CUMPLA CON LAS NORMATIVAS LEGALES Y EMPRESARIALES CON EL MAYOR GRADO DE CONFIANZA

En la era de los documentos digitales, la confianza y la identidad son fundamentales

Ahora que los documentos digitales reemplazan cada vez más a los procesos en papel, resulta imperioso trabajar con soluciones de firma confiables, ya que las compañías, los gobiernos y las personas necesitan conocer con certeza la identidad de las organizaciones y los individuos con los que interactúan para evitar los riesgos de manipulación o fraude en las transacciones, los acuerdos y los contratos.

DigiCert Document Signing Manager valida las identidades y brinda confianza

Aunque muchas soluciones pregonen la seguridad de la firma de documentos, no da igual una herramienta que otra. DigiCert Document Signing Manager está integrado en la infraestructura de clave pública, una tecnología de cifrado, autenticación e identidad de probada eficacia. Esta solución no solo firma los documentos con una identidad criptográficamente segura, sino que permite que cualquier persona que los lea sepa quién los firmó y se asegure de que los documentos no fueron alterados.

¿Qué es un proveedor cualificado de servicios de confianza?

Las normas que establecen la Unión Europea y el Instituto Europeo de Estándares Técnicos (ETSI, por sus siglas en inglés) en materia de servicios de firma son la referencia más confiable a nivel mundial para la seguridad y la identidad de las firmas. El mayor nivel de seguridad en este estándar son los proveedores cualificados de servicios de confianza (QTSP, por sus siglas en inglés). Como parte de la adquisición de QuoVadis, la UE y el ETSI certifican que DigiCert cumple con los estándares de firma dispuestos en la normativa de eIDAS, lo que lo convierte en uno de los pocos QTSP selectos a nivel mundial. Además, DigiCert cumple con todos los requisitos de las firmas cualificadas en Suiza, según la Ley Suiza de Firmas (ZertES).

De hecho, la firma de documentos que ofrecen DigiCert y QuoVadis equivale a una firma manuscrita y, en muchos países, representa una prueba de identidad equivalente a una forma de identificación gubernamental.

En su carácter de QTSP, DigiCert ofrece soluciones de firma que satisfacen y superan los estándares de seguridad, autenticación e identidad más estrictos del mundo.

Distintos niveles de seguridad para cada tipo de documento

Las firmas digitales reconocidas varían en términos de requisitos y validación según el grado de seguridad que necesite la persona u organización.

Tipo de firma	Firma electrónica básica o estándar (SES)	Firma digital avanzada (ADS/AATL)	Firma digital electrónica cualificada (QES)
Requisitos de la firma	Esta es una firma electrónica que un signatario incluye en un documento como prueba de su aceptación o aprobación. Puede incluir la incorporación de una imagen escaneada de la firma o la selección del botón «Acepto».	Esta es una firma digital que cumple con requisitos específicos y que brinda un mayor grado de seguridad, integridad y verificación con respecto a la identidad del signatario.	Esta es una firma digital que cumple con requisitos avanzados, que cuenta con el respaldo de un QTSP de la Lista de confianza de la Unión Europea y que está certificada por un estado miembro de la UE o por un QTSP de la Lista de confianza de Suiza. Por lo general, se usa como equivalente de una firma manuscrita.
Requisitos de seguridad y validación de la identidad	Ninguno	La firma debe estar vinculada a un único signatario. El signatario puede identificarse con un documento gubernamental, pero esto no está garantizado. La firma se crea con los datos de identidad específicos bajo el control exclusivo del signatario. La firma está vinculada a los datos firmados, en los cuales se puede detectar si se producen cambios. La firma cumple con los requisitos de la Lista de confianza aprobada por Adobe (AATL).	El QTSP debe establecer la integridad y autenticidad del signatario: 1. Los datos de la creación de la firma electrónica son seguros y confidenciales. 2. El QTSP puede probar la identidad del signatario en un encuentro cara a cara o mediante un proceso de verificación con un grado de seguridad similar.
Ejemplos	Firma de documentos por parte de los empleados al momento de su incorporación a la plantilla Acuerdos comerciales entre entidades corporativas Convenios con consumidores Acuerdos de licencia de software	Acuerdos de préstamo o crédito para consumidores Contratos laborales colectivos Contratos laborales entre agentes y empleados	Contratos de alquiler, transferencia o compra de bienes raíces Documentos relacionados con la ley de familia Incorporación de una sociedad de responsabilidad limitada
Nivel de seguridad de eIDAS	Seguridad baja	Seguridad considerable	Seguridad alta
Nivel de validación	Sin validación	Cierto grado de validación	Validación máxima (rigurosa)

Dos maneras de firmar

Firma individual (firma electrónica)

Una persona física, en carácter de signatario individual, puede firmar diferentes documentos de forma fácil y segura, como contratos personales para la compraventa de inmuebles, la apertura de una cuenta bancaria o el almacenamiento de información confidencial (p. ej., historias clínicas).

Firma organizativa (sello electrónico)

En el caso de las empresas y los gobiernos, una persona jurídica, en carácter de signatario organizativo, puede firmar en nombre de la empresa o entidad —e incluso firmar documentos de forma masiva— y, al mismo tiempo, garantizar la integridad de los archivos.

Ventajas de la firma de documentos

Permita que sus clientes firmen los documentos de manera digital en cualquier momento y lugar. Nuestra solución integral incluye certificados, avances tecnológicos y opciones de automatización que suponen una fuerte ventaja competitiva y optimizan la experiencia de los clientes.

Funciones

Procesos de firma personalizados
Desarrolle procesos completos con varias opciones de tecnología, como Ascertia SigningHub, Adobe Acrobat Sign o DocuSign.

Validación sencilla
Permita que sus clientes creen una identidad segura de forma remota en cuestión de minutos por medio de Verify de DigiCert, que cuenta con la tecnología de IDnow.

Gestión de claves simplificada
Proteja las claves en un dispositivo cualificado de creación de firmas que se aloja en un entorno de confianza.

Administración optimizada
Simplifique la gestión que llevan a cabo los administradores con una política y un control centralizados para los usuarios finales y los signatarios.

Seguimiento detallado
Acceda a informes y registros de auditoría en relación con la política de su empresa o la reglamentación gubernamental.

Mayor seguridad
Refuerce la seguridad con diferentes opciones de autenticación de dos factores (2FA).

Integración fácil
Incorpore distintos servicios web y procesos de terceros, como Adobe Acrobat Sign, Ascertia SigningHub y muchos más.

Opciones de implementación flexibles
Implemente una solución alojada o local.

Principales ventajas

- Reduzca el costo que suponen el uso de papel, las tareas administrativas y los procesos de envío.
- Simplifique los requisitos de firma o incorporación para mejorar la experiencia de los clientes y afianzar su fidelidad.
- Disminuya la duración de las transacciones de firma de días a minutos.
- Refuerce la seguridad de las transacciones en las que intervengan grandes sumas de dinero.
- Genere confianza con firmas que tienen validez legal.
- Garantice la continuidad de los negocios y desarrolle una ventaja competitiva.
- Cumpla con las regulaciones internacionales y las normas del sector.

Especificaciones técnicas e integraciones

Protocolos de firma digital

- API de REST
- API de CSC

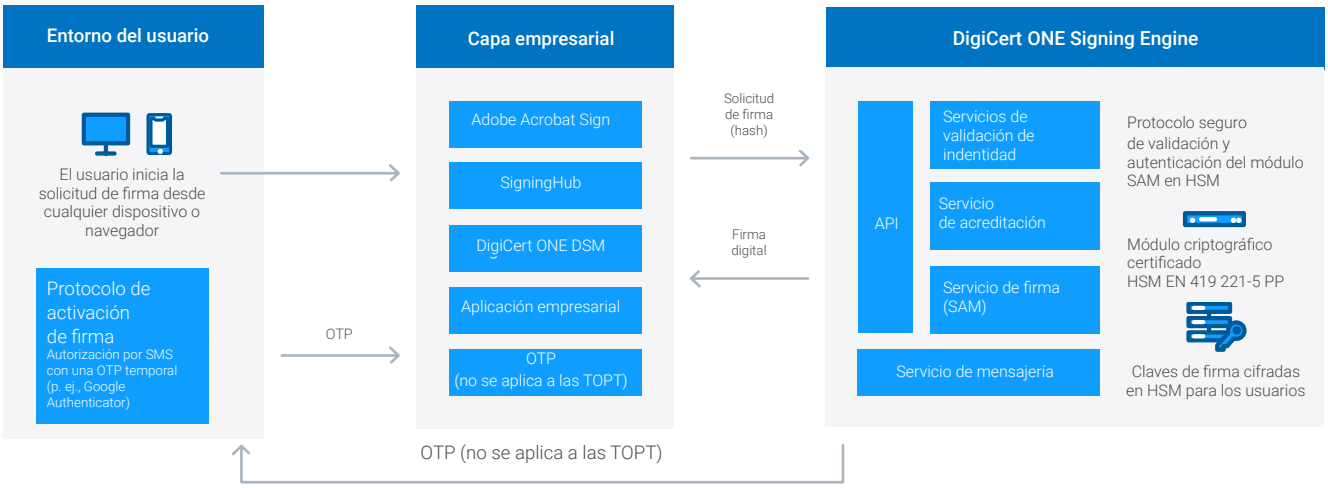
Integraciones disponibles

- Adobe Acrobat Sign
- Ascertia SigningHub
- DocuSign

Soluciones compatibles

- Microsoft Office®
- Adobe® Acrobat y Adobe Reader
- LibreOffice®
- OpenOffice™
- Otras soluciones de terceros, como DocuSign
- Diversos tipos de documentos, incluidos PDF, ODF, DOCX y XML

Arquitectura de firma remota basada en la nube



DigiCert® ONE

Document Signing Manager forma parte de DigiCert ONE, un modelo integral y moderno para la gestión de PKI. Este modelo, desarrollado en una arquitectura avanzada y basada en contenedores, le permite realizar implementaciones rápidas en cualquier tipo de entorno, lanzar nuevos servicios en menos tiempo y gestionar a los usuarios y los dispositivos de toda su organización a cualquier escala.

Si desea obtener más información sobre DigiCert® Document Signing Manager, envíe un correo electrónico a docsigning@digicert.com para comunicarse con uno de nuestros expertos en PKI para documentos.

Líder de confianza en PKI

DigiCert surgió del deseo de proteger mejor Internet y, desde entonces, ha sido fiel a ese espíritu. Por eso nuestros certificados inspiran confianza en todas partes, millones de veces al día, y son los favoritos de empresas de todo el mundo. Por eso las reseñas de nuestros clientes sobre nuestros servicios y asistencia son las que reciben más calificaciones de cinco estrellas del sector, encuesta tras encuesta. Y por eso seguiremos siendo punteros en nuestro campo, en aras de un futuro más seguro e innovador. En cuestión de soluciones de SSL, IoT, PKI —por poner solo unos ejemplos—, DigiCert ofrece algo único. Somos, en definitiva, lo opuesto al denominador común.