OneSpan
Be bold. Be secure.

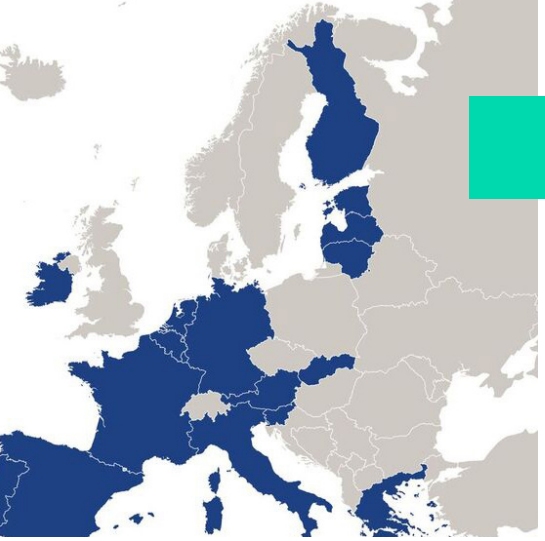
eIDAS Y LAS FIRMAS ELECTRÓNICAS UNA PERSPECTIVA LEGAL: FIRMAS ELECTRÓNICAS EN LA UNIÓN EUROPEA

LIBRO BLANCO

ÍNDICE DE CONTENIDOS

Sobre los autores

Este libro es el resultado de la colaboración entre Lorna Brazell, de Osborne Clarke LLP, y OneSpan. En la primera parte, Osborne Clarke brinda una opinión legal sobre la validez legal de las firmas electrónicas en la Unión Europea. La segunda parte ha sido preparada por OneSpan, y resume las recomendaciones de mejores prácticas en cuanto a conformidad legal a la hora de implementar las firmas electrónicas.



PARTE 1

Introducción

El Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior1 ("eIDAS") de 2014 entró en vigor en toda la Unión Europea ("UE") el 1 de Julio de 2016, reemplazando a la Directiva sobre firmas electrónicas2 de 1999 (la "Directiva"). Si bien dicha Directiva no había sido objeto de ninguna controversia en sus 16 años de historia, tampoco había supuesto un éxito. Su objetivo, que era permitir el uso generalizado de las firmas electrónicas para realizar negocios dentro de las fronteras de la UE, no se había cumplido.

Existían tres razones clave para ello:

I. La mayoría de las legislaciones de los Estados Miembro de la UE no especifican ningún tipo de firma para contratos comerciales, excepto garantías o contratos para asignar propiedades inmobiliarias.

II. Muchas personas pensaban erróneamente que la Directiva estipulaba el uso de firmas electrónicas avanzadas respaldadas por un certificado cualificado para que una firma electrónica tuviera validez legal. En realidad, la Directiva estipula lo contrario. Los tribunales pueden aceptar que cualquier tipo de firma electrónica tenga validez legal. No obstante, en el caso de las firmas electrónicas cualificadas, el tribunal no puede sino aceptarlas. No obstante, el coste y la carga administrativa de implementar la tecnología necesaria para las firmas electrónicas cualificadas superaban los potenciales beneficios de poder utilizarlas.

III. Existía una divergencia entre los Estados Miembro respecto al régimen regulatorio con el cual debían cumplir los proveedores de firmas o certificaciones. Como resultado de ello, las firmas plasmadas utilizando servicios de certificación aprobados en un Estado Miembro corrían el riesgo de no ser reconocidas legalmente en otro.

Dado que los mecanismos de la Directiva se han utilizado tan poco, no es sorprendente que no exista jurisprudencia europea para brindar orientación sobre cómo debería interpretarse.

Los defectos de la Directiva no han respaldado el desarrollo del comercio transfronterizo en la UE. En 2015, el Tribunal de Justicia de la Unión Europea ("TJUE") dictaminó que los términos de un acuerdo "pulsar y comprar" B2B pueden tener validez legal incluso si la parte pulsante/firmante no ha leído los términos de dicho acuerdo. En ese caso, El Madjoub, un vendedor de coches, buscaba ejecutar un contrato en línea para la adquisición de un coche de segunda mano, a través de procedimientos en su tribunal local alemán. Perdió el caso, ya que había hecho clic para indicar su aceptación de términos que no había leído. Y dichos términos incluían someterse a la jurisdicción de los tribunales belgas. El TJUE determinó que dicha persona estaba sujeta a dichos términos a pesar de no haberlos leído, dado que había tenido la oportunidad de leerlos e hizo clic para indicar que estaba de acuerdo con ellos. Igualmente, la forma más sencilla de firmas electrónicas imaginable –utilizar el cursor para hacer clic en un botón- puede tener validez legal, y la mayoría de las transacciones B2B o B2C pueden completarse sin firmas equivalentes a las manuscritas, siempre y cuando exista evidencia satisfactoria, sea en la forma que sea, para probar que cada parte había convenido en estar vinculada al contrato.

No obstante, la Comisión Europea concluyó que la falta de harmonización entre los Estados Miembros seguía constituyendo un potencial obstáculo para el mercado interno. De ese modo, al introducir el reglamento eIDAS y dejar a los Estados Miembro sin margen de implementación o interpretación, esperan asegurar que los documentos firmados de forma electrónica se aceptarán ahora en la totalidad de los 28 Estados Miembro de la UE, independientemente de los enfoques nacionales, legales o regulatorios.

> Bajo eIDAS, cualquiera de las tres categorías de firma electrónica puede tener validez legal. La diferencia entre ellas es tan sólo qué evidencia será necesaria para convencer a un tribunal de que la firma es genuina y de que se aplicó al documento en cuestión de forma intencional.

Aspectos clave del reglamento eIDAS

eIDAS tiene un alcance mucho más amplio que la Directiva, ya que además de las firmas, incluye asimismo identificación electrónica, entrega, servicios de archivado y autenticación de sitios web.

Firmas

eIDAS define las tres mismas categorías de firmas electrónicas, tal y como lo hacía la Directiva. Existen:

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

El enfoque para las tres es explícitamente neutro en cuanto a la tecnología. El Reglamento no estipula que deba utilizarse una tecnología específica, tan sólo los criterios que una firma debe satisfacer. No obstante, los requisitos para los certificados cualificados sugieren que tan sólo la tecnología de certificados digitales es la más adecuada.

De igual modo, en un amplio rango de casos de uso, tales como el contrato de compraventa de un coche en línea objeto de la decisión del TJEU detallado anteriormente, las firmas electrónicas que no son ni avanzadas ni cualificadas pueden tener validez legal, siempre y cuando las pruebas disponibles establezcan:

1. Que están vinculadas o lógicamente asociadas al documento firmado
2. Que la parte firmante tenía la intención de utilizar la firma electrónica para firmar, es decir, identificarse a sí mismo/a e indicar aceptación, aprobación, o simplemente conocimiento de los contenidos del documento.

De ello se desprende que las AES tienen asimismo validez legal como firmas, ya que por definición una AES captura gran parte de la evidencia necesaria. Una AES debe:

1. Estar vinculada de forma exclusiva a la parte firmante
2. Tener la capacidad de identificar a dicha parte firmante
3. Haber sido creada utilizando datos de creación de firma electrónica que la parte firmante puede, con un alto grado de confianza, usar únicamente bajo su control.
4. Estar vinculada a los datos firmados de modo que cualquier cambio posterior a dichos datos sea detectable

Esto no quiere decir que las cuestiones relacionadas con las evidencias no puedan solucionarse por otros medios.

Por ejemplo, si se escribe un nombre al final de un documento y se guarda en un ordenador localizado en un entorno laboral, la evidencia circunstancial en cuanto a qué personas hayan tenido acceso a dicho ordenador puede que sea suficiente para establecer que la persona que escribió el nombre era en efecto la persona así nombrada. Pero una AES requiere tecnología que no estaría disponible a un(a) compañero/a de trabajo que de forma maliciosa intentara firmar con el nombre de otra persona, y así reduce las posibilidades de que surja una impugnación, y mucho menos de que ésta resulte exitosa. (La definición no intenta circunscribir qué tecnología pueda ser.)

[1] Reglamento (UE) No 910/2014

[2] Directiva 1999/93/EC

[3] En este contexto, un certificado es una garantía de una tercera parte de que la identidad de la parte firmante ha sido verificada de forma adecuada.

Las QES se basan en las AES, y deben cumplir con estos requisitos adicionales:

1. Ser creadas por medio de un dispositivo de creación de QES
2. Estar respaldadas por un certificado cualificado

Los dispositivos de creación de las QES son en gran medida los mismos que los dispositivos seguros de creación de firma bajo la Directiva, con el requisito añadido de que la confidencialidad de los datos de creación de la firma electrónica están razonablemente asegurados. De igual forma, la definición de certificado cualificado coincide en su mayor parte con la definición equivalente en la Directiva.

La disposición tanto de eIDAS como de la Directiva de que las firmas electrónicas cualificadas deben reconocerse como legalmente equivalentes a las firmas manuscritas, sin necesidad de evidencia adicional, puede verse ahora simplemente como una confirmación de que la evidencia capturada por una firma electrónica avanzada, con la adición de alguna forma de verificación de la identidad y ciberseguridad adecuada, debe aceptarse como evidencia suficiente. Esto no implica, no obstante, que las QES no puedan verse impugnadas, al igual que las firmas manuscritas, si la evidencia demuestra que el dispositivo de creación ha sido sustraído, o se ha recurrido a algún tipo de fraude para engañar a la parte firmante para que firme el documento.

Más específicamente, el considerando 51 de eIDAS declara expresamente que una parte firmante debería poder confiar los dispositivos de creación de QES a una tercera parte, siempre y cuando se implementen mecanismos y procedimientos adecuados para asegurar que la parte firmante tenga el control exclusivo sobre el uso de los datos. En otras palabras, la autoridad de la firma puede delegarse siempre y cuando se implementen controles y salvaguardias organizacionales adecuados. El considerando 52 reconoce la posibilidad de la prestación de firmas electrónicas a distancia (tal y como servicios basados en la nube), sujeta a procedimientos de seguridad de gestión y administrativos, sistemas fiables y productos adecuados para garantizar que la parte firmante tiene el control exclusivo.

REQUISITOS DE eIDAS		
Firmas electrónicas	La firma electrónica debe: • Ser aplicada por la persona asociada a la firma • Ser aplicada de una forma que demuestre la intención de la parte firmante • Estar asociada al documento o datos que la parte firmante pretendía firmar	 Se requieren pruebas de apoyo adicionales  No se requieren pruebas de apoyo adicionales 
Firmas electrónicas avanzadas (AES)	Esta forma de firma electrónica agrega cuatro requisitos adicionales. La firma electrónica avanzada debe: • Estar vinculada exclusivamente a la parte firmante • Identificar a la parte firmante • Estar bajo el control exclusivo de la parte firmante • Detectar cambios en el documento o los datos tras la aplicación de la AES	
Firmas electrónicas cualificadas (QES)	Se trata de una firma electrónica avanzada que, además, debe: • Ser creada utilizando un dispositivo de creación de QES • Estar respaldada por un certificado cualificado (que se emite para la parte firmante en una forma que la misma puede mantener bajo su control)	

Identidades electrónicas

eIDAS trata aspectos de documentos de identidad electrónicos (eIDs), pero tan sólo en el contexto limitado de eIDs utilizados para las interacciones de los ciudadanos con la administración pública, tales como acceder a los servicios sanitarios o pagar impuestos. No se estipula ningún sistema de eID, ya que no todos los Estados Miembro tienen un tipo de documento nacional de identidad implementado. Más bien, para aquellos Estados Miembro que desean que se reconozcan sus documentos de identidad electrónicos más allá de su frontera, eIDAS busca asegurar el reconocimiento mutuo de los sistemas de documentos de identidad electrónicos existentes. Para ello, define diferentes niveles de garantía de la identidad y obliga a cada Estado Miembro a aceptar los documentos de identidad electrónicos emitidos por otro Estado Miembro, siempre y cuando el documento de identidad electrónico cumpla con el nivel de garantía de la identidad requerido para el acceso al servicio en cuestión. Este proceso podría caracterizarse como favorecedor de la armonización, en lugar de como imposición de la armonización. Este es el contexto en el que se crea la mayoría de las iniciativas del sector privado, tales como iDIN, BankID, it'sMe, NemID, FranceConnect, etc. Estos servicios están basados en el hecho de que un individuo ya esté inscrito por el gobierno de un Estado Miembro. El eID entonces se da a través de:

- El proceso CSC de un banco
- BankID
- NemID
- O la identificación de un servicio público, tal como FranceConnect

Sus soluciones son por lo tanto interoperativas en toda la Comunidad Europea. Probablemente pasen varios años antes de que la mayoría de los Estados Miembro acepten eIDs emitidos en el extranjero como evidencia de legitimación para acceder a sus servicios públicos.

Al igual que la Directiva, eIDAS no afecta a la validez de las disposiciones existentes en cuanto a firmas dentro de los sistemas cerrados, y no se pronuncia respecto a la cuestión de la administración pública. Una serie de Estados Miembro extrajeron las comunicaciones electrónicas con las instancias públicas de las leyes generales que implementaban la Directiva, pero eso ya no va a ser posible. Incluso en aquellos Estados Miembro que no cuenten con sistemas de eID, será posible firmar documentos oficiales electrónicamente.

eIDAS estuvo en la legislación durante dos años antes de su fecha de entrada en vigor, el julio de 2016, para dejar tiempo para realizar diversos trabajos de preparación. En particular, la Comisión Europea recibió el mandato de preparar especificaciones técnicas, normas y procedimientos para asegurar que el reconocimiento mutuo sea efectivo tanto en la práctica como en las leyes.

La lista de sistemas de eID que aceptan el reconocimiento mutuo se publicará únicamente un año después de la preparación de dichos materiales, que no se han finalizado todavía. Tendrá que pasar más tiempo antes de que las disposiciones relevantes de eIDAS entren en vigor.

Efecto legal de los diferentes tipos de firma

Bajo eIDAS, cualquiera de las tres categorías de firma electrónica puede tener validez legal. La diferencia entre ellas es tan sólo qué evidencia será necesaria para convencer a un tribunal de que la firma es genuina y de que se aplicó al documento en cuestión de forma intencional.

- Una forma sencilla de firma electrónica, como teclear un nombre, o una copia en PDF de una firma manuscrita, resulta fácil de falsificar, de modo que es probable que un tribunal requiera evidencia adicional sustancial para demostrar que fue en efecto aplicada por la persona nombrada al documento en cuestión.
- Una AES es mucho más difícil de falsificar y está asociada más estrechamente al documento firmado, de modo que la evidencia adicional requerida será considerablemente menor.
- Una QES, por otra parte, no requiere evidencia adicional, ya que según el Artículo 25 de eIDAS, un tribunal está obligado a aceptar su equivalencia con una firma manuscrita. De hecho, una QES pasa la carga de la prueba a la parte firmante, al contrario de lo que ocurre con una AES, la cual, si resulta impugnada, requiere que el proveedor de servicios de confianza demuestre que la firma tiene validez legal. Por supuesto, puede que sea necesario demostrar que la QES cumple en efecto con los requisitos de la QES.

Para evaluar la idoneidad de cualquier tipo de firma para su uso en un documento en particular, la primera pregunta a plantear es por qué se requiere la firma. Cuando las leyes no especifican qué tipo de firma es necesaria para que un documento tenga validez legal, existirán menos probabilidades de que los tribunales requieran tipos más elaborados de firmas. Las firmas electrónicas sencillas o AES deberían ser aceptables en dichas circunstancias.

Igualmente, si la firma indica que se ha recibido cierta información cuando existe un requisito legal de que haya que notificar a los clientes ciertos hechos, una firma electrónica sencilla o AES debería ser suficiente.

Cuando la firma tiene validez legal para vincular a la parte firmante, se asumirá un menor riesgo si se utiliza un modo más formal de firma -AES o QES- ya que las formalidades de dichas firmas capturan automáticamente gran parte de la evidencia necesaria para probar su autenticidad ante los tribunales. Pero si las partes convienen conjuntamente en qué tipo de firma electrónica es adecuada usar, esto se tendrá en cuenta en cualquier proceso judicial.

eIDAS no tiene repercusión sobre los requisitos legales nacionales respecto a qué documentos requieren una firma para que éstos tengan validez legal, ya que es una cuestión que depende de un amplio abanico de leyes: las que gobiernan los testamentos, transferencias de propiedad, garantías, procesos electorales, etc. Sigue siendo necesario comprobar cuáles son los requisitos legales nacionales caso por caso para verificar si un documento requiere una firma, y en caso afirmativo, con qué propósito (notificación, validez legal u otro).

> No puede denegarse la admisibilidad de la evidencia o efecto legal de una firma electrónica simplemente en base a que tiene un formato electrónico o que no cumple con los requisitos de firmas electrónicas cualificadas.

Como resultado de ello, eIDAS reconoce explícitamente que otras formas de firma electrónica deberían tener validez legal en las circunstancias adecuadas. Además, reconoce que los tribunales de un Estado Miembro tienen la obligación de considerar la evidencia y las circunstancias para poder llegar a una conclusión, y no simplemente desestimar las firmas electrónicas que no sean QES. Con el transcurso del tiempo, las decisiones del TJUE empezarán a establecer normas para lograr la contundencia de la evidencia de firmas electrónicas que no sean QES.

Reglamento de los servicios de confianza

La proliferación de normas y sistemas nacionales dispares en cuanto al reglamento y supervisión de los proveedores de servicios de certificación fue una de las razones por la cual la Directiva no logró promover el uso transfronterizo de las firmas electrónicas, ya que los Estados Miembro elaboraron requisitos ampliamente divergentes para el sector. Por ejemplo, el Reino Unido optó por dejar que el sector se regulara a sí mismo, mientras que Alemania e Italia introdujeron requisitos legales rígidos. En dichas circunstancias, no resultó muy sorprendente que se esperase que los certificados de un país no fueran a ser reconocidos en otro, y muy pocos proveedores ofrecieron certificados transfronterizos en el sentido de que fueran certificados que respaldasen firmas de entidades de cualquier nacionalidad que no fueran la del proveedor del servicio en sí.

Por ello, uno de los objetivos clave de eIDAS es permitir a los proveedores de servicios de confianza (TSP, por sus siglas en inglés) de todo tipo ofrecer servicios transfronterizos, incluyendo a los proveedores de certificados que respaldan firmas electrónicas.

La Directiva trataba únicamente de firmas electrónicas y certificados acreditativos, y por ello utilizaba el término proveedor de servicios de certificación. Esto es demasiado reducido para eIDAS, que abarca un abanico más amplio de servicios electrónicos, incluyendo servicios de validación y preservación de firmas, sellos (tanto ordinarios como avanzados), marcas temporales, servicios de entrega y autenticación de sitios web. Por ello se introdujo el término colectivo TSP.

Se considera necesario prescribir normas operacionales legales y técnicas para todos los TPS, ya que ocupan una posición única en cualquier transacción en la que participan dos partes: consumidores, ciudadanos y empresas. No existe una "copia física" exacta equivalente a una parte que, sin participar en la transacción como tal, resulta no obstante decisiva a la hora de permitir su realización. El papel más similar es el del notario que verifica y certifica la identidad de una parte contratante con el fin de llevar a cabo una transacción a distancia.

Los notarios están regulados por sus normas profesionales.

Existen dos categorías de TSP: ordinarios y cualificados (QTSP, por sus siglas en inglés). Un QTSP es un TSP que brinda uno o más servicios de confianza cualificados, tales como la creación, verificación, y validación de firmas electrónicas cualificadas, y que recibe su estatus de cualificado de un organismo supervisor nominado por un Estado Miembro. Ambas categorías pueden proveer cualquier tipo de servicio de confianza.

Todos los TSP deben conformarse a normas de seguridad adecuadas para prevenir y reducir al mínimo la repercusión de cualquier posible incidente de seguridad e informar a las partes interesadas de los efectos negativos de cualquier incidente.4 En el caso de que un fallo de seguridad o pérdida de datos tenga una repercusión significativa en el servicio de confianza o la información personal almacenada, el TSP debe notificar de ello al órgano supervisor en el transcurso de 24 horas tras tener conocimiento de dicho incidente. Los clientes afectados deben asimismo ser notificados sin dilaciones injustificadas.

Además de los requisitos de seguridad, eIDAS impone la responsabilidad a los TSP por cualquier daño causado de forma intencional o negligente a cualquier

persona debido a que el TSP no hubiera cumplido con sus obligaciones.5 Más específicamente, esto no se ve limitado a las partes de la transacción: Podría tratarse de una tercera parte (una compañía matriz o subsidiaria, por ejemplo). La parte demandante tiene la carga de probar que los daños fueron causados de forma intencional o negligente, a menos que el TSP sea un QTSP, en cuyo caso se presume la intención o negligencia. Por supuesto, un QTSP tiene el derecho de rebatir la presunción de intencionalidad o negligencia.

Al contrario de lo que ocurre con el esquema de la Directiva, tanto los TSP "ordinarios" como los QTSP pueden limitar su responsabilidad a partes usuarias para la emisión de un certificado.

Bajo la Directiva, tan solo los QTSP podían imponer dichos límites. La responsabilidad se ve limitada al alcance de cualquier limitación sobre el uso de sus servicios (del cual el TSP puede haber dado aviso por adelantado a sus clientes), siempre y cuando dichas limitaciones sean reconocibles asimismo a terceras partes. Lo que se requiere para que una limitación sea "reconocible" no está claro, pero una notificación de un modo fácilmente accesible es probablemente eficaz. Además de cumplir con las normas de seguridad, los QTSP deben:

- Pasar auditorías con regularidad
- Aplicar procedimientos adecuados bajo las leyes nacionales a tareas tales como verificar identidades
- Emplear a personal con las cualificaciones adecuadas y utilizar sistemas fiables tanto para procesar como para almacenar datos
- Contratar un seguro de responsabilidad
- Mantener registros adecuados
- Mantener un plan de terminación actualizado para asegurar la continuación del servicio si el QTSP cierra.[6]

La mayoría de éstas son, por supuesto, buenas prácticas empresariales. Nada impide a un TSP cumplir con los requisitos y aplicar las normas aprobadas para sistemas y productos fiables, sin tener que optar al estatus de QTSP.

Un QTSP no necesita ser "cualificado" respecto a todos los servicios de confianza que ofrece, y esto se muestra en la lista publicada de proveedores. De igual modo, un QTSP podría estar cualificado a efectos de autenticación de sitios web, por ejemplo, pero no estar cualificado para la entrega electrónica de firmas electrónicas.

Las ventajas de obtener el estatus de QTSP giran esencialmente en torno al marketing. El hecho de estar supervisados por una agencia gubernamental y recibir dicho estatus debería ayudar a persuadir a potenciales clientes de que sus servicios son verdaderamente fiables. Su estatus como QTSP será público a lo largo de la publicación de la lista fiable de QTSP de los Estados Miembro. El único derecho adicional disponible para los QTSP que no está disponible para los TSP es el uso de la nueva marca de fiabilidad de la UE para servicios de confianza cualificados.

Buenas prácticas legales

Como se mencionó anteriormente, las firmas electrónicas resultan perfectamente aceptables en muchos contextos sin necesariamente requerir las características técnicas de las AES, y mucho menos de las QES. En el contexto contractual, una firma no es más que una forma de evidencia de que se ha convenido en los términos. Otra evidencia, como por ejemplo una cadena de autorizaciones internas anteriores a la firma, pueden estar disponibles y pueden resultar suficientes para asegurar que el acuerdo es exigible.

No obstante, la mayoría de los Estados Miembro tienen leyes nacionales que requieren que se firmen categorías particulares de documentos. Los contratos de créditos al consumidor se encuentran entre los formularios que comúnmente requieren firmas, al igual que los contratos de compraventa de bienes inmuebles y garantías, o, en general, aquellos documentos que requieren una firma manuscrita como prueba de consentimiento. Existen asimismo requisitos legales de firma para numerosos documentos corporativos y de banca. Estas categorías no están en sí mismas armonizadas bajo las leyes de la UE y por eso varían de un país a otro. Como resultado, es necesario verificar para cada caso de uso propuesto si un documento corporativo, bancario o de otro tipo necesita ser firmado bajo las leyes aplicables.

Afortunadamente, eIDAS sí armoniza el estatus de todos los documentos en formato electrónico como evidencia admisible. Ningún tribunal puede rechazar la admisión de un documento únicamente en base a eso. Además, el reconocimiento legal de los servicios de entrega registrada electrónica está avanzado. Los tribunales tiene prohibido denegar la validez legal y la admisibilidad de los datos enviados o recibidos por medio de dicho formato únicamente en base a que el servicio es puramente electrónico en forma, independientemente de si el servicio en cuestión es un servicio cualificado.

En particular, eIDAS eleva los servicios de entrega registrados electrónicos cualificados más allá de la equivalencia con los servicios postales públicos para igualarlos con la transmisión de materiales por mensajería.

Un servicio de entrega registrado electrónico cualificado confiere:

- La integridad de los datos que transmite
- El envío de los datos por el remitente identificado y la recepción por el destinatario identificado
- La exactitud de la fecha y la hora de envío y recepción indicadas por el servicio

Esto equivale a una completa prueba de entrega, a menos de que exista evidencia de lo contrario. Los datos transmitidos deber estar asegurados por una AES en tránsito para eliminar cualquier riesgo de manipulación, y debe aplicarse una marca de tiempo electrónica cualificada (que requiere asimismo una AES). La dependencia de una AES en este contexto, en lugar de una QES, ilustra que eIDAS prevé que las AES sean tratadas como suficiente garantía de la integridad de los datos.

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

PARTE 2

Conformidad con las regulaciones

eIDAS contiene numerosas disposiciones diferentes respecto a la conformidad. Bajo eIDAS, una firma electrónica en su sentido más amplio incluye cualquier dato en formato electrónico que está vinculado a o asociado lógicamente a otros datos en formato electrónico y que la parte firmante utiliza para firmar electrónicamente. Comúnmente denominada firma electrónica básica o sencilla, esta forma de firma electrónica tiene validez legal, pero eIDAS no se pronuncia demasiado sobre cómo dicha firma puede cumplir sus requisitos.

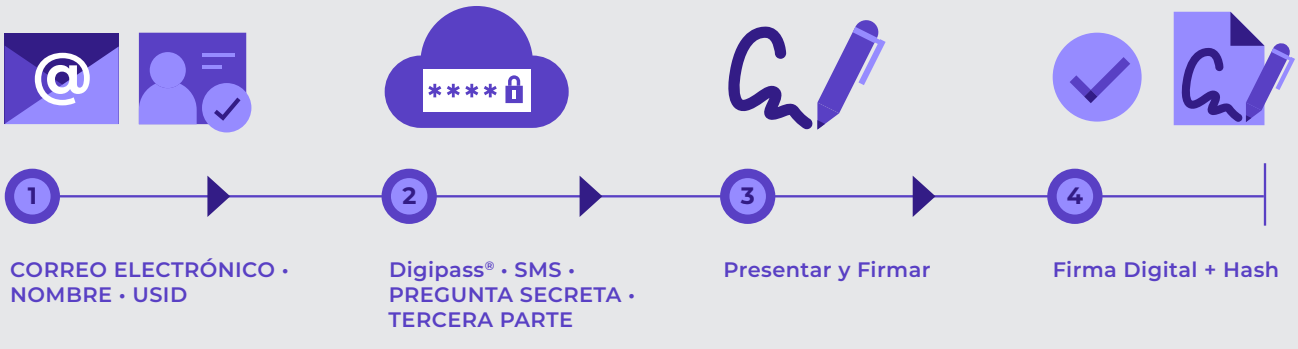
No obstante, tanto las AES como las QES definen requisitos adicionales para niveles más altos de fiabilidad. La solución OneSpan Sign cumple con todos los requisitos de eIDAS para firmas electrónicas, incluyendo AES y QES.

Firmas electrónicas avanzadas

OneSpan Sign cumple con los requisitos de AES bajo eIDAS controlando el acceso a la fecha de creación de firmas electrónicas de la parte firmante durante el proceso de firma electrónica.

- Antes de firmar, se identifica a la parte firmante, quien proporciona su nombre y dirección de correo electrónico. Esta información se añade de forma segura a OneSpan Sign como parte de los datos de creación de la firma electrónica. Se crea un identificador de firma único (USID) asociado a la parte firmante, que se añade a los datos de creación de la firma electrónica en OneSpan Sign.
- Los documentos que se deben firmar se añaden de forma segura a OneSpan Sign
- La parte firmante debe entrar a OneSpan Sign por medio de la autenticación correcta de uno de los métodos de autenticación o puntos de acceso respaldados por OneSpan Sign.
- Una vez autenticada, la parte firmante inicia una sesión en línea con los documentos y ejecuta uno o más actos de firma, según se requiera.
- Cada firma electrónica se crea con los datos de creación de la firma electrónica de la parte firmante, que es accesible únicamente a través de la autenticación y las marcas de hora y fecha de la firma, o como meta-datos relacionados con la sesión de firma electrónica.
- A continuación, cada firma electrónica se protege con una firma digital.

FIGURA 1. FLUJO DE TRABAJO DE FIRMAS AVANZADAS



OneSpan Sign cumple con los requisitos de AES de la siguiente forma:

1. **Está vinculada de forma exclusiva a la parte firmante.** Para crear su firma electrónica, la parte firmante debe ser autenticada por OneSpan Sign (o por la organización que usa dicho servicio, como por ejemplo un banco, en calidad de Autoridad de Registro) para acceder a y aplicar los datos de creación de su firma electrónica para firmar un documento. La firma electrónica resultante está vinculada exclusivamente a la parte firmante.

2. **Es capaz de identificar a la parte firmante.** La firma electrónica incorpora los datos de firma de la parte firmante, que se añaden tan sólo después de identificar a la parte firmante. En este caso, todos los datos de identidad y la transacción se almacenan en un archivo de evidencia que está disponible a todas las partes firmantes.

3. **Se crea utilizando datos de creación de firmas electrónicas que la parte firmante puede, con un elevado nivel de confianza, utilizar bajo su exclusivo control.** Los datos de creación de la firma electrónica contienen su nombre, dirección de correo electrónico, y el USID al que solo la parte firmante puede acceder y que solo la parte firmante puede utilizar tras su autenticación correcta por parte de OneSpan Sign. Dado que OneSpan Sign respalda numerosos métodos de autenticación, se puede seleccionar uno o más para que la seguridad establecida sea proporcional al riesgo involucrado en el proceso de firma.

4. **Está vinculada a los datos firmados de tal forma que cualquier cambio posterior en los datos sea detectable.** Cada firma electrónica está protegida por una firma digital que contiene un hash o control único asignado a los datos firmados y los datos de creación de la firma electrónica de la parte firmante.

Cabe destacar que las firmas digitales de OneSpan Sign para AES son diferentes a las creadas por certificados cualificados en QES. Las firmas digitales para AES de OneSpan Sign utilizan un único conjunto de teclas y un único certificado digital para firmar digitalmente todas las transacciones para todas las partes firmantes. Cada firma electrónica se diferencia por los datos de creación de la firma electrónica de la parte firmante, incluyendo nombre, dirección de correo electrónico, USID y datos de autenticación. En este caso, el dispositivo de creación de firma es un Módulo de Seguridad Hardware (HSM, por sus siglas en inglés) vinculado al servicio de OneSpan Sign en el que se crean las firmas digitales.

Notas sobre el uso de AES y autenticación con OneSpan Sign

OneSpan Sign incluye la siguiente autenticación nativa:

- Inicio de sesión en la cuenta de OneSpan Sign por medio de una contraseña, en Internet o un cliente móvil
- Ingreso a OneSpan Sign desde un enlace contenido en un correo electrónico de notificación en el que el/la usuario/a fue autenticado por el sistema de correo electrónico. Esto puede aumentarse añadiendo una pregunta secreta o código de un solo uso enviado por SMS
- Autenticación de terceras partes respaldada por SAML, OAUTH o por medio de una llave API

Se puede añadir autenticación de dos factores con los productos OneSpan Digipass. OneSpan Sign es compatible asimismo con el uso de certificados digitales basados en normas en tarjetas inteligentes y dispositivos USB para firmar electrónicamente, incluyendo certificados cualificados.

Durante el transcurso de una transacción de firma electrónica, la parte 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 de ello, OneSpan Sign brinda a la parte firmante un elevado nivel de confianza de que los datos de la firma permanecen bajo su control exclusivo.

Cómo verificar la validez de una firma electrónica

La verificación de la firma electrónica puede realizarse de varias formas. Primero, la firma digital de OneSpan Sign puede verificar la integridad del documento firmado electrónicamente utilizando Adobe Reader, sin necesidad de plug-ins, ya que el certificado digital de OneSpan Sign está vinculado al certificado raíz que se encuentra en Reader. El ID de la parte firmante está asimismo protegido y es verificable dentro de Reader.

Los datos de creación de la firma electrónica (nombre, dirección de correo electrónico, USID) pueden validarse comparándolos con los datos originales almacenados en el sistema de OneSpan Sign. OneSpan Sign es completamente seguro y únicamente puede accederse al mismo tras la autenticación exitosa de la parte firmante.

Los datos pueden asimismo ser validados por medio de un archivo de evidencia de valor probatorio en el cual se archivan todos los datos de la transacción, que se marcan con la fecha y la hora (una forma de registro auditable estático: Consultar “Evidencia adicional” en la siguiente página), que se exporta y firma electrónicamente desde el sistema de OneSpan Sign. El formato de los datos de la firma electrónica es conforme con ETSI TS 102 778-2 PAdES Basic.

Firmas electrónicas cualificadas

OneSpan Sign cumple asimismo los requisitos para QES. Una QES se basa en una firma digital creada a través de un dispositivo de creación de firma que usa una clave única y un certificado digital asignado a una persona individual. El certificado cualificado y su clave asociada deben obtenerse a través de un Proveedor de Servicios de Confianza Cualificado (QTSP) y debe proporcionarse en una tarjeta inteligente o dispositivo USB compatible para usarlo en un sistema informático. Cuando se utiliza OneSpan Sign para firmar electrónicamente con una QES, la tarjeta inteligente o dispositivo USB debe estar conectado al ordenador o dispositivo móvil con el que se está accediendo al servicio de OneSpan Sign.

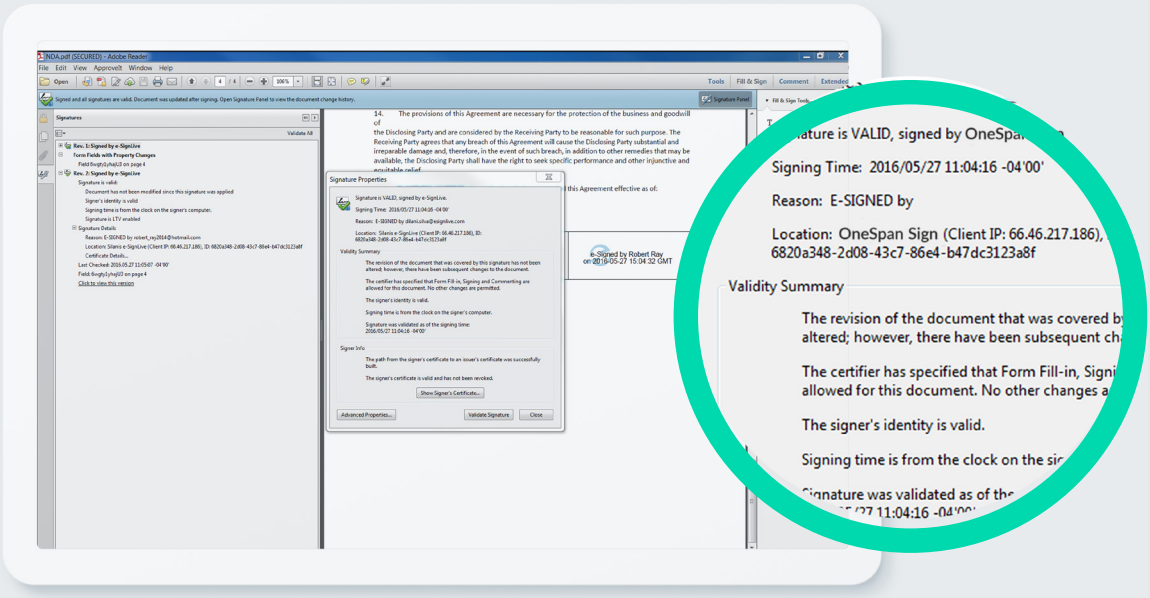
Al igual que con las AES, OneSpan Sign controla y gestiona el uso del certificado cualificado durante el proceso de firma electrónica:

- Antes de firmar electrónicamente, los documentos se añaden de forma segura a OneSpan Sign y se asocian a la parte firmante
- La parte firmante debe entrar a OneSpan Sign a través de una autenticación correcta por medio de uno de sus métodos de autenticación o puntos de acceso compatibles
- La parte firmante inicia una sesión en línea con los documentos y ejecuta uno o más actos de firma, según se requiera
- Según se va firmando cada documento, las firmas electrónicas se protegen con firmas digitales creadas utilizando el certificado cualificado y su clave asociada para crear la QES
- Las firmas digitales se crean en la tarjeta inteligente o sistema informático con el dispositivo USB conectado compatibles, y en cada caso se requiere al menos un ID de usuario y contraseña para el acceso

OneSpan Sign cumple con los requisitos de QES, de la manera siguiente:

1. **It 1. Está basado en AES.** Todos los requisitos para la creación de una QES cumplen asimismo con los requisitos de las AES
2. **Se crea por un dispositivo de firma electrónica cualificado.** Mientras que OneSpan Sign maneja y controla todos los aspectos del flujo de trabajo y seguridad de la firma electrónica, la firma digital en sí debe realizarse en una tarjeta inteligente o sistema informático con un dispositivo USB conectado compatibles. Este es el dispositivo de firma electrónica cualificada que definen las regulaciones.
3. **Utiliza un certificado cualificado para firmas electrónicas.** Tal y como se ha descrito anteriormente, es un requisito contar con dicho certificado.
4. **La QES debe ser creada por un QTSP.** Con la QES, OneSpan Sign requiere que el usuario proporcione su certificado cualificado en una tarjeta inteligente o dispositivo USB emitido por un QTSP tercera parte. Mientras que OneSpan Sign posibilita y controla la firma electrónica con el certificado y el dispositivo, el requisito de firma digital lo cumple el QTSP tercera parte.

FIGURA 2. VERIFICACICÓN DE FIRMAS ELECTRÓNICAS CON ONESPAN SIGN



OneSpan Sign es compatible con certificados cualificados emitidos por cualquier TSP siempre y cuando estén basados en la norma X.509 de certificados digitales. Al contrario de lo que ocurre con otros proveedores de firmas digitales, OneSpan Sign puede utilizar certificados de cualquier emisor. Esto permite asimismo a las organizaciones aprovechar certificados emitidos por sus propias infraestructuras de clave pública (PKI), desde su propia Autoridad de Certificación (CA).

Normas sobre el formato

Bajo el Artículo 27 de eIDAS, la Comisión Europea tiene la potestad para establecer normas técnicas y formatos de referencia adicionales para AES, cuando vayan a ser utilizadas en el sector público. Una decisión con fecha de septiembre de 2015 introdujo estos formatos.

Las normas para firmas del Instituto Europeo de Normas de Telecomunicación (ETSI) incluyen:

- Firma electrónica avanzada con sintaxis de mensajes criptográficos (CAdES)
- Firma electrónica avanzada XML (XAdES)
- Más recientemente, firma electrónica avanzada en PDF (PAdES)

Tanto CAdES como XAdES posibilitan soluciones de firma que o bien definen un lugar dentro del formato de datos de la firma digital para albergar los datos originales, o bien usan un formato "paquete" en el que tanto la firma electrónica como los datos originales se colocan lado a lado.

OneSpan Sign produce documentos en PDF firmados electrónicamente basados en AES o QES que son conformes con ETSI TS 102 778-2 PAdES Basic.

Evidencia adicional

Dependiendo del caso de uso, una organización puede optar por las firmas electrónicas sencillas, avanzadas o cualificadas. Como se mencionó anteriormente, las AES y QES proporcionan progresivamente mayor evidencia de la identidad de la parte firmante y deberían seleccionarse según el nivel de riesgo involucrado en el proceso. Por ejemplo, un proceso de firma interno como una autorización de gastos no implica el mismo nivel de riesgo que una apertura de cuenta bancaria a distancia y, como tal, no requiere el mismo tipo de evidencia y firma. De hecho, la apertura de una cuenta bancaria está gobernada por varias normas de cumplimiento que están integradas en la transacción misma, tal como la descripción del proceso de suscripción o la aceptación de las condiciones generales, o incluso los pasos inherentes a procedimientos para evitar el blanqueo de dinero. Cabe destacar, no obstante, que ninguna de las formas de firmas electrónicas tratadas en este artículo brinda evidencia de:

- Cómo se produjo el proceso de firma
- La intención de la parte firmante

OneSpan Sign suplementa los tres tipos de firma electrónica con evidencia electrónica en forma de registros auditables duales para asegurar aún más la ejecutabilidad de contratos y acuerdos firmados electrónicamente. Esto incluye:

- **El registro auditable estático** (lo que firmó la parte firmante): Este registro auditable contiene el certificado digital utilizado para firmar, así como la imagen de bloque de la firma, la marca de hora y el USID. OneSpan Sign ofrece dos tipos de registros auditables estáticos. El primero es el registro auditable integrado, en el que la información auditable clave se integra de forma segura en el documento firmado electrónicamente, sin necesidad de gestionar documentos, firmas y evidencia de forma separada. El segundo es el Informe de resumen de evidencia. Esto es un registro auditable detallado de la transacción de firma en su totalidad que está disponible como documento PDF completo asociado a la transacción.
- **El registro auditable visual** (cómo y qué firmó la parte firmante): Con OneSpan Sign, cada página web se muestra en el navegador y se registran todas las acciones realizadas por la parte firmante, incluyendo pasar al siguiente documento o página web, hacer clic en un botón, aplicar una firma electrónica, y descargar copias cumplimentadas de los documentos. Se registra la fecha y hora de cada acción, así como la dirección IP de cada participante en la transacción. Esto proporciona un conjunto de pruebas que puede utilizarse para hacer un seguimiento de la transacción en su totalidad, y así definir el modo en que se presentó, revisó y firmó un registro electrónico. La organización puede extraer el registro auditable visual y reproducirlo pantalla por pantalla en cualquier momento para probar qué ocurrió, como lo haría una cámara de seguridad.

Utilizar Internet o aplicaciones móviles para presentar y controlar la firma de los documentos permite a las organizaciones crear una mejor experiencia para el usuario, a la vez que asegura su conformidad con las leyes relacionadas con la transacción comercial.

No obstante, en litigios que implican procesos basados en Internet, el proceso y contenido en su totalidad pueden verse impugnados incluso si la organización tiene los documentos finales en PDF firmados electrónicamente y protegidos. Por esta razón, no es aconsejable confiar en un registro auditable estático para probar de forma convincente que la intención estaba establecida y que se siguió el proceso adecuado. Un registro auditable estático por sí solo no evitará que alguien declare:

- "Quizás alguien manipuló esa información"
- "No se me presentó esa información"
- "No entendí qué estaba firmando"

Para protegerle de esto, el registro auditable visual de OneSpan Sign captura la experiencia de la parte firmante en su totalidad (es decir, todas las páginas web, documentos, descargas de responsabilidad, y otra información que aparezca en pantalla, junto con la fecha y hora de cada evento). Un enlace criptográfico asegura que no se ha manipulado el registro auditable visual y que éste corresponde exclusivamente al documento firmado electrónicamente. Esta capacidad única ha permitido a los clientes de OneSpan Sign evitar numerosos potenciales conflictos judiciales antes de que se conviertan en litigios.

Conclusión

OneSpan comprende los requisitos particulares del mercado europeo y lleva automatizando transacciones de cara al cliente para organizaciones reguladas durante más de 20 años. En OneSpan Sign, nuestra tecnología y pericia están basadas en conocimientos obtenidos a través de implementaciones en los principales bancos de todo el mundo, así como aseguradoras, proveedores de servicios sanitarios y agencias gubernamentales, y también en las mejores prácticas probatorias y de admisibilidad.

Consultar la lista de verificación de evaluación de firmas electrónicas en la siguiente página >>

Obras citadas

[1] El objetivo de nuestra revisión de las leyes aplicadas aquí se conciben como una visión general de alto nivel y no debería considerarse asesoría legal en relación a ninguna situación factual. Este documento es únicamente para uso de la parte destinataria (eSignLive). No puede citarse, ya sea en su totalidad o en parte, o de cualquier otro modo mencionarse o utilizarse con otro propósito que el de brindar información general sin el consentimiento previo por escrito tanto de eSignLive como Stikeman Elliott LLP.

[2] Las leyes federales pueden resultar en la no-aplicación de un contrato (por ejemplo, bajo las leyes federales sobre insolvencia). La aplicación de un contrato es un asunto distinto a la aplicabilidad de un contrato.

[3] Bryan A. Garner, ed., Black's Law Dictionary (9th ed. 2009), sub verbo "signature", en línea: Westlaw Canada.

[4] ING Insurance Co. of Canada v. Jetty, 2010 ONSC 1091 (Div. Ct.).

[5] Ibid. en párr. 8; el caso trataba de un acuerdo de conciliación de una aseguradora que, según la legislación, debía ser firmado tanto por la aseguradora como por la parte asegurada.

[6] Por ejemplo, hacer clic en el icono "Estoy de acuerdo": Rudder v. Microsoft Corp., [1999] OJ No 3778 (SCJ) en párr. 16-17 (por Winkler J. (en ese momento)); Kanitz v. Rogers Cable Inc. (2002), 58 OR (3d) 299 (SCJ) en párr. 31-33.

[7] John Gregory, "A Book Review: Stephen Mason, Electronic Signatures in Law (3d Edition, Cambridge University Press, 2012)" (22 Ago. 2013), www.slaw.ca (blog), disponible en línea: http://www.slaw. ca/2013/08/22/a-book-review-stephenmason-electronic-signatures-in-law-3d-edition-cambridge- universitypress-2012/. Consultar asimismo Druet v. Girouard, 2012 NBCA 40 en párr. 28.

[8] La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996), y Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001), ambas disponibles en línea en: http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce.html.

[9] ULCC, Ley Uniforme de Comercio Electrónico (1999) ("UECA"), disponible en línea en: http://www.ulcc.ca/en/. La UECA en sí misma está basada principalmente en los modelos de leyes de la ONU.

[10] SO 2000, c. 17.

[11] La ECA es sustancialmente similar a las restantes leyes provinciales sobre comercio electrónico. Las diferencias (por lo general menores) entre las leyes provinciales sobre comercio electrónico están más allá del alcance de este breve documento.

[12] ECA, s. 11(1).

[13] ECA, s. 1(1); consultar asimismo la Ley de protección de datos personales y de documentos electrónicos, SC 2000, c. 5 ("PIPEDA"), s. 31.

[14] Black's, supra note 3, sub verbo "electronic signature".

[15] ECA, s. 3.

[16] ULCC, Prof. Michael Deturbide, "Electronic Communications Convention - Impact on common law jurisdictions" (2008), disponible en línea en: http://www.ulcc.ca/en/uniform-acts-new-order/current-uniform- acts/680-uncitralelectronic-communications-convention/1621-convention-on-the-use-ofelectronic-communications-in-international-contracts-impact-on--commonlaw-jurisdictions-2008.

[17] Ver por ejemplo, ECA, s. 31; cabe destacar que algunas provincias han modificado su legislación sobre comercio electrónico para permitir las firmas electrónicas y los documentos electrónicos en conexión con la creación o transferencia de un interés sobre un terreno.

[18] (1988), 25 BCLR (2d) 377 (SC).

[19] Ibid. at para. 21.

[20] Ibid. en párr. 29; consultar asimismo Century 21 Canada Ltd. Partnership v. Rogers Communications Inc. 2011 BCSC 1196 en párr. 65 ("Si bien Beatty trató el uso de documentos enviados por fax, las observaciones de Hinds J. no son menos aplicables... cuando se aplican a la tecnología de internet"). En Re. Buckmeyer Estate,2008 SKQB 141, un tribunal de Saskatchewan (sin referencia a Beatty) encontró que una firma de correo electrónico era una firma válida para el propósito de designar a una parte beneficiaria bajo las leyes provinciales sobre seguros. Se pueden encontrar normas relativas a la admisión de pruebas en la Ley sobre evidencias (Ontario), y equivalentes en la mayoría de las provincias restantes, que por lo general estipulan que los documentos electrónicos pueden tener el mismo valor probatorio que otras pruebas.

[22] Ley sobre aseguradoras, SC 1991, c. 47 ("ICA"); Ley sobre bancos, SC 1991, c. 46; Ley sobre compañías fiduciarias y de préstamos, SC 1991, c. 45; Ley sobre cooperativas de crédito, SC 1991, c. 48 (colectivamente, "leyes FRE").

[23] RSC 1985, c. C-44.

[24] Consultar por ejemplo, ICA, s. 1044.

[25] Consultar por ejemplo, ICA, s. 1037(1).

[26] Se pueden encontrar normas relativas a la admisión de pruebas para documentos electrónicos similares a las que se encuentran en los estatutos provinciales sobre pruebas en la ley canadiense sobre pruebas, RSC 1985, c. C-5.

[27] Consultar por ejemplo ICA, s. 1043 (declaraciones estatutarias y declaraciones juradas). Las firmas electrónicas seguras contemplan requisitos técnicos y de autenticación más estrictos que las firmas electrónicas genéricas; consultar las regulaciones sobre firmas electrónicas seguras, SOR/2005-30, promulgadas bajo PIPEDA.

[28] ICA, ss. 1043, 1044.

OneSpan

OneSpan permite alcanzar el éxito a instituciones financieras y otras organizaciones, al hacer avances audaces en su transformación digital. Conseguimos esto estableciendo confianza en la identidad de las personas, los dispositivos que utilizan, y las transacciones que son determinantes para sus vidas. Creemos que esta es la base de una habilitación de negocios mejorada y de crecimiento. Más de 10.000 clientes, incluyendo más de la mitad de los 100 primeros bancos globales, confían en las soluciones de OneSpan para proteger sus relaciones y procesos comerciales más importantes. Desde la integración digital a la reducción de fraudes, pasando por la gestión del flujo de trabajo, la plataforma unificada y abierta de OneSpan reduce costes, acelera adquisiciones por parte del cliente, y aumenta la satisfacción del cliente.

Este libro blanco no está concebido como asesoría legal o interpretación legal respecto a ESIGN, UETA o cualquier otra ley o regulación. La información aquí presentada tiene únicamente propósitos generales, y no constituye asesoría legal.

CONTACTE CON NOSOTROS
Para obtener más información:
info@OneSpan.com
OneSpan.com/Sign

Lista de verificación de soluciones de firmas electrónicas

La selección de la solución de firma electrónica adecuada para su organización depende de una serie de factores. Comprender los criterios clave y cómo adoptar rápidamente la decisión acertada es esencial a la hora de usar las firmas electrónicas de manera eficaz en sus casos de uso previstos.

	He aquí varias consideraciones para evaluar las diferentes soluciones del mercado, con referencia al Reglamento eIDAS y los requisitos específicos a la UE. Verifique que el proveedor y la solución:
	Cumplen con el último Reglamento eIDAS respecto a firmas electrónicas, AES y QES
	Son compatibles con certificados cualificados basados en la norma X.509, de cualquier TSP
	Son compatibles con certificados del PKI propio de una compañía
	Son compatibles con AES por medio del uso de firmas digitales con sólida autenticación y basadas en servidores para proteger y vincular la firma al documento
	Son compatibles con QES para documentos con varias partes firmantes
	Ofrecen un amplio abanico de opciones de autenticación integradas (p.ej., código por SMS, pregunta secreta, conocimientos, certificados digitales, compatibilidad con sólida autenticación de dos factores con soluciones como Digipass, y más)
	Complementan a las firmas electrónicas, AES y QES con registros auditables duales, como por ejemplo registros auditables estáticos y registros auditables visuales, que ilustran qué se firmó y cómo se firmó
	Crean una firma digital y hash o control para cada parte firmante de la transacción, poniendo el documento a prueba de manipulaciones entre partes firmantes y cumpliendo con los requisitos de PAdES
	Garantizan la integridad del documento directamente desde el documento firmado electrónicamente, independientemente del proveedor de la solución y sin tener que conectar a su servicio
	Ofrecen los idiomas en los que usted opera y hace negocios, tanto para los remitentes como para los destinatarios
	Ofrecen asistencia técnica receptiva y equipos de éxito del cliente que ofrezcan sus servicios a los clientes durante su horario laboral
	Tratan la residencia de datos con opciones de implementación flexibles (p.ej., in situ o en una nube pública o privada en su país o región en la UE)