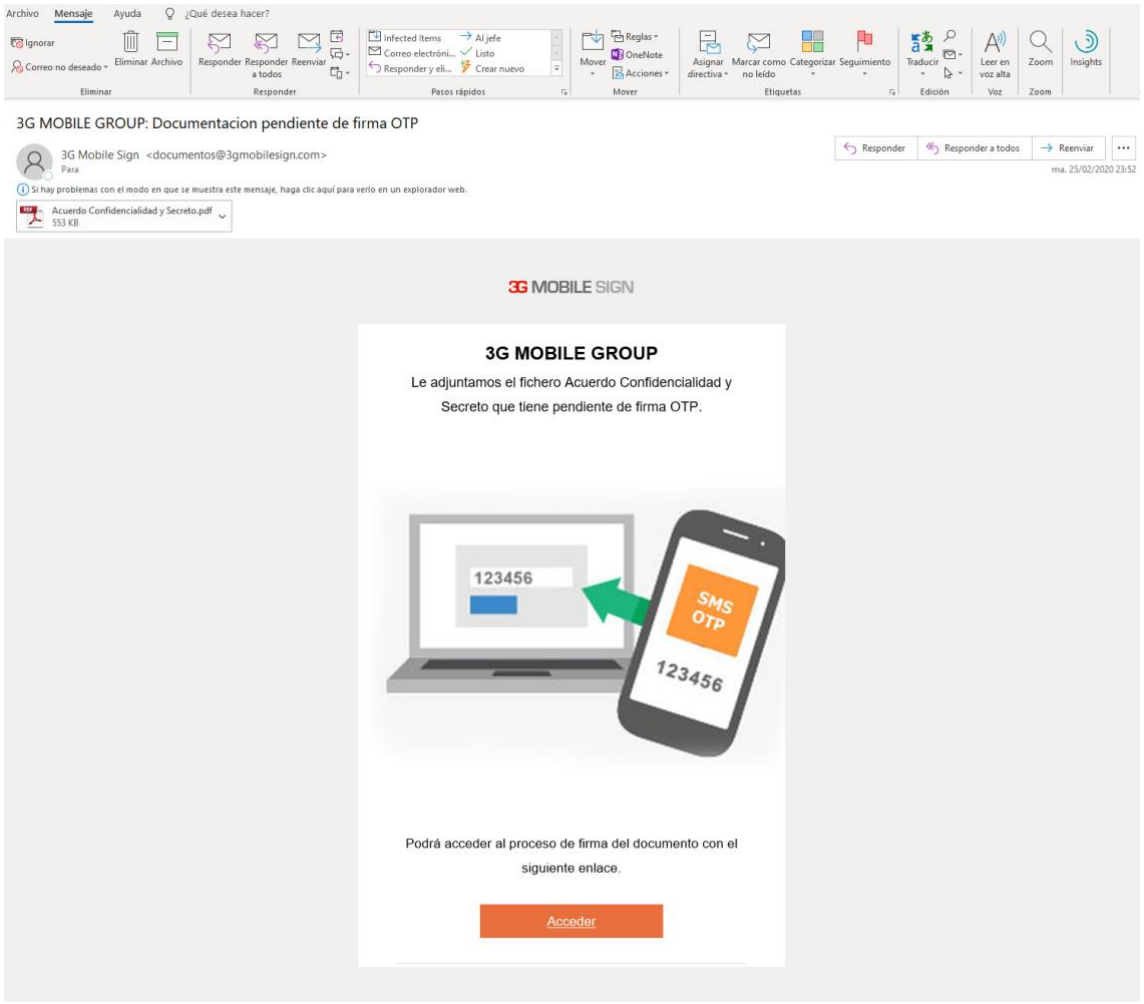
El sistema OTP de la plataforma 3G puede funcionar de las tres formas detalladas a continuación.

5.1 COMUNICACIÓN VÍA EMAIL Y OTP VIA SMS TELÉFONO MÓVIL.

El firmante recibirá una notificación por mail donde se le informa que tiene un documento pendiente de firma en una URL determinada.

Para acceder al documento desde la URL recibida, puede hacerlo a través de tres métodos diferentes, que elige el cliente de 3G que genera el proceso de firma.

a) Por el simple hecho de pinchar el enlace a la URL del documento, éste se puede visualizar en pantalla.
b) Identificarse mediante la dirección de correo electrónico y una clave que se le facilita en el propio mail.
c) Identificándose a través de uno o más campos con información personal que no está incluida en la propia comunicación por email, por ejemplo, el DNI, un numero de seguridad social, un numero de abonado, etc.



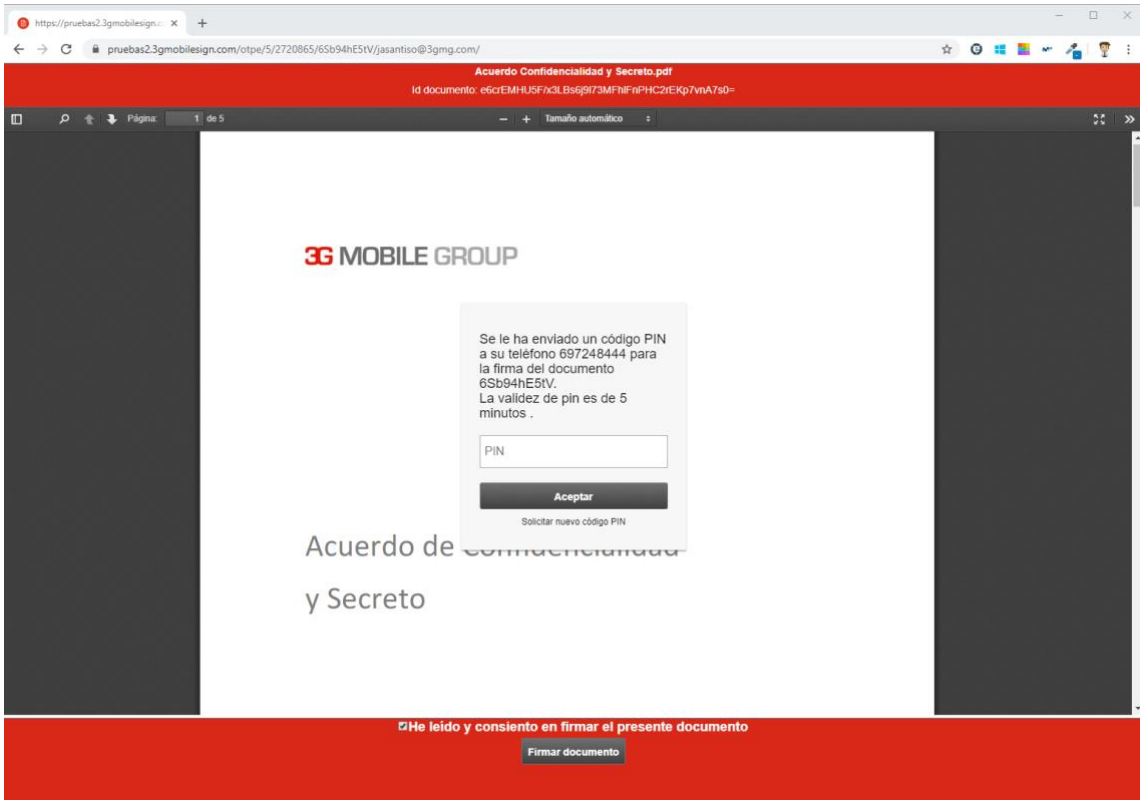
Evidencia 1: notificación por mail con URL de acceso al documento

Una vez el firmante se ha identificado por alguno de estos métodos, accede a la plataforma, que se encuentra en un entorno privado y securizado, y puede ver los documentos pendientes de firma por su parte.

El equipo auditor de ECIJA recomienda la utilización del método c), de autenticación previa al acceso al documento, para evitar que, en caso de un correo que haya sido interceptado, otra persona pueda acceder al documento.

Al pulsar en "Firmar documento" se envía un OTP a través de un sms al movil para su uso para firmar. En dicho SMS se informará del identificador del documento, que debe coincidir con el id del documento mostrado en pantalla y que queda archivado en la base de datos, debidamente cifrada e integra.

Evidencia 2: acceso al documento para la firma

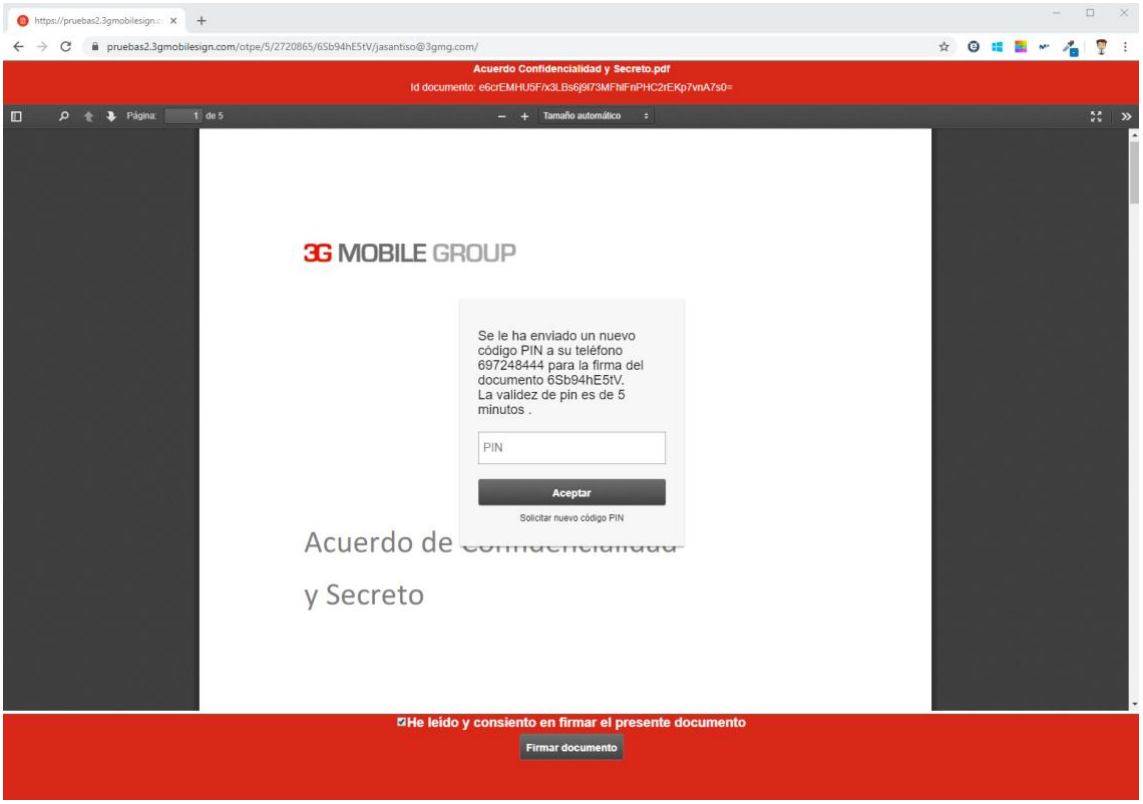


Evidencia 3: comunicación por SMS de envío de OTP, tiempo de validez e identificador del documento.

Evidencia 4: mensaje SMS con la clave OTP y el identificador del documento.

La plataforma permite el reenvío del OTP por SMS en caso de que no se hubiera recibido o hubiera caducado, generándose en este caso una nueva comunicación con una clave diferente a la generada en el momento inicial.

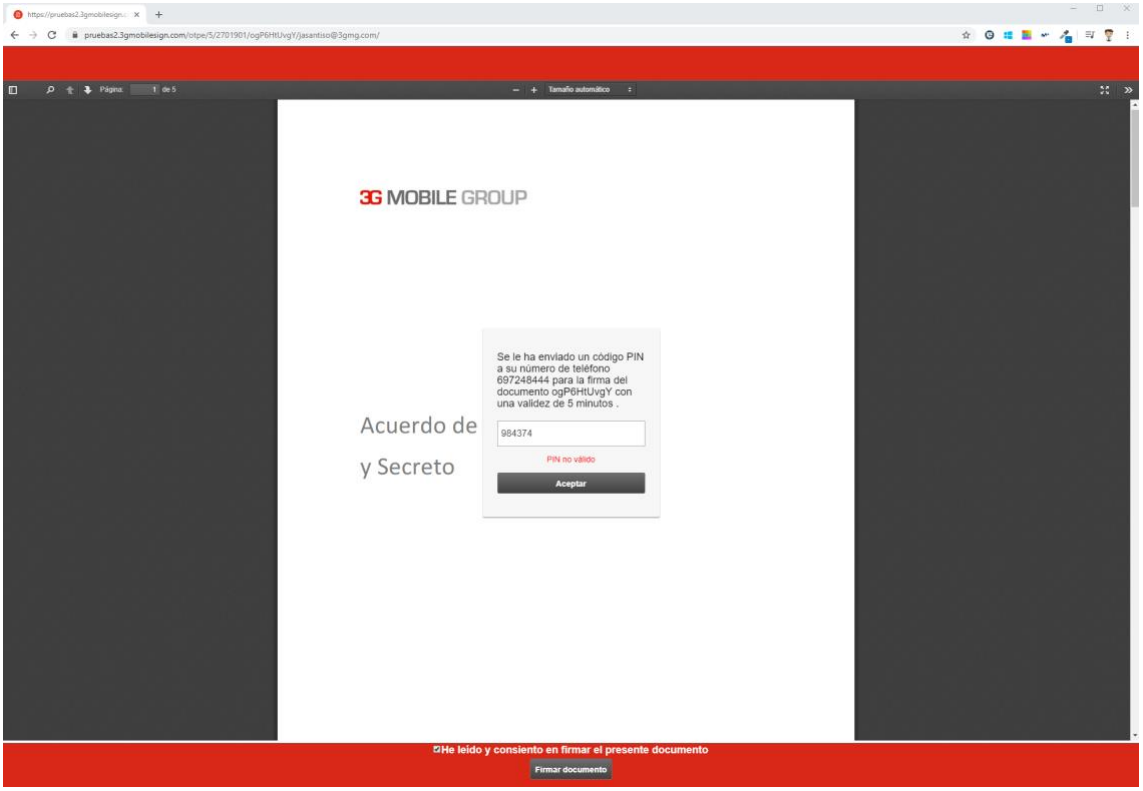
En la siguiente pantalla, se muestra que se puede volver a solicitar el OTP en caso de haberlo perdido, olvidado o no recibido. Se comunica que el OTP recibido será válido durante 5 minutos.



Evidencia 5: solicitud de nuevo envío de PIN para el mismo id de documento.

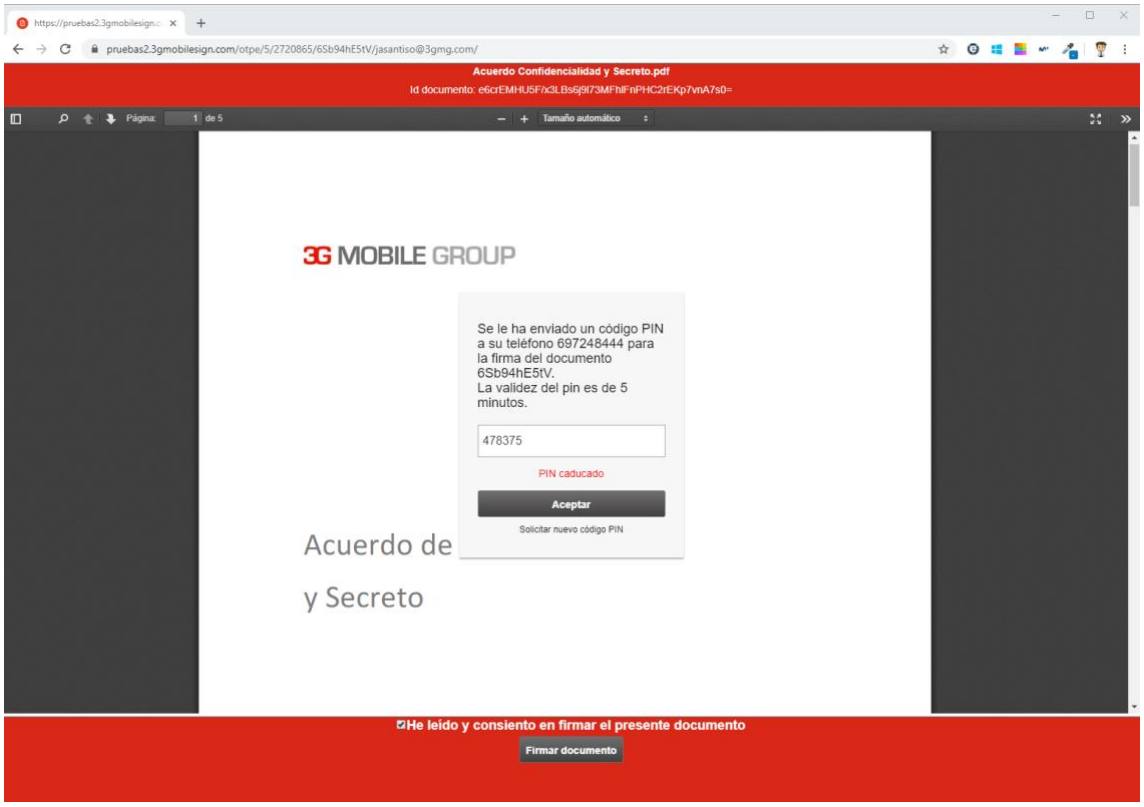
Evidencia 6: SMS con el nuevo de PIN solicitado para el mismo id de documento.

En caso de que el PIN introducido fuera erróneo, la plataforma lo rechaza y lo comunica al usuario que dicho pin SMS no es válido.



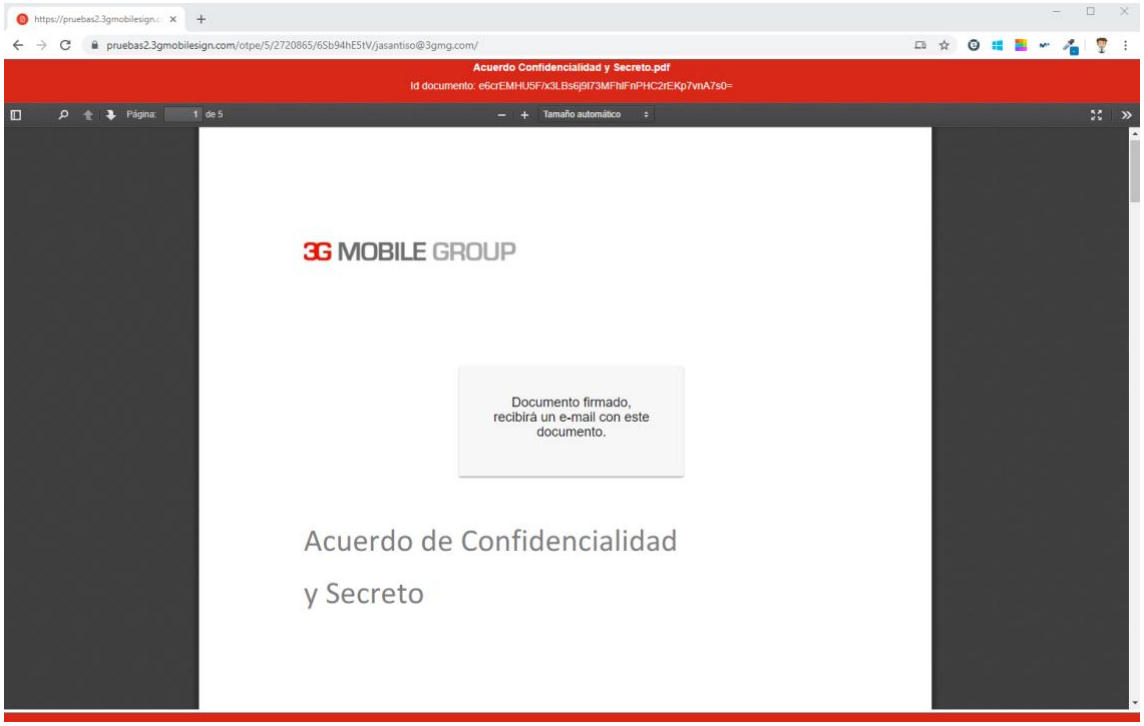
Evidencia 6: comunicación de PIN no válido

En caso de que el PIN introducido fuera del periodo de validez, la plataforma lo rechaza y lo comunica al usuario que dicho pin SMS no es válido.

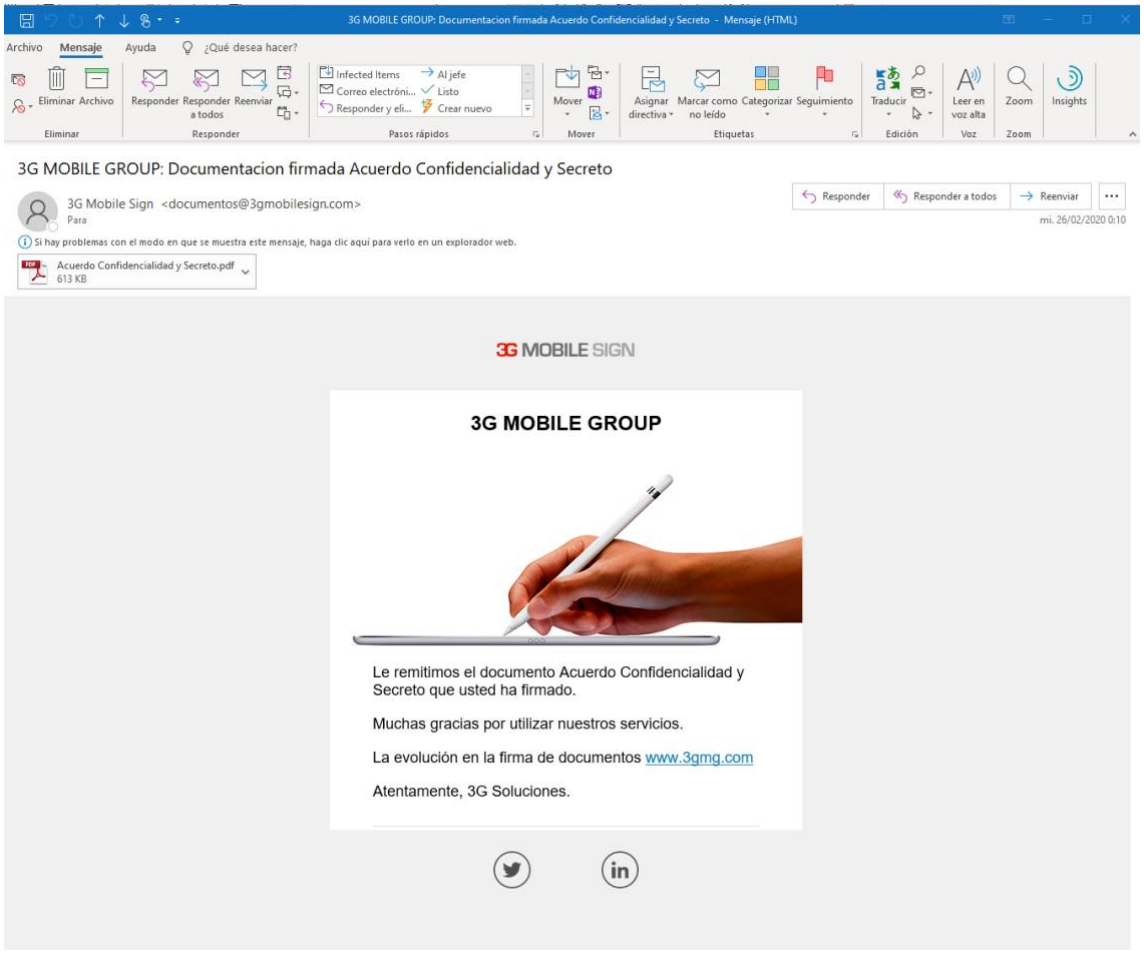


Evidencia 7: comunicación de PIN caducado

Una vez se ha firmado el documento, si así se configura por el cliente de 3G, la plataforma comunica que ha sido firmado correctamente, y el firmante recibirá un correo electrónico con dicho documento firmado.



Evidencia 8: notificación de documento firmado con éxito



Evidencia 9: correo electrónico de remisión del documento firmado

El método utilizado para generar los códigos aleatoriamente, y que son remitidos al firmante, permite garantizar un nivel de pseudo-aleatoriedad suficientemente seguros, conforme a los criterios establecidos en la norma RFC 4086, puesto que el proceso de generación de claves de 3G se realiza mediante el software CryptGenRandom de .NET.

El código de identificación generado es configurable. El administrador del sistema puede decidir tanto la longitud como el número de caracteres, siendo el mínimo 6 dígitos. Efectivamente, el equipo auditor de ECIJA confirma que, para que sea considerado seguro, el código de identificación debe tener una longitud al menos de 6 dígitos, que es el mínimo recomendado por la RFC 6238, que establece un mínimo de 32 bits.

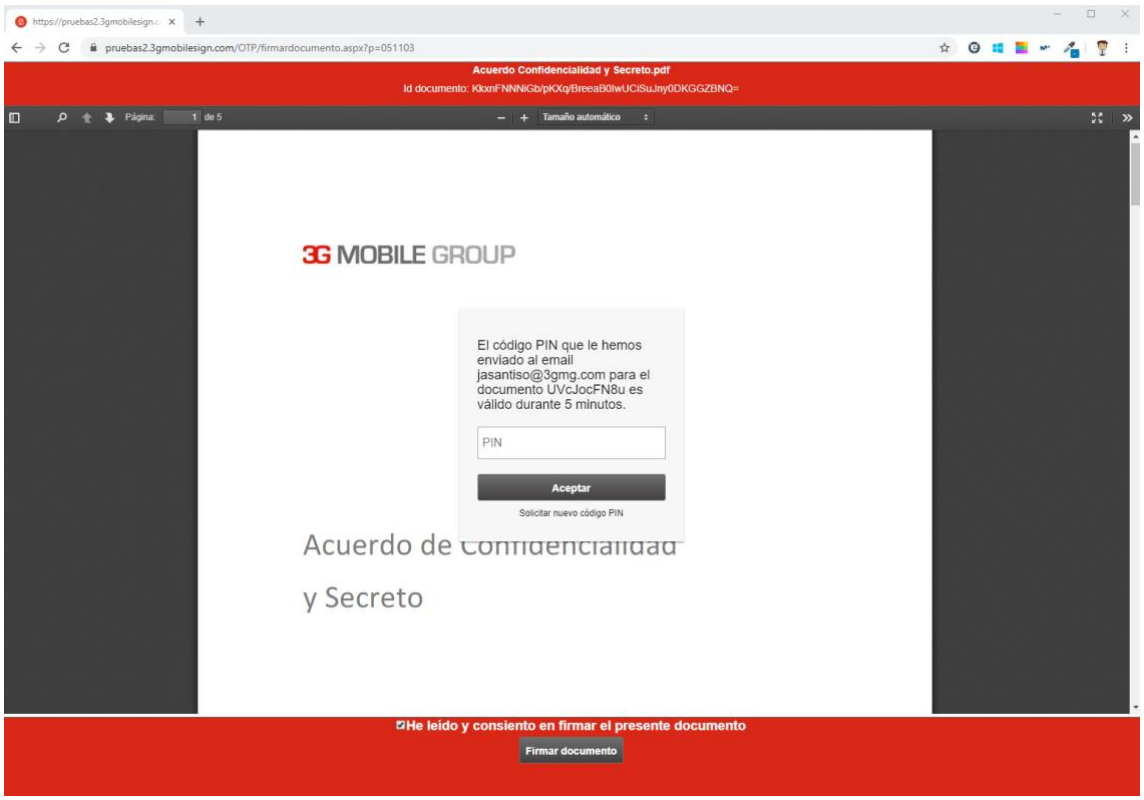
5.2 COMUNICACIÓN Y OTP VÍA EMAIL.

Al igual que en el sistema analizado anteriormente, la plataforma permite la remisión de los códigos OTP al email facilitado por el firmante, siendo la única diferencia del proceso el medio utilizado para remitir dicho código OTP.

El firmante recibe un correo electrónico donde se notifica que existe un documento pendiente de firma, así como el link de acceso al mismo.

Pueden definirse los mismos tres métodos de identificación antes de acceder al documento que en el punto 5.1.

En el momento de la solicitud del pin, se le muestra un mensaje al firmante donde se le informa de que el pin se le enviara por mail a una dirección de correo electrónico.



Evidencia 10: mensaje de envío del PIN OTP a través de correo electrónico

El proceso de generación de claves, CryptGenRandom de .NET, la longitud de las claves, y los tiempos de caducidad de las mismas son idénticos que el proceso anterior.

También puede volver a solicitarse una nueva clave si se ha perdido o caducado, generándose al igual que en el proceso anterior, una nueva clave diferente a la original.

5.3 COMUNICACIÓN Y OTP VÍA SMS TELÉFONO MÓVIL.

Al igual que en el sistema analizado en el punto 5.1, la plataforma permite la remisión tanto de la comunicación con la URL como de la clave OTP por SMS al número de teléfono móvil facilitado por el firmante.

El firmante recibe un SMS donde se notifica que existe un documento pendiente de firma, así como el link de acceso al mismo.

Evidencia 11: mensaje de envío del acceso al documento a través de SMS al teléfono móvil

Pueden definirse los mismos tres métodos de identificación antes de acceder al documento que en el punto 5.1.

En el momento de la solicitud del pin, se le muestra un mensaje al firmante donde se le informa de que el pin se le enviara por SMS a su número de teléfono móvil, al igual que en los casos anteriores.

El proceso de generación de claves, CryptGenRandom de .NET, la longitud de las claves, y los tiempos de caducidad de las mismas son idénticos que en los procesos anteriores.

También puede volver a solicitarse una nueva clave si se ha perdido o caducado, generándose una nueva clave diferente a la original, del mismo modo que en los procesos analizados en los puntos 5.1 y 5,2.

6 COMUNICACIÓN ENTRE EL FIRMANTE Y EL SISTEMA.

La plataforma envía al firmante el PIN de firma a través de un canal diferente al que será utilizado para la firma, y con comunicación diferente a la que contiene el documento a firmar, tal y como se puede comprobar en las Evidencias 1, 2 y 3 de este informe, de modo que pueda acreditarse y justificarse la utilización de un doble factor de autenticación que aporte mayores garantías a la transacción y firma. Por lo tanto, en este caso, el canal utilizado es diferente al canal por el que se relaciona el servidor y el cliente.

No obstante, puede configurarse la plataforma de 3G para que el OTP se envíe por mail o la comunicación por SMS, por lo que, en ambos casos, tanto el PIN de la firma como la recepción del enlace al documento se realizan a través del mismo canal, como se ha podido evidenciar anteriormente (*Evidencias 10 y 11*).

Todas las comunicaciones entre el firmante y el sistema se realizan bajo protocolo seguro: Protocolo de comunicación SSL, de 2048 bits.

Puesto que la plataforma envía el OTP al email o por SMS, el firmante puede visionar dicho código de forma permanente. Pero la plataforma se configura para que dicho código tenga

una validez durante un tiempo. La vigencia del pin para ser introducido en la plataforma de 3G es configurable, teniendo en todo caso un periodo de vigencia máxima de 10 minutos. Ello cumple con la validez recomendable por el estándar RFC 6238, que establece que la vigencia del pin debe ser como máximo de 10 minutos.

Los códigos se generan aleatoriamente, siendo almacenados inmediatamente y manteniéndose seguro durante su ciclo de vigencia.

7 CONFIRMACIÓN DE LA TRANSACCIÓN E INTEGRIDAD DE LA MISMA.

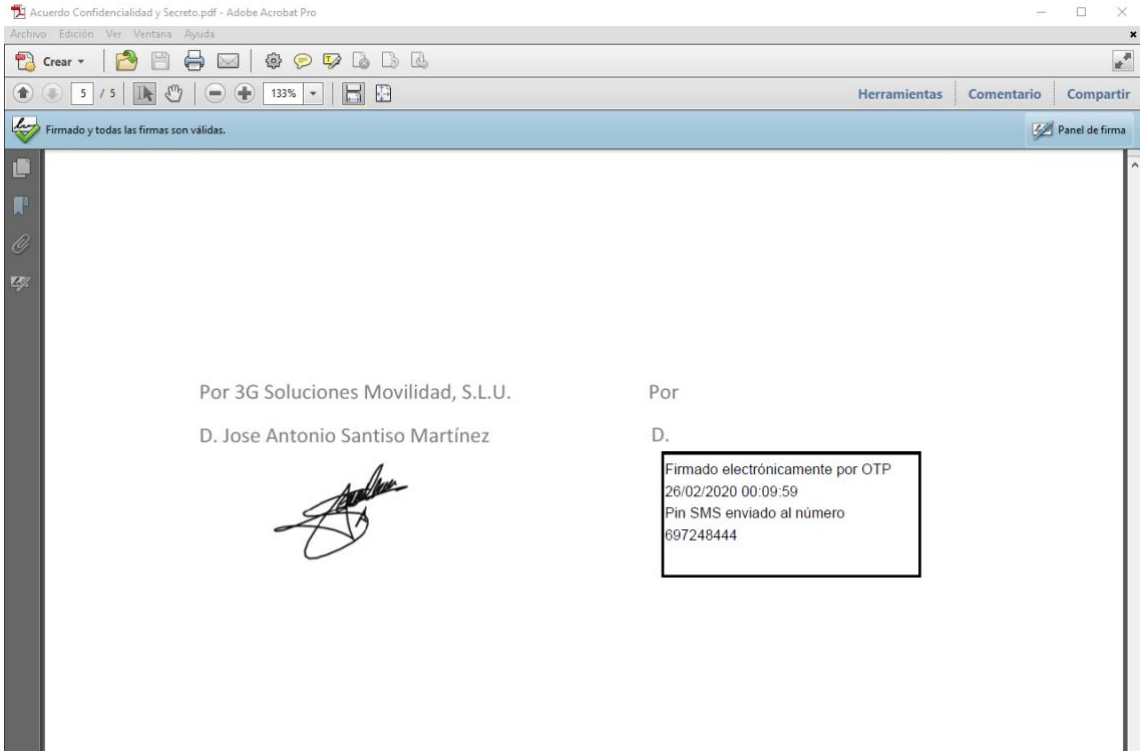
La seguridad de los sistemas depende de generar una password suficientemente seguras, claves criptográficas y similares; en definitiva, algoritmos criptográficos sólidos que frustren los intentos de análisis de patrones.

El algoritmo empleado para generar el código de seguridad empleado por el sistema OTP debe permitir garantizar un grado de pseudoaleatoridad suficientemente seguro, entendiéndose, de conformidad con el estándar ETSI TS 102 176-1 en el que se indican como métodos adecuados, los siguientes: ANSI X9.17, AIS 20, FIPS 186 generator o RSA DRNG, o Blum-Blum-Shub DRNG. Igualmente, según la RFC 4086 la recomendación de Microsoft a los usuarios del sistema operativo Windows es utilizar la llamada de generación de números pseudo-aleatorios CryptGenRandom con el proveedor de servicios criptográficos de CryptAPI.

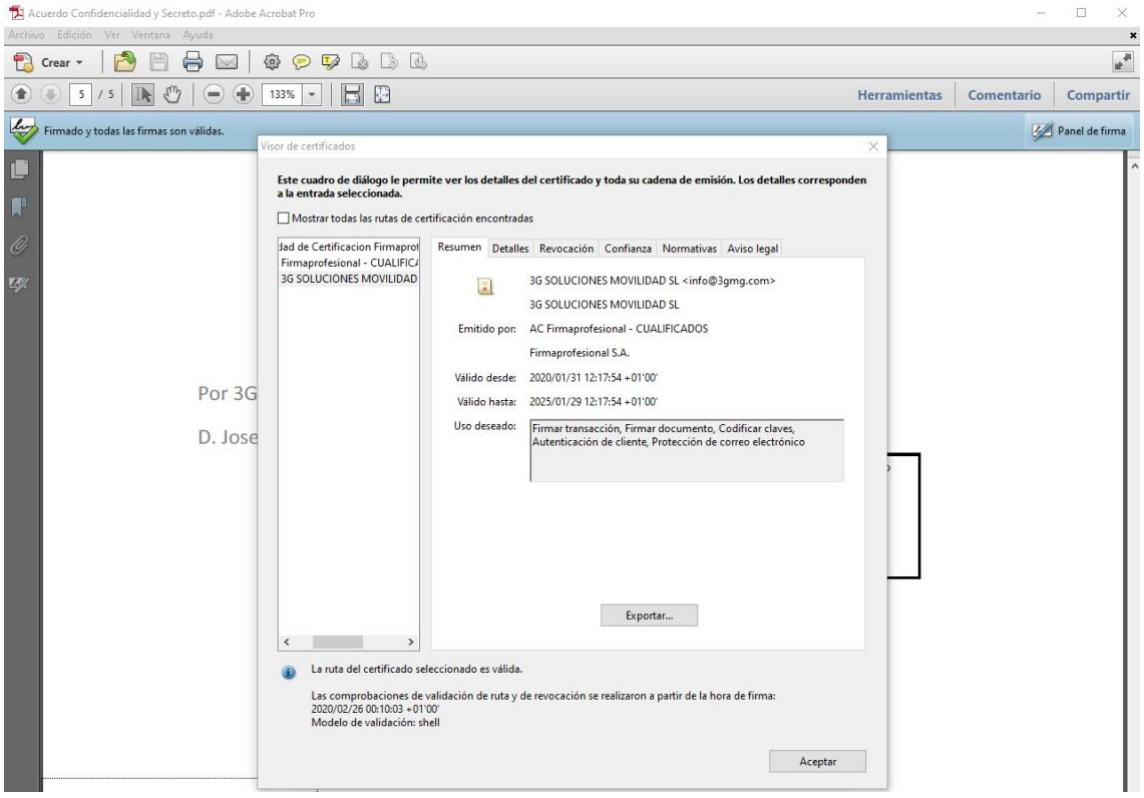
Como se ha comprobado por el equipo auditor, el código generado por la plataforma de 3G tiene una longitud mínima de 6 dígitos, de conformidad con las normas y recomendaciones de aplicación, que establecen que el código de identificación generado debe tener una longitud de, al menos, 32 bits y 6 dígitos, y esta generado con la fuente de aleatoriedad propuesta por Microsoft.

Por ello, la plataforma 3G garantiza que, una vez utilizado o en su caso, caducado el código que se ha generado aleatoriamente, no podrá ser reutilizado en otra transacción realizada a través del sistema, ya que, según se ha constatado a través de la información aportada por la entidad, el código no es reutilizable.

La firma generada con OTP si está visible, y se puede observar que el documento ha sido firmado. En el caso de la firma en la plataforma de 3G, el documento firmado, una vez incrustados los metadatos, se firma electrónicamente con un certificado de firma o de sello electrónico cualificado del cliente que contrata la plataforma de 3G. Se calcula el hash y se almacena el hash del documento final firmado con SHA2. Al firmar el documento final con un certificado electrónico cualificado, e incluir un sello de tiempo cualificado, la plataforma de 3G garantiza la integridad del documento firmado y el no repudio de la firma.



Evidencia 12: widget de firma por OTP

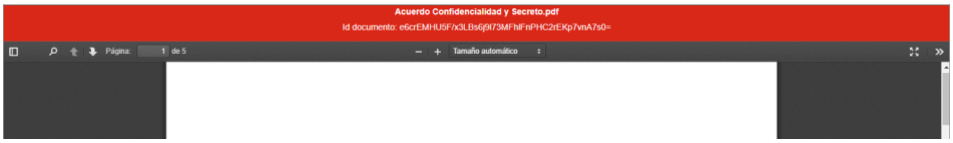


Evidencia 11: sellado electrónico del documento con certificado cualificado

El certificado electrónico garantiza la integridad del documento y los metadatos asociados al mismo, como son:

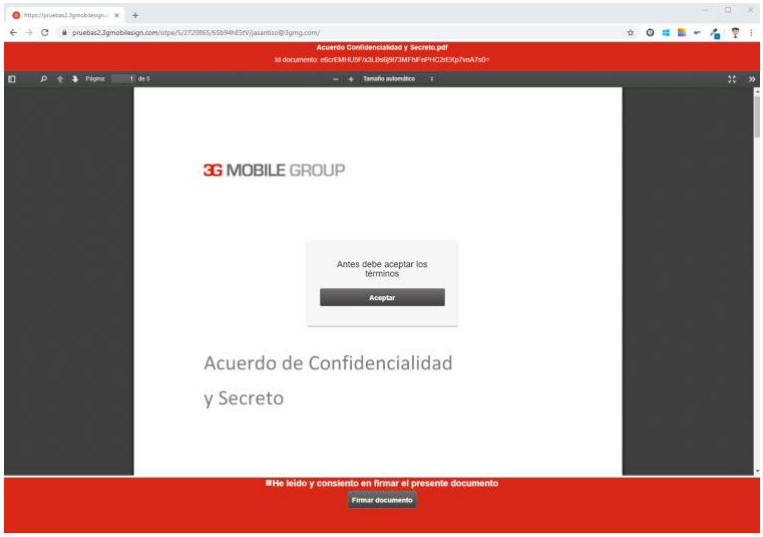
- Dirección de correo electrónico (salvo en el proceso descrito en el punto 5.3)
- Teléfono (salvo en el proceso descrito en el punto 5.2)
- PIN
- Orden de firma
- Código de empresa
- ID del documento
- Modelo y versión del navegador
- IP de conexión
- ID del firmante
- Geolocalización del firmante, en caso de tenerlo habilitado
- Imagen del momento de la firma con el HASH del documento

Esta imagen se realiza en el momento de finalizar el proceso de firma, y contiene el HASH calculado en tiempo real, que puede cotejarse con el HASH del documento original que entro en la plataforma, y se almacena cifrado como evidencia del contenido del documento que se le está mostrando y ve el firmante.



Evidencia 12: imposibilidad de generar la clave OTP sin aceptar la casilla de consentimiento

El consentimiento de firma por parte del interesado se evidencia mediante la utilización del OTP enviado por la plataforma, de forma inmediata a la recepción de la misma. Se requiere por ello, una acción por parte del firmante. Adicionalmente, la plataforma de firma de 3G utiliza un texto con una casilla que no está marcada previamente donde se dice: "He leído y consiento en firmar el presente documento", que el firmante debe clicar antes de firmar y enviar el documento firmado.



Evidencia 13: imposibilidad de generar la clave OTP sin aceptar la casilla de consentimiento

Conforme a la normativa vigente de protección de datos de carácter personal, el firmante deberá ser informado por parte del Cliente de 3G (Responsable de los datos) del tratamiento de sus datos personales incluyendo al menos:

- Datos del Responsable del tratamiento y DPO en su caso.
- Finalidad del tratamiento de los datos biométricos.
- Plazo de conservación de estos.
- Derechos del interesado.
- Posibilidad de reclamar ante la AEPD.

8 FIRMA CON OTP CATEGORIZADA COMO FIRMA 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.

La utilización de sistemas mixtos que permitan la identificación a través de medios como el teléfono y/o el correo electrónico, reforzado con el envío de un OTP, con una vigencia limitada, podría llegar a considerarse un sistema de identificación avanzado según eIDAS.

Por este método de identificación se están combinando dos factores de autenticación: por un lado, un factor basado en la posesión, donde la persona debe demostrar la posesión de un número de teléfono, una cuenta de correo electrónico, y por otro lado, otro factor basado en el conocimiento (el OTP recibido).

El sistema de autenticación mediante OTP es un sistema de autenticación dinámica, que proporciona un medio de crear a petición del cliente, una prueba electrónica que demuestra que el cliente posee los datos de autenticación y que cambia con cada autenticación entre el cliente y el servidor que verifica su identidad.

El sistema deberá, previamente a la utilización del mismo, recopilar los datos de identidad pertinentes necesarios para la prueba y verificación de la identidad.

Se considera más seguro la entrega del OTP al firmante por un canal alternativo a la conexión web, mediante el cual se puede suponer que solo se entrega a la persona a la que pertenece.

El algoritmo OTP no encripta la información, por lo que no prevé la privacidad en la transmisión de los datos. Por ello, es importante utilizar otros mecanismos para garantizar la confidencialidad de la información que viaja a través de redes de telecomunicaciones. Se recomienda la utilización de certificados electrónico para el cifrado de las comunicaciones (Certificado de Servidor Seguro SSL o certificado de autenticación web), emitido por un Prestador de Servicios de Certificación Cualificado.

Para que una firma realizada con OTP pueda llegar a considerarse avanzada, deberá ser utilizada junto a otros sistemas que aporten las evidencias necesarias para que eleven su nivel de seguridad. Dichas evidencias serán:

- Utilización de certificados digitales que cifren el documento y detecten cualquier cambio ulterior de los datos firmados con OTP. Si el certificado utilizado es un certificado cualificado, aún tendrá mayor nivel de seguridad y su prueba será más evidente. Por ello se recomienda el uso de certificados electrónicos de apoyo en la firma de documentos que puedan producir efectos jurídicos frente a terceros, para poder acreditar y evidenciar la firma realizada con OTP, así como la integridad del documento firmado.
- Utilización de sellos de tiempo cualificados para sellar las evidencias necesarias para verificación de la identidad antes del acto de firma, así como el consentimiento del interesado de realizar dicho acto de firma almacenando dichas evidencias en el sistema de información junto con la información presentada. La integridad y conservación de los documentos electrónicos almacenados y de sus metadatos asociados obligatorios quedará garantizada a través del sellado con el sello electrónico cualificado de la plataforma de 3G y del resto de medidas técnicas que aseguren su inalterabilidad.

Con ello, el sistema de firma con OTP, podrá ser considerada una firma electrónica avanzada si cumple con los requisitos expuestos anteriormente, dado que:

1) **Permite identificar al firmante**, en tanto se trata de una firma asociada directamente al titular de un número de teléfono y/o una dirección de correo electrónico.
2) **Permite detectar cualquier cambio ulterior de los datos firmados**, en tanto el documento firmado y el resultado de la firma con OTP pueden ser debidamente cifrados mediante un certificado cualificado de firma electrónica.
3) **Que se encuentre vinculada de manera única al firmante**, en tanto el factor de autenticación (el móvil o el email) como el OTP generado se encuentra directa y únicamente asociados a una persona concreta, siendo acreditado mediante prueba de perito informático 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 utilización del password de un solo uso recibido en su dispositivo.

Por todo ello, entendemos que la firma resultado del sistema cumpliendo los requisitos anteriormente expuestos 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 Civil1", según establece el art. 3.8 de la LFE.

1 *"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".

b) "No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación con 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.

c) Según el considerando 49 del Reglamento eIDAS, "El presente Reglamento debe establecer el principio de que no se deben denegar los efectos jurídicos de una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla todos los requisitos de la firma electrónica cualificada. Sin embargo, corresponde a las legislaciones nacionales determinar los efectos jurídicos de las firmas electrónicas en los Estados miembros, salvo para los requisitos establecidos en el presente Reglamento según los cuales una firma electrónica cualificada debe tener el efecto jurídico equivalente a una firma manuscrita." Y lo mismo se establece en su artículo 25 "Efectos jurídicos de las firmas electrónicas 1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada. "

9 CONCLUSIONES

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

1) La Firma electrónica tiene como finalidades:

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).

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

- Obtener garantías de que la firma 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 personales, 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 de OTP con un certificado cualificado que genere Firma electrónica cualificada o al menos con Firma electrónica avanzada.

3) 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 OTP analizado en el presente informe a través de:

- Obtención del código único generado para la firma con OTP, que es de 32 bits o 6 dígitos como mínimo y puesto a disposición del firmante por un plazo máximo de 10 minutos.
- Envío y comunicación de la firma con OTP obtenida y los metadatos de manera cifrada utilizando al efecto los correspondientes certificados electrónicos. 3G utiliza certificados de autenticación web para el cifrado de las comunicaciones.

4) El sistema de firma OTP de 3G cuenta con un servicio de sellado de tiempo.

En este caso, el documento se almacena con el OTP, 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. Se ha constatado que el sello de tiempo utilizado está emitido por un Prestador de Servicios de Confianza cualificado conforme a eIDAS.

5) La firma electrónica realizada mediante OTP por la plataforma de 3G, cumple con todos los requisitos descritos a lo largo del presente informe, por lo que queda englobada dentro del concepto de **firma electrónica avanzada** de conformidad con lo dispuesto en la Ley de Firma Electrónica.

6) El almacenamiento de los datos de Firma 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 Reglamento General de Protección de Datos (RGPD), cuestión que queda debidamente regulada en las condiciones de contratación previstas por 3G. El proveedor del servicio de almacenamiento será un Encargado del tratamiento, por lo que se incluirá en el contrato, la cláusula correspondiente.

7) La aportación en juicio de la Firma electrónica 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 por un perito informático especialista en seguridad.

8) Los datos personales deben tratarse de tal forma que se garantice su seguridad y confidencialidad adecuadas, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento. Por ello, se recomienda que se utilice el método de autenticación previa al acceso al documento.

9) La criptografía trabaja mediante el uso de certificados digitales y varios algoritmos de cifrado garantizando la confidencialidad, el cifrado de los datos y la vinculación única de los datos en el documento. Por lo tanto, demuestra de manera fiable que los códigos generados no han podido ser manipulados ni reutilizados.

10) La garantía de eficacia, para los fines señalados, dependerá de la fortaleza de las metodologías y algoritmos de obtención y análisis, 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).

10 RECOMENDACIONES

Como se ha analizado, el sistema de firma mediante OTP de 3G alcanza el nivel de seguridad suficiente como para poder ser considerada "firma avanzada". No obstante, podrán tenerse en cuenta las siguientes recomendaciones:

1) Se recomienda la entrega del OTP al firmante por un canal alternativo al que será utilizado para la firma, y con comunicación diferente a la que contiene el documento a firmar, por lo que recomendamos utilizar el método descrito en el punto 5.1 en detrimento del 5.2 y 5.3.
2) El PIN recibido será válido como máximo durante 10 minutos, La validez recomendable por el estándar RFC 6238 supone que establece que la vigencia del pin debe ser como máximo de 10 minutos, y siendo el escenario ideal 30 segundos después de ser recibido en el teléfono. Esto se justifica en la medida en que el mayor riesgo de este tipo de sistemas se encuentra en el plazo de tiempo existente para lograr poner en entredicho la seguridad de las claves generadas por el sistema.
3) El servidor de validación deberá validar el valor calculado por el cliente OTP. Si el valor recibido por el servidor no coincide con el valor calculado por el cliente, el servidor deberá iniciar un protocolo de resincronización antes de que solicite otro. Si la resincronización falla, el servidor debe pedir otro protocolo de autentificación a realizar, hasta que se alcance el número máximo de intentos autorizados. Cuando se alcance éste, el servidor deberá bloquear la cuenta e iniciar un procedimiento para informar al usuario.
4) La plataforma 3G deberá garantizar que, una vez utilizado o en su caso, caducado el código que se ha generado aleatoriamente, no podrá ser reutilizado en otra transacción realizada a través del sistema.
5) Se recomienda la utilización de certificados de sello electrónico cualificado, emitido por un Prestador de Servicios de Confianza Cualificado, para la firma de la documentación firmada y el cifrado de los metadatos por parte de la plataforma.
6) Se recomienda la utilización de Sellado de Tiempo Cualificado emitido por un Prestador de Servicios de Confianza Cualificado conforme a eIDAS. En la actualidad, la plataforma de 3G utiliza sellos de tiempo cualificados emitidos por un Prestador de Servicios de Confianza Cualificado.
7) Se recomienda la comprobación periódica de que los certificados utilizados (tanto el de sello electrónico instalado por el cliente como el de sello de tiempo de la plataforma) continúan siendo cualificados.
8) Por ser 3G encargado del tratamiento de los datos de sus clientes, se recomienda que se informe al Cliente que contrata con 3G que, conforme a la normativa vigente de protección de datos de carácter personal, el firmante deberá ser informado del tratamiento de sus datos personales incluyendo al menos:
    - Datos del Responsable del tratamiento y DPO en su caso
    - Finalidad del tratamiento de los datos biométricos
    - Plazo de conservación de los mismos
    - Derechos del interesado
    - Posibilidad de reclamar ante la AEPD.

9) Aunque la identificación inicial del firmante no es objeto del presente informe, se recomienda que dicha identificación inicial sea lo suficientemente robusta para poder garantizar que la persona que firma es quien dice ser, por lo que es recomendable que, al acceder a la plataforma y previo a la consulta del documento, se autentique al firmante por medio de un dato conocido por él y que no esté contenido en la propia comunicación, en lugar de acceder directamente al documento desde la URL.