EIDAS y E-Signature: una perspectiva jurídica

Firmas electrónicas en la Unión Europea

Este trabajo es una colaboración entre Lorna Brazell del despacho jurídico Osborne Clarke LLP y eSignLive de VASCO. En la primera parte, Osborne Clarke proporciona una opinión sobre la validez jurídica de la firma electrónica en la Unión Europea. La segunda parte ha sido preparada por eSignLive y resume las recomendaciones de mejores prácticas para el cumplimiento legal al implementar las firmas electrónicas.

Parte 1

INTRODUCCIÓN

El 1 de julio de 2016 entrará en vigor en el conjunto de la Unión Europea ("UE") el Reglamento de 2014 sobre la identificación electrónica y los servicios fiduciarios para las transacciones electrónicas en el mercado interior[1] ("eIDAS"), que sustituye a la Directiva de 1999 sobre firmas electrónicas[2] ("la Directiva"). Aunque la Directiva no había sido objeto de ninguna controversia en sus 16 años de historia, tampoco había sido un éxito. Su objetivo, que permitía el uso generalizado de las firmas electrónicas para llevar a cabo actividades transfronterizas dentro de la UE, no se cumplió.

Hay tres razones principales para esto:

I. La mayoría de las legislaciones de los Estados miembros de la UE no especifican ninguna forma de firma para contratos comerciales distintos de las garantías o contratos de adjudicación de bienes inmuebles.

II. Muchas personas creen erróneamente que la Directiva ordena el uso de firmas electrónicas avanzadas apoyadas por un certificado cualificado, es decir las firmas electrónicas cualificadas, para que una firma electrónica sea legalmente efectiva. De hecho, la Directiva dice lo contrario: los tribunales pueden aceptar cualquier forma de firma electrónica que tenga efectos jurídicos. La distinción es que en el caso de una firma electrónica cualificada, el tribunal no tiene otra opción que aceptarla. Sin embargo, el costo y la carga administrativa de implementar la tecnología requerida para firmas electrónicas cualificadas ha superado los beneficios potenciales por su dificultad de utilización.

III. La divergencia existente entre los Estados miembros en cuanto al régimen regulador con el que deben cumplir los proveedores de la firma o de la certificación. Como resultado, las firmas producidas con servicios de certificación aprobados en un Estado miembro corren el riesgo de no ser reconocidas como conformes en otro.

Dado que los mecanismos de la Directiva han sido tan poco utilizados, no es de extrañar que no exista una jurisprudencia europea que ofrezca orientación sobre cómo debe interpretarse.

Las deficiencias de la Directiva no han frenado el desarrollo del comercio transfronterizo en la UE. En 2015, el Tribunal de Justicia de la Unión Europea ("CJEU") dictaminó que los términos de un acuerdo B2B " click-wrap " pueden ser jurídicamente vinculantes incluso si el usuario no ha leído los términos del acuerdo. En ese caso El Madjoub, un concesionario de automóviles, intentó hacer valer un contrato on line para la compra de un coche usado, a través de una denuncia en un tribunal alemán local, pero perdió porque había hecho clic para indicar su aceptación de términos que no había leído. Esos términos incluyeron la sumisión a la jurisdicción de los tribunales belgas. El TJUE consideró que estaba obligado por los términos a pesar de no haberlos leído, porque había tenido la oportunidad de leerlos y hacer clic en su acuerdo. Por consiguiente, la forma más simple de firma electrónica imaginable -utilizando un cursor para hacer clic en un botón- puede tener efecto legal y la mayoría de las transacciones B2B o B2C pueden ser completadas sin firmas equivalentes a una firma manuscrita, siempre y cuando haya pruebas satisfactorias, de una forma u otra, para probar que cada parte había aceptado su compromiso.

Sin embargo, la Comisión Europea llegó a la conclusión de que la falta de armonización entre los Estados miembros sigue representando un posible obstáculo para el mercado interior. Por consiguiente, al introducir el Reglamento eIDAS y no dejar a los Estados miembros ninguna posibilidad para su aplicación o interpretación, esperan conseguir que los documentos firmados electrónicamente ahora se acepten en cada uno de los 28 Estados miembros de la UE, independientemente de los enfoques jurídicos o reglamentarios nacionales.

PUNTOS CLAVE DEL REGLAMENTO EIDAS

EIDAS tiene un alcance mucho más amplio que la Directiva, ya que además de las firmas también abarca la identificación electrónica, la entrega, los servicios de archivo y la autenticación de sitios web.

Firmas

EIDAS define las mismas tres categorías de firmas electrónicas que la Directiva. Existen:

- Firmas electrónicas
- Firmas electrónicas avanzadas ("AES")
- Firmas electrónicas cualificadas ("QES")

El enfoque de los tres es explícitamente neutro desde el punto de vista tecnológico. El Reglamento no estipula que se debe utilizar ninguna tecnología específica, sino sólo los criterios que debe cumplir una firma. Sin embargo, los requisitos para certificados cualificados sugieren que la tecnología de certificados digitales es la más adecuada.

1 Reglamento (UE) Nº 910/2014

2 Directiva 1999/93/CE

3 En este contexto, un certificado es una garantía de un tercero de que la identidad del titular de la firma ha sido debidamente verificada

Bajo eIDAS, una firma electrónica incluye cualquier dato en forma electrónica que se adjunta o está lógicamente asociado con otros datos en forma electrónica y que es utilizado por el firmante para firmar. Además, no puede denegarse la admisibilidad de la firma electrónica ni de la prueba ni del efecto jurídico por el mero hecho de que esté en forma electrónica o no cumpla los requisitos para firmas electrónicas cualificadas.

En consecuencia, para una amplia gama de casos de uso, como el acuerdo de compra de automóviles en línea en la decisión del TJUE anterior, las firmas electrónicas que no están avanzadas ni cualificadas pueden ser legalmente efectivas, siempre que la evidencia disponible establezca:

I. Que están adscritos al documento firmado, o están lógicamente asociados con él.

II. Que el firmante pretendía utilizar la firma electrónica para firmar - es decir, identificarse e indicar la aceptación, aprobación o simplemente aviso del contenido del documento.

De ello se desprende que las firmas avanzadas AES también son capaces de dar efectividad legal como firmas, ya que por definición una firma AES captura gran parte de la evidencia necesaria. Una firma AES debe ser:

I. Únicamente vinculado al firmante.

II. Capaz de identificarlo.

III. Creado con datos de creación de firmas electrónicas que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.

IV. Vinculado a los datos firmados de tal manera que cualquier cambio posterior en los datos es detectable.

Esto no quiere decir que las preguntas probatorias no puedan ser contestadas por otros medios - cuando un nombre se mecanografía al final de un documento, y se guarda en un ordenador mantenido en un entorno de empresa, las pruebas circunstanciales de las personas que tenían acceso a ese ordenador pueden ser suficientes para establecer que la persona que mecanografió el nombre era de hecho la persona nombrada. Sin embargo, una firma AES requiere una tecnología que no estaría disponible para un compañero de trabajo de al lado que maliciosamente intentó firmar el nombre de un colega y, por lo tanto, reduce la posibilidad de que esa posibilidad se pueda montar, y mucho menos con éxito. (La definición no intenta circunscribir qué tecnología podría ser.)

Las firmas QES se basan en las firmas AES que deben cumplir con estos requisitos adicionales:

- Ser creado utilizando un dispositivo de creación QES.
- Ser apoyado por un certificado cualificado.

> Bajo eIDAS, cualquiera de las tres categorías de firma electrónica puede ser legalmente efectiva; la diferencia entre ellos es sólo la evidencia que tomará para asegurar a un tribunal que la firma es genuina e intencionalmente aplicada al documento en particular.

Los dispositivos de creación de firmas QES son en gran parte iguales a los dispositivos seguros de creación de firmas de la Directiva, con un requisito adicional de que la confidencialidad de los datos de creación de firma electrónica está razonablemente asegurada. Del mismo modo, la definición de certificado cualificado se ajusta en gran medida a la definición equivalente de la Directiva.

La disposición de eIDAS y de la Directiva que las firmas electrónicas cualificadas deben ser reconocidas como legalmente equivalentes a las firmas manuscritas, sin recurrir a pruebas adicionales, puede considerarse simplemente como una confirmación de que las pruebas obtenidas mediante una firma electrónica avanzada con alguna forma de verificación de la identidad y ciberseguridad apropiada, debe ser aceptada como evidencia suficiente. (Esto no implica, sin embargo, que la firma QES no pueda ser impugnada, al igual que las firmas manuscritas pueden ser si la evidencia demuestra que el dispositivo de la creación había sido robado, o algún tipo de fraude era utilizado para engañar al firmante en la firma de un documento).

En particular, considerando el artículo 51 de eIDAS establece expresamente que un firmante debe poder confiar a terceros los dispositivos de creación de la firma QES, siempre que se apliquen los mecanismos y procedimientos adecuados para garantizar que el firmante tiene el control exclusivo sobre el uso de los datos. En otras palabras, la autoridad de firma puede ser delegada siempre y cuando se establezcan controles y equilibrios organizativos adecuados. Considerando el artículo 52 reconoce la posibilidad de la prestación de la firma electrónica remota (como los servicios basados en la nube), con sujeción a procedimientos adecuados de gestión y de seguridad administrativa, sistemas y productos fiables, para garantizar que el firmante tenga el control exclusivo.

Identidades electrónicas

eIDAS aborda cuestiones de identidades electrónicas ("eIDs"), pero lo hace sólo en el contexto limitado de eIDs utilizados para las interacciones de los ciudadanos con la administración pública como el acceso a la asistencia sanitaria o el pago de impuestos. No se exige ningún sistema de eIDs, ya que no todos los Estados miembros disponen de una tarjeta de identificación nacional. Más

Requisitos de eIDAS

Firmas electrónicas	Firmas Electrónicas Avanzadas (AES)	Firmas Electrónicas Cualificadas (QES)
La firma electrónica debe ser: · Aplicada por la persona asociada con la firma. · Aplicado de una manera que demuestre la intención del firmante. · Asociado con el documento o datos que el firmante pretendía firmar.	**Esta forma de firma electrónica añade cuatro requisitos adicionales. La firma electrónica avanzada debe:** · Estar unida exclusivamente al firmante. · Identificar al firmante. · Estar bajo el control exclusivo del firmante. · Detectar cambios en el documento o en los datos después de la aplicación del AES.	**Esta es una firma electrónica avanzada que, además, debe ser:** · Creado utilizando un dispositivo de creación QES. · Apoyado por un certificado cualificado (que se entrega al firmante en una forma que él o ella puede mantener bajo su control).
← Se necesitan pruebas de apoyo adicionales	⚖	No se requieren pruebas de apoyo adicionales →

bien, para los Estados miembros que desean que sus eIDs se reconozcan a través de las fronteras, eIDAS pretende garantizar el reconocimiento mutuo de los sistemas existentes de eID. Para ello, define diferentes niveles de garantía de identidad y obliga a cada Estado miembro a aceptar eIDs emitidos por otro Estado miembro, siempre que el eID cumpla con el nivel de garantía de identidad requerido para su acceso a servicios. Este enfoque podría caracterizarse como una habilitación más que una imposición de armonización; es probable que transcurra unos años antes de que la mayoría de los Estados miembros acepten las eIDs emitidas en el extranjero como prueba del derecho a acceder a sus servicios públicos.

Al igual que la Directiva, eIDAS no afecta a la validez de los acuerdos de firma existentes dentro de sistemas cerrados, y no hace mención a la cuestión de la administración pública. Varios Estados miembros han elaborado comunicaciones electrónicas con organismos públicos a partir de su legislación general de aplicación de la Directiva, pero ya no será posible. Así, incluso en los Estados miembros que no cuentan con sistemas de eID, será posible firmar documentos oficiales electrónicamente.

El Reglamento ha sido incluido en los estatutos durante dos años antes de su fecha de vigencia en julio de 2016 para dejar tiempo para varios trabajos preparatorios que deben realizarse. En particular, la Comisión Europea tuvo la tarea de preparar especificaciones técnicas, normas y procedimientos para garantizar que el reconocimiento mutuo sea efectivo tanto en la práctica como en la legislación. La lista de esquemas de eID que aceptan reconocimiento mutuo sólo se publicará un año después de la preparación de dichos materiales, que aún no están completos. Por lo tanto, deberá transcurrir más tiempo antes de que las disposiciones pertinentes de eIDAS entren en vigor.

El efecto jurídico de los diferentes tipos de firmas y su impacto en el tribunal

Bajo eIDAS, cualquiera de las tres categorías de firma electrónica puede ser legalmente efectiva; la diferencia entre ellas es sólo la evidencia que tomará para tranquilizar a un tribunal que la firma es genuina e intencionalmente aplicada al documento en particular.

- Una forma simple de firma electrónica, tal como un nombre mecanografiado o una copia en formato PDF de una firma manuscrita, es fácil de falsificar, por lo que es probable que un tribunal requiera pruebas adicionales sustanciales para demostrar que fue efectivamente aplicada por la persona nombrada en el documento firmado.
- Una firma AES es mucho más difícil de falsificar y más estrechamente asociado al documento firmado, por lo que la evidencia adicional de apoyo requerida será considerablemente menor.
- Una firma QES, por otro lado, no requiere evidencia adicional ya que por el Artículo 25 eIDAS el tribunal tiene el mandato de aceptar su equivalencia a una firma manuscrita. Por supuesto, puede ser necesario demostrar que la firma QES cumple efectivamente los requisitos de QES.

Con el fin de evaluar la conveniencia de cualquier forma de firma para su uso con un documento en particular, la primera pregunta es por qué se requiere la firma. Cuando las leyes no especifican una firma para darle efecto jurídico, es menos probable que los tribunales requieran formas elaboradas de firma. Las firmas electrónicas simples o firmas AES deberían ser aceptables en tales circunstancias.

Del mismo modo, cuando la firma indique la recepción de información como cuando existe un requisito obligatorio de notificar al cliente de ciertos hechos, una simple firma electrónica o firma AES debería ser suficiente.

Cuando la firma tenga efecto legal para obligar al firmante, se producirá un menor riesgo si se utiliza un modo más formal de firma - AES o QES -, ya que las formalidades de estas firmas

> Una firma electrónica no puede negarse a la admisibilidad como prueba o efecto jurídico por el mero hecho de que está en forma electrónica o no cumple los requisitos para firmas electrónicas cualificadas.

automáticamente captan gran parte de la evidencia necesaria para asegurar a un tribunal su autenticidad. Pero si las partes convienen entre ellas qué tipo de firma electrónica es apropiado utilizar, entonces esto se tendrá en cuenta en cualquier procedimiento judicial.

eIDAS no tiene ningún impacto en los requisitos legales nacionales respecto de los documentos que requieren firma manuscrita para darles efecto legal ya que se trata de una amplia variedad de leyes -las que rigen testamentos, transferencias de tierras, garantías, procesos electorales, etc. Sigue siendo necesario chequear los requisitos legales de cada país caso por caso para verificar si un documento requiere firma; y en caso afirmativo, con qué fin (aviso, efecto legal u otro).

Sin embargo, eIDAS anula las leyes nacionales sobre la admisibilidad de las pruebas sobre el punto específico de la admisibilidad de las firmas electrónicas. Sin perjuicio de las normas nacionales sobre las pruebas en todos los demás aspectos, en virtud del artículo 25, apartado 1, un tribunal no puede negar la admisibilidad de la prueba electrónica en los procedimientos judiciales únicamente por el hecho de que se encuentra en forma electrónica o no cumple los criterios de firma QES.

En consecuencia, eIDAS reconoce explícitamente que las formas de firma electrónica distintas de la firma QES deben tener efecto jurídico en circunstancias apropiadas y que los tribunales de un Estado miembro tienen la obligación de considerar las pruebas y circunstancias para llegar a una conclusión y no simplemente descartar la firma electrónica que no sea QES. Con el tiempo, las decisiones del TJUE comenzarán a establecer normas para la eficacia de las pruebas de las firmas electrónicas distintas de la QES.

REGULACIÓN DE SERVICIOS DE CONFIANZA

La proliferación de normas y sistemas nacionales dispares para la reglamentación y la supervisión de los proveedores de servicios de certificación fue una de las razones por las que la Directiva no fomentó el uso transfronterizo de firmas electrónicas, ya que los Estados miembros elaboraron requisitos muy divergentes para el sector. Por ejemplo, el Reino Unido decidió dejar la industria para regularse, mientras que Alemania e Italia introdujeron requisitos legales rígidos. En estas circunstancias, no es sorprendente que no se prevea que los certificados de un país se reconozcan en otro, y muy pocos proveedores ofrecen certificados transfronterizos en el sentido de certificados que respalden las firmas de entidades de cualquier nacionalidad distintas de la del proveedor de servicios sí mismo.

Este es, pues, un objetivo clave de eIDAS: permitir a los proveedores de servicios de confianza (TSP) de todo tipo ofrecer servicios transfronterizos, incluidos los proveedores de certificados que respalden las firmas electrónicas.

La Directiva se refería exclusivamente a las firmas electrónicas y los certificados de apoyo, y utilizaba así el término de proveedor de servicios de certificación. Esto es demasiado corto para eIDAS, que se refiere a una gama más amplia de servicios electrónicos, incluyendo servicios de validación y preservación de firmas, sellos (ordinarios y avanzados), sellos de tiempo, servicios de entrega y también autenticación de sitios web. Por lo tanto, se ha introducido el término colectivo TSP (Trust Service Providers).

Se considera necesario prescribir normas operativas legales y técnicas para todos los TSP, ya que ocupan una posición única en cualquier transacción en la que participen dos partes (consumidores, ciudadanos y empresas). No existe una figura jurídica exacta equivalente a una parte que, sin participar en la transacción como tal, es, no obstante, instrumental para permitir que se efectúe. El papel más cercano es el del notario que verifica y certifica la identidad de una parte contratante para el propósito de una transacción remota. Los notarios están regulados bajo sus normas profesionales.

Hay dos categorías de proveedores de servicios de confianza: ordinario (TSP) y cualificado ("QTSP"). Un QTSP es un TSP que proporciona uno o más servicios fiduciarios cualificados, tales como la creación, verificación y validación de firmas electrónicas cualificadas, y que es reconocido por un organismo de supervisión designado por un Estado miembro. Ambas categorías pueden proporcionar cualquier tipo de servicio de confianza.

Todos los proveedores de servicios de confianza (TSP) deben cumplir con los estándares de seguridad apropiados para prevenir y minimizar el impacto de cualquier incidente de seguridad e informar a las partes interesadas de los efectos adversos de cualquier incidente.[4] Cuando un incumplimiento de seguridad o una pérdida de datos cause un impacto significativo en el servicio de confianza o en los datos personales almacenados, los TSP deben notificar al órgano de supervisión dentro de las 24 horas de haber tomado conocimiento del incidente. Los clientes afectados también deben ser notificados, sin demora indebida.

Además de los requisitos de seguridad, eIDAS impone responsabilidad a los TSP por cualquier daño causado intencionalmente o por negligencia a cualquier persona a través del incumplimiento por parte del TSP de sus obligaciones.[5] En particular, esto no se limita a las partes en la transacción; podría ser por un tercero (una empresa matriz o filial, por ejemplo). El reclamante tiene la carga de probar que el daño fue causado por intención o negligencia, a menos que el TSP sea un QTSP, en cuyo caso se supone intención o negligencia. Por supuesto, un QTSP tiene el derecho de contrarrestar la presunción de intención o negligencia.

A diferencia del régimen de la Directiva, tanto los TSP «ordinarios» como los QTSP pueden limitar su responsabilidad a las partes que confían en la expedición de un certificado. En virtud de la Directiva, sólo los QTSP podían imponer tales límites. La responsabilidad se limita en la medida de cualquier limitación en el uso de sus servicios (que el TSP puede haber dado a sus clientes notificación previa de), siempre que esas limitaciones también sean reconocibles a terceros. Lo que puede ser necesario para que una limitación sea "reconocible" no está claro, pero la notificación en una forma fácilmente accesible es probable que sea efectiva.

Además de cumplir con los estándares de seguridad, los QTSP están sujetos a otros requisitos, incluyendo:

- Realizar auditorías periódicas;
- Aplicar procedimientos apropiados de conformidad con la legislación nacional a tareas tales como la verificación de identidades;
- Emplear personal adecuadamente cualificado y utilizar sistemas confiables tanto para procesar como almacenar datos;
- Mantener un seguro de responsabilidad civil;
- Mantener registros apropiados; y
- Mantener un plan de finalización actualizado para asegurar la continuidad del servicio si el QTSP se extingue.

La mayoría de estas son, por supuesto, buenas prácticas comerciales. Nada impide que un TSP cumpla con los requisitos y aplique los estándares aprobados para sistemas y productos confiables, sin solicitar el estatus de QTSP.

Un QTSP no necesita ser "cualificado" con respecto a todos los servicios de confianza que ofrece, y esto se hará evidente en la lista publicada y confiable. En consecuencia, un QTSP podría ser cualificado con el propósito de autenticación de sitios web, por ejemplo, sin estar cualificado para entrega electrónica o firmas electrónicas.

Las ventajas de adquirir el estatus de QTSP son esencialmente en torno a la comercialización. El hecho de ser supervisado por una agencia gubernamental y concedido ese estatus debe ayudar a persuadir a los clientes potenciales que sus servicios son, de hecho, de confianza. El hecho de ser un QTSP será público a través de la publicación de la lista de QTSPs confiable del Estado miembro en cuestión. El único derecho adicional disponible para los QTSP que no está abierto a los TSP es el uso de la nueva marca de confianza de la UE para servicios fiduciarios cualificados.

MEJORES PRÁCTICAS LEGALES

Como se mencionó anteriormente, las firmas electrónicas son perfectamente aceptables en muchos contextos sin que incluso sea necesario requerir las características técnicas de AES, y menos aún QES. En el contexto contractual, la firma no es más que una forma de evidencia de que los términos fueron acordados; otras pruebas (como una cadena de autorizaciones internas antes de la firma) pueden estar disponibles y pueden ser suficientes para asegurar que el acuerdo sea ejecutable.

Sin embargo, la mayoría de los Estados miembros tienen leyes nacionales que exigen la firma de determinadas categorías de documentos. Los contratos de crédito al consumo se encuentran entre los más comunes que requieren firma, junto con los contratos de venta de inmuebles y garantías. También hay requisitos legales de firma para muchos documentos corporativos y bancarios, categorías que no están en sí mismas armonizadas bajo la legislación de la UE y por lo tanto, varían de un país a otro. Como resultado, es necesario verificar para cada caso de uso propuesto si es necesario firmar un documento corporativo, bancario u otro tipo de documento bajo la ley aplicable.

Afortunadamente, eIDAS armoniza el estado de todos los documentos en forma electrónica como prueba admisible: ningún tribunal puede negarse a admitir un documento únicamente sobre esa base. Además, se promueve el reconocimiento legal de los servicios electrónicos de entrega registrada, ya que se prohíbe a los tribunales negar el efecto jurídico y la admisibilidad de los datos enviados o recibidos utilizando dicho servicio únicamente por el hecho de que el servicio es puramente electrónico (sea o no el servicio en cuestión un servicio cualificado).

Cabe destacar que el Reglamento eleva los servicios de entrega electrónica con certificación electrónica más allá de la equivalencia con los servicios postales públicos para equiparar a la transmisión de materiales por mensajería. Un servicio de entrega con registro electrónico cualificado le confiere:

- La integridad de los datos que transmite;
- Envío de los datos por el remitente y recibo identificados por el destinatario identificado;
- Precisión de la fecha y hora de envío y de recepción indicadas por el servicio.

Esto equivale a una prueba completa del servicio - a menos que haya evidencia en contrario (por ejemplo, como si un destinatario de un paquete de mensajería alegara que alguien más firmó para confirmar la recepción). Los datos transmitidos deben ser asegurados por un AES en tránsito para eliminar cualquier riesgo de alteración y se debe aplicar una marca de tiempo electrónica cualificada (que también requiere un AES). La dependencia en este contexto de AES en lugar de QES ilustra que el Reglamento pretende que AES sea tratado como suficiente garantía de integridad de los datos.

4 Artículo 19 5 Artículo 13(1) 6 Artículo 24

Parte 2

Cumplimiento del Reglamento

Claramente, existe una base legal para el uso de firmas electrónicas en la Unión Europea. El Reglamento es intencionalmente neutro desde el punto de vista tecnológico y no especifica cómo una solución debe cumplir los requisitos de eIDAS. Para las organizaciones que evalúan soluciones de firma electrónica, las siguientes páginas explican cómo eSignLive cumple con el Reglamento.

eIDAS contiene muchas disposiciones diferentes para el cumplimiento. En el marco de eIDAS, una firma electrónica en su sentido más amplio incluye cualquier dato en forma electrónica que se adjunte o esté lógicamente asociado con otros datos en formato electrónico y que el firmante utilice para firmar electrónicamente. Esta forma de firma electrónica es comúnmente conocida como la firma electrónica básica o simple, pero legalmente es admisible, pero eIDAS hace poco para definir cómo una tal firma puede satisfacer los requisitos del Reglamento.

Sin embargo, tanto AES como QES definen requisitos adicionales para mayores niveles de confiabilidad. La solución eSignLive cumple con todos los requisitos de eIDAS para firmas electrónicas, incluyendo AES y QES.

FIRMAS ELECTRÓNICAS AVANZADAS

eSignLive cumple con los requisitos de AES bajo eIDAS controlando el acceso a los datos de creación de firma electrónica del firmante durante el flujo de trabajo de firma electrónica.

- Antes de firmar, el firmante es identificado y proporciona su nombre y dirección de correo electrónico. Esta información se agrega de forma segura a eSignLive como parte de los datos de creación de firma electrónica. Se crea un identificador de firma único (USID) asociado al firmante y se añade a los datos de creación de firma electrónica en eSignLive.
- Los documentos que se firman electrónicamente se agregan de forma segura a eSignLive.
- El firmante debe introducir eSignLive mediante una autenticación satisfactoria a través de uno de los métodos de autenticación o puntos de acceso admitidos de eSignLive.
- Una vez autenticado, el firmante entra en una sesión en línea con los documentos y ejecuta uno o más actos de firma según sea necesario.
- Cada firma electrónica se crea con los datos de creación de firmas electrónicas del firmante, que sólo se puede acceder a través de la autenticación más la hora de firma y los sellos de fecha, así como metadatos relacionados con la sesión de firma electrónica.
- Cada firma electrónica se asegura mediante una firma digital.

ESignLive cumple con los requisitos de AES de la siguiente manera:

I. **Está unido exclusivamente al firmante.** Con el fin de crear su firma electrónica, el firmante debe ser autenticado por eSignLive para acceder y aplicar sus datos de creación de firma electrónica para firmar un documento. La firma electrónica resultante está unida exclusivamente al firmante.

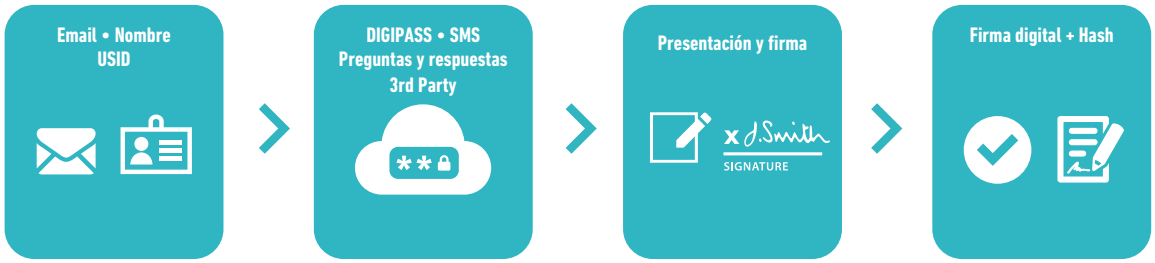
II. **Es capaz de identificar al firmante.** La firma electrónica incorpora los datos de firma de un firmante, que sólo se añade después de identificar al firmante.

III. **Se crea utilizando datos de creación de firma electrónica que el firmante puede utilizar con un alto nivel de confianza, bajo su control exclusivo.** Los datos de creación de firmas electrónicas del firmante contienen su nombre, dirección de correo electrónico y el identificador de firma único (USID), que sólo puede acceder y utilizar el firmante después de su autenticación exitosa por eSignLive. Puesto que eSignLive admite varios métodos de autenticación, uno o más pueden ser seleccionados para establecer una seguridad proporcional al riesgo involucrado en el proceso de firma.

IV. **Está vinculado a los datos firmados de tal manera que cualquier cambio posterior en los datos es detectable.** Cada firma electrónica está asegurada por una firma digital que contiene un valor de hash único para los datos firmados y los datos de creación de firma electrónica del firmante.

Es importante señalar que las firmas digitales eSignLive para AES son diferentes de las creadas por los certificados cualificados en QES. Las firmas digitales eSignLive para AES utilizan un solo conjunto de claves y un solo certificado digital para firmar digitalmente todas las transacciones para todos los firmantes. Cada firma electrónica se diferencia por los datos de creación de firmas electrónicas del firmante incluyendo nombre, dirección de correo electrónico, USID y datos de autenticación. En este caso, el dispositivo de creación de firmas es un módulo de seguridad de hardware (HSM) conectado al servicio eSignLive donde se crean las firmas digitales.

Figura 1. Flujo de trabajo avanzado de firma electrónica



Notas sobre el uso de AES y autenticación con eSignLive

ESignLive incluye la siguiente autenticación nativa:

- Iniciar sesión de cuenta de eSignLive mediante una contraseña a través de la web o de un cliente móvil;
- Introducir eSignLive desde un enlace de notificación por correo electrónico en el que el usuario fue autenticado por el sistema de correo electrónico. Esto se puede aumentar agregando un secreto compartido o una contraseña de una sola vez transmitida a través de SMS.
- Autenticación de terceros admitida a través de SAML, OAUTH o a través de la clave API.

La autenticación de dos factores se puede añadir con los productos VASCO DIGIPASS. eSignLive también admite el uso de certificados digitales basados en estándares en tarjetas inteligentes y dispositivos USB para la firma electrónica, incluyendo certificados cualificados.

Durante el transcurso de una sesión de firma electrónica, el firmante controla el acceso a la sesión en línea en todo momento y puede interrumpir una sesión y volver más tarde utilizando el mismo método de autenticación. Como resultado, eSignLive proporciona al firmante un alto nivel de confianza de que los datos de la firma permanecen bajo su control exclusivo.

Verificación de la validez de una firma electrónica

La verificación de la firma electrónica puede realizarse de varias maneras. En primer lugar, la firma digital eSignLive puede verificar la integridad del documento con firma electrónica utilizando Adobe Reader sin necesidad de complementos especiales, ya que el certificado digital eSignLive está vinculado al certificado raíz de Adobe que se encuentra en Reader. El ID del firmante también está protegido y verificable dentro de Reader.

Los datos de creación de firmas electrónicas (nombre, dirección de correo electrónico, USID) se pueden validar comparándolo con los datos originales almacenados en el sistema eSignLive. eSignLive está totalmente protegido y sólo se puede acceder después de la autenticación del firmante.

Los datos también pueden ser validados a través del informe de Resumen de Evidencia (una forma de pista de auditoría estática – véase "Evidencia Adicional" en la página siguiente) que se exporta desde y es digitalmente firmada por el sistema eSignLive. El formato de datos de firma electrónica cumple con ETSI TS 102 778-2 PAdES Basic.

FIRMAS ELECTRÓNICAS CUALIFICADAS

eSignLive también cumple con los requisitos para QES. Un QES se basa en una firma digital creada a través de un dispositivo de creación de firmas utilizando una llave única y un certificado digital conocido como un certificado cualificado asignado a una persona individual. El certificado cualificado y la clave asociada deben obtenerse de un Proveedor de Servicios de Confianza Cualificado (QTSP) y deben proporcionarse en una tarjeta inteligente o dispositivo USB compatible para usar con un sistema informático. Cuando se utiliza eSignLive para firmar con un QES, la tarjeta inteligente o el dispositivo USB debe estar conectado al equipo o al dispositivo móvil que accede al servicio eSignLive.

Al igual que con el AES, eSignLive controla y administra el uso de un certificado cualificado durante un flujo de trabajo de firma electrónica:

- Antes de la firma electrónica, los documentos se agregan de forma segura a eSignLive y se asocian al firmante.
- El firmante debe acceder a eSignLive mediante una autenticación satisfactoria a través de uno de sus métodos de autenticación o puntos de acceso soportados.
- El firmante entra en una sesión en línea con los documentos y ejecuta uno o más actos de firma según sea necesario.
- Como cada documento está firmado electrónicamente, las firmas electrónicas están aseguradas por firmas digitales creadas usando el certificado cualificado y la clave asociada para crear el QES.
- Las firmas digitales se crean en la tarjeta inteligente o en el sistema informático compatible con el dispositivo USB adjunto y, en cada caso, se requiere al menos un ID de usuario y una contraseña de acceso.

ESignLive cumple con los requisitos de QES de la siguiente manera:

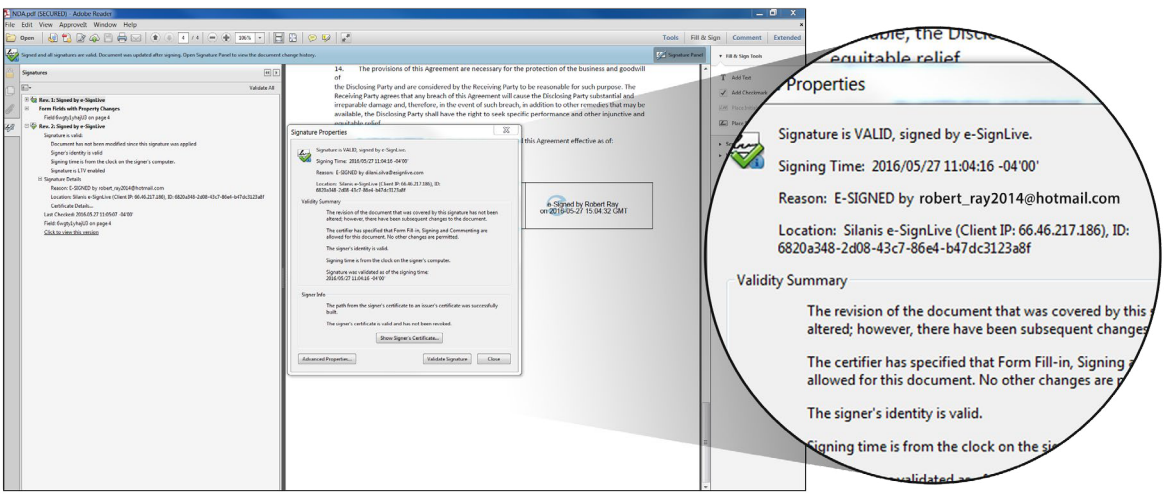
V. Se basa en un AES. Todos los requisitos para la creación de un QES también cumplen con los requisitos para un AES.

VI. Es creado por un dispositivo de firma electrónica cualificado. Mientras que eSignLive gestiona y controla todos los aspectos del flujo de trabajo y la seguridad de la firma electrónica, la firma digital real, utilizando el certificado cualificado, debe tener lugar en una tarjeta inteligente o sistema informático compatible con dispositivo USB conectado. Este es el dispositivo de firma electrónica cualificado como se define en el Reglamento.

VII. Utiliza un certificado cualificado para firmas electrónicas. Como se describió anteriormente, tener tal certificado es un requisito.

VIII. El QES debe ser creado por un QTSP. Con el QES, eSignLive requiere que el usuario proporcione su certificado cualificado en una tarjeta inteligente o dispositivo USB emitido por un tercero QTSP. Mientras que eSignLive habilita y controla la firma electrónica con el certificado y el dispositivo, el requisito de firma digital es satisfecho por el emisor tercero QTSP.

Figura 2. Verificación de firma electrónica en eSignLive.



ESignLive puede admitir certificados cualificados emitidos por cualquier TSP, siempre y cuando se base en el estándar de certificado digital X.509. A diferencia de otros proveedores de firma electrónica, eSignLive puede utilizar certificados de cualquier emisor. Esto también permite a las organizaciones aprovechar los certificados emitidos por su propia infraestructura de clave pública (PKI).

ESTÁNDARES DE FORMATOS

Con arreglo al artículo 27 de la eIDAS, la Comisión Europea está facultada para establecer normas técnicas adicionales y formatos de referencia para AES, cuando éstos se vayan a utilizar en el sector público. Una decisión de septiembre de 2015 introdujo estos formatos.

Las normas de firma de la European Telecommunications Standards Institution (ETSI) incluyen:

- Firma electrónica avanzada de sintaxis de mensajes criptográficos (CAdES)
- Firma electrónica avanzada XML (XAdES)
- Más recientemente, PDF Advanced Electronic Signature (PAdES)

Tanto CAdES como XAdES permiten soluciones de firma que definen un lugar dentro de los formatos datos de firma digital para contener los datos originales, o hacen uso de un formato de "empaquetado" en el que tanto la firma electrónica como los datos originales se colocan uno al lado del otro.

eSignLive produce documentos PDF con firma electrónica basados en AES o QES que se ajustan a ETSI TS 102 778-2 PAdES Basic.

EVIDENCIA ADICIONAL

Dependiendo del caso de uso, una organización puede optar por la firma electrónica simple, avanzada o cualificada. Como se mencionó anteriormente, AES y QES proporcionan una evidencia progresivamente más fuerte de la identidad del firmante y deben elegirse de acuerdo al nivel de riesgo involucrado en el proceso. Por ejemplo, un proceso de firma interno como una autorización de informe de gastos no implicaría el mismo nivel de riesgo que una apertura de cuenta bancaria remota y, como tal, no requiere el mismo tipo de firma electrónica.

Sin embargo, vale la pena señalar que ninguna de las formas de firma electrónica discutidas en este artículo proporciona evidencia de:

- Cómo ocurrió el proceso de firma;
- La intención del firmante.

eSignLive complementa los tres tipos de firma electrónica con evidencia electrónica en forma de pistas de doble auditoría para asegurar aún más la aplicabilidad de los contratos y acuerdos firmados electrónicamente. Esto incluye:

- **El rastro de auditoría estática** (lo firmado por el firmante): Este rastro de auditoría contiene el certificado digital utilizado para firmar, así como la imagen de bloque de firma, la marca de hora y el USID. eSignLive ofrece dos tipos de pistas de auditoría estática. La primera es la pista de auditoría integrada, en la que la información clave de auditoría está firmemente incrustada en el documento firmado electrónicamente, sin necesidad de administrar documentos, firmas y pruebas por separado. El segundo es el informe Resumen de Evidencia. Este es un registro de auditoría detallado de toda la transacción de firma electrónica que está disponible como un documento PDF completo asociado a la transacción.
- **El rastro de auditoría visual** (cómo y qué firmó el firmante): Con eSignLive, cada página web se muestra en el navegador y todas las acciones tomadas por cada firmante se registran, incluyendo pasar al siguiente documento o página web; hacer clic en un botón; aplicar una firma electrónica; y descargar copias completas de los documentos. La fecha y la hora se registran para cada acción, así como la dirección IP de cada participante en la transacción. Esto proporciona evidencia de cómo un registro electrónico fue presentado, revisado y firmado. La empresa puede sacar la prueba de auditoría visual y reproducirla pantalla por pantalla en cualquier momento para probar lo que sucedió, como una cámara de seguridad.

El uso de aplicaciones web o móviles para presentar y controlar la firma de documentos permite a las organizaciones crear la mejor experiencia de usuario al tiempo que garantiza el cumplimiento de las leyes relacionadas con la transacción comercial.

Sin embargo, en disputas legales relacionadas con procesos basados en la web, todo el proceso y el contenido presentado en el navegador pueden ser contestados incluso si la organización tiene los documentos finales, firmados y firmados en formato PDF. Por esta razón, no es aconsejable confiar en una prueba de auditoría estática para demostrar convincentemente que se estableció la intención y se siguió el proceso correcto. Una prueba de auditoría estática por sí sola no disuadirá a la gente de reclamar:

- "Alguien puede haber alterado el sistema."
- "No se me presentó esa información".
- "No entendí lo que estaba firmando."

Para protegerse contra esto, la prueba de auditoría visual de eSignLive captura la experiencia completa del firmante (es decir, todas las páginas web, documentos, revelaciones y otra información en pantalla, así como correos electrónicos y mensajes SMS enviados, junto con la hora y la fecha de cada evento). Un enlace criptográfico garantiza que la prueba de auditoría visual no ha sido alterada y se corresponde únicamente con el documento firmado electrónicamente. Esta capacidad única ha permitido a los clientes de eSignLive desviar numerosas disputas legales potenciales antes de que se conviertan en litigios.

CONCLUSIÓN

Como empresa de VASCO, eSignLive entiende los requisitos únicos del mercado europeo y ha estado automatizando las transacciones orientadas al cliente para las organizaciones reguladas por más de 20 años. En eSignLive, nuestra tecnología y experiencia se basa en los aprendizajes adquiridos a través de implementaciones en bancos líderes en todo el mundo, compañías de seguros, proveedores de cuidados médicos y agencias gubernamentales, así como las mejores prácticas de evidencia y admisibilidad. Para obtener más información sobre la firma electrónica de documentos, póngase en contacto con nosotros en sales@esignlive.com o visite www.esignlive.com.

Ver la lista de verificación de la firma electrónica en la página siguiente >>

Acerca de eSignLive™ de VASCO

ESignLive ™ es la solución de firma electrónica detrás de algunas de las marcas más confiables del mundo. Las industrias reguladas y las principales firmas de analistas reconocen a eSignLive por su capacidad para equilibrar los niveles más altos de seguridad, cumplimiento y auditabilidad con facilidad de uso para automatizar cualquier proceso, desde el flujo de trabajo de firma interno más simple hasta las transacciones más complejas y orientadas al cliente. Disponible en la nube y en las instalaciones, y con plena capacidad de etiquetado en blanco, eSignLive soporta la estrategia de transformación digital de una organización en toda la empresa.

ESignLive es el nombre comercial de Silanis Technology Inc., una empresa del grupo VASCO. VASCO Data Security International Inc., líder mundial en autenticación, firmas electrónicas y gestión de identidades, permite a más de 10.000 clientes en 100 países asegurar acceso, gestionar identidades, verificar transacciones y proteger activos a través de empresas financieras, empresariales, de comercio electrónico y de gobierno. Y los mercados sanitarios. Obtenga más información en **www.esignlive.com**

Lista de verificación de la solución E-Signature

La selección de la solución de firma electrónica adecuada para su organización depende de una serie de factores. La comprensión de los criterios clave y la forma de llegar rápidamente a la decisión correcta es esencial en la utilización eficaz de firmas electrónicas para los casos de uso previsto.

Estas son las consideraciones clave a medida que evalúan las diversas soluciones en el mercado en relación con el Reglamento eIDAS y los requisitos específicos de la UE. Verifique que el proveedor y la solución:

	Cumple con el último Reglamento eIDAS de la UE para firmas electrónicas, AES y QES
	Soporta certificados cualificados basados en el estándar X.509 - desde cualquier TSP
	Soporta certificados de la propia PKI de una organización
	Soporta AES mediante la autenticación fuerte y la firma digital basada en servidor para asegurar y enlazar la firma al documento
	Soporta QES para documentos con múltiples firmantes
	Ofrece una amplia gama de opciones de autenticación integradas (por ejemplo, código de texto SMS, desafío-respuesta, certificados digitales basados en el conocimiento, soporte para la autenticación fuerte de dos factores con soluciones como DIGIPASS y más)
	Completa las firmas electrónicas, AES y QES con pistas de auditoría duales - por ejemplo, pistas de auditoría estática y pistas de auditoría visual - que ilustran lo firmado y cómo se firmó
	Crea una firma digital y un hash para cada firmante en la transacción - sella el documento entre firmantes y cumple los requisitos de PAdES
	Garantiza la integridad del documento directamente desde el documento e-signed - independientemente del proveedor de la solución y sin tener que conectarse a su servicio
	Soporta los idiomas en los que opera y realiza negocios - tanto para los remitentes como para los firmantes
	Cuenta con un equipo de soporte técnico y de éxito de clientes que responden a sus necesidades, sirviendo a los clientes durante las horas de oficina locales
	Aborda la residencia de datos con opciones flexibles de implementación (por ejemplo, en el local o en una nube pública o privada en su país o región en la UE)