



NUESTRO ÉXITO EMPIEZA CONTIGO



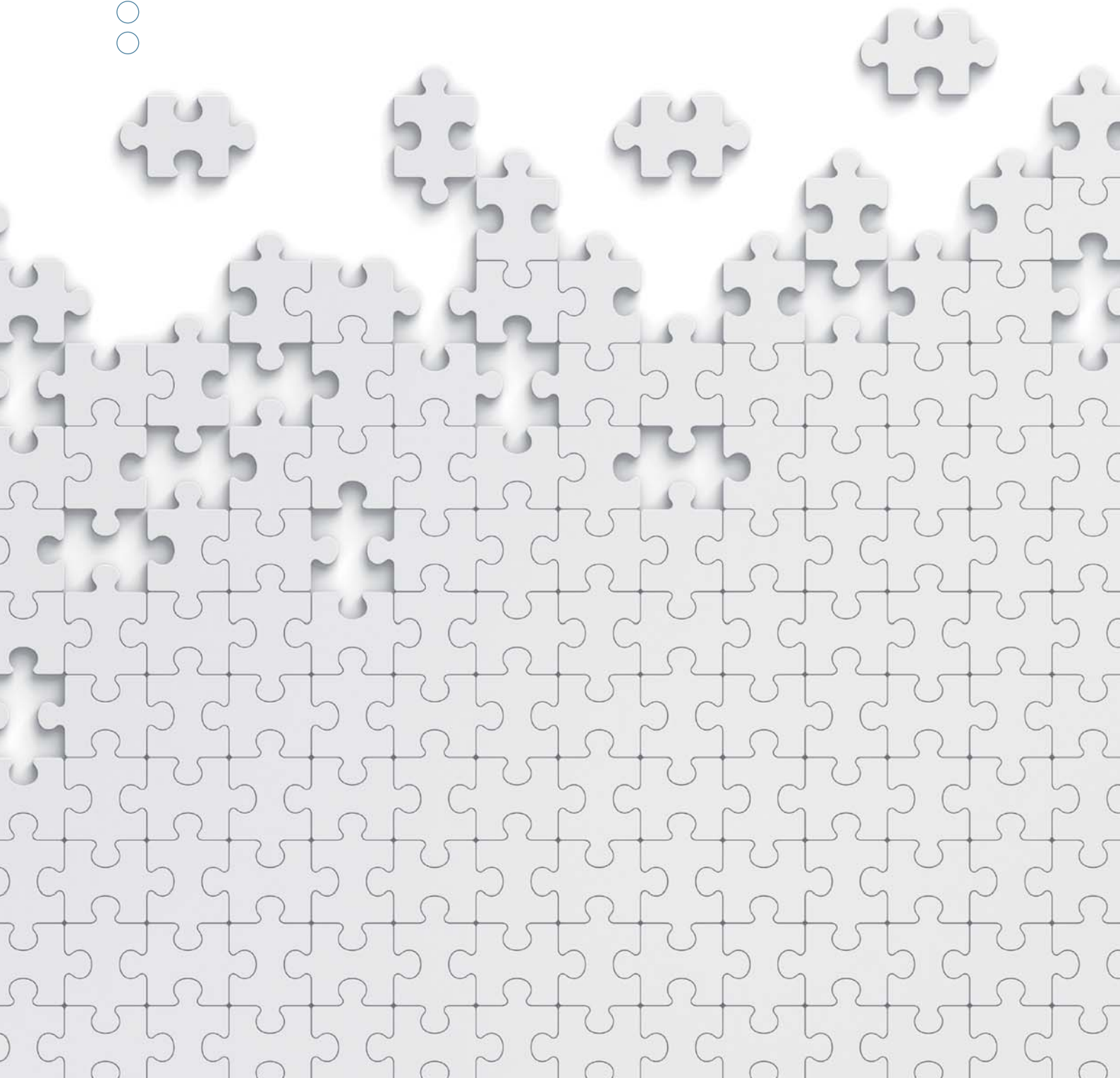
service provider | supply chain management...



SOA | application
outsourcing | SOA | application
... outsourcing | SOA | application

... xml/edi | customer efficiency response | value added network | edifact | business intellig

ediwin | xbrl |
ebi mapping tool | edicom business integrator | odette | X12 ..



NUESTRO ÉXITO EMPIEZA CONTIGO

Para nosotros solo existe una forma de entender nuestro trabajo, y es poniéndonos en la piel de nuestros clientes y usuarios.

Especialistas en consultoría y desarrollo de software para la transmisión e integración de datos, desde EDICOM diseñamos sistemas transaccionales de alto rendimiento destinados a cubrir las necesidades de proyectos e-commerce B2B. Soluciones de desarrollo propio que en poco más de una década se han posicionado como una referencia que ha incrementado el valor de las transacciones de miles de clientes en todo el mundo.

Para lograrlo, nos hemos especializado en ti, en tus necesidades, en tus expectativas, en tu negocio... Para que no tengas que preocuparte de la instalación, gestión y actualización de avanzados sistemas, que desde EDICOM desarrollamos, implantamos y mantenemos bajo estrictas políticas de servicio y orientación total al cliente.

Y es que el éxito de cada uno de nuestros proyectos empieza contigo. Con tus sugerencias, con tus ideas, pero sobre todo con tus decisiones. Decisiones que impulsan a tu negocio hacia avanzados modelos, que constituyen toda una garantía para lograr las más altas cotas de excelencia en tu gestión.

SEDES EDICOM

- VALENCIA
- MILANO
- PARIS
- NEW YORK
- SÃO PAULO
- MEXICO D.F.
- BUENOS AIRES

algunos de nuestros clientes...

Retailers

El Corte Inglés, Carrefour, Harrods, Leroy Merlin, Toys 'R' Us, Delhaize, Dia, Douglas, Alcampo, Ahorramás, Aki, Intersport, Sephora, Consum, Eroski, Makro, Cortefiel, Mercadona, Fnac, Media Markt, Conforama, Gruppo Pam, Esselunga, Cisolfa, Grupo Expert, Printemps, Galeries Lafayette, C1000 BV, Bon Preu, Inditex...

Fabricantes

Unilever, Bonduelle, Energizer, Red Bull, Heinz, Saint Gobain, Schweppes, Bic, Bandai, L'Oreal, Kellogg's, Kimberly Clark, Reckitt Benckiser, Procter & Gamble, Tommy Hilfinger, Guess, Arbona & Ausonia, Valentino, Nintendo, MaxMara, Ferrero, Giochi Preziosi, BioCentury, Adolfo Dominguez, Vodafone, Tod's, Rip Curl, Aubade, Nutrexp, Loewe, Samsonite, Microsoft, Danone, Hans Grohe, Coronel Tappioca, Kraft, Bourjois, Sony, Billabong, Riso Gallo, Replay, Star, 3M, Estee Lauder, Candy Hoover, General Mills, Antonio Puig, Sunpower, American Apparel, Desigual, Michael Kors, FrieslandCampina,...

Logística y Transporte

Kuehne & Nagel, Gefco, Transaher, Norbert Dentressangle Gerposa, DHL Exel, Movianto, Dispatching, Corriere Cecchi, Ochoa, Azkar, Cargo Depot, Carreras, Cat, Logista, FCC, Exel Logistics, Aldeasa, Sitrans Entrepósito, ID Logistics, Transcommerce Net, Hermes, Logisargo, Rhenus Tetras, Snatt Logistica, SDF Iberica, TNT Express, Transnatur...

Automoción

Norauto, Feu Vert, Midas, Daimler Chrysler, Nissan, Arcelor Mittal, Pirelli, Gestamp, Ficos, Durex, Showa Europe, Rubi,

Kayaba, Ruffini, Fujitsu Ten, Good Year, Michelin, Magna Electronics, Denso, Daimler Chrysler, TRUMPF GmbH + Co. KG, Mercedes-Benz ESPAÑA, S.A.

Sanidad

Servicios Centrales de salud: Servicio Valenciano, IB-Salut, Osakidetza, SAS...

Proveedores: Roche, GlaxoSmithKline, Pfizer, Novartis, Boehringer Ingelheim, Lilly, Bristol-Myers, Abbot, Becton Dickinson, Sanofi-Adventis, Novartis, Grifols, Alter, Bayer, Pierre Fabre, Cofares, Alliance Healthcare, Cecofar, Federación Farmacéutica, Novafar, Hefame, Hospira, Mead Johnson, Biomet...

Turismo

Viajes El Corte Inglés, Viajes Barceló, Carlson Wagonlit España, Logitravel, Catai,

Beds Online, Costa Crociere, Avis, Ibero Cruceros, Pullmantour Cruises, NH, Europcar, Atesa, Hertz, Marina D'Or, Insignia Hoteles, Sport Hoteles...

Medios y Publicidad

El País, Box News, Unión Radio (Cadena Ser, 40 Principales, M80,...), Santillana, Media Planning, Anaya, Edebe, Planeta de Agostini, Dom Quixote, SGEL (Relay), Random House Mondadori, Everest, Espasa Calpe, Europa Press...

Finanzas

Cesce, Mapfre, Nacional Financiera, Caixa Laietana, Inverseguros Gestión, Banca Inbursa...

Administración Pública

Ministerio de Economía y Hacienda, Generalitat Valenciana, Ayuntamiento de Valencia, INVASSAT...



¿POR QUÉ UNA AUTORIDAD DE CERTIFICACIÓN?

LA CONFIANZA COMO ELEMENTO CLAVE EN LAS TRANSACCIONES ELECTRÓNICAS

Las transacciones electrónicas de todo tipo que realizamos con clientes, bancos, proveedores o administraciones públicas son una realidad que suponen millones de comunicaciones diarias con interlocutores de todo el mundo.

Las órdenes de compra, facturas, avisos de expedición, contratos, etc., son transacciones a menudo sensibles y de gran importancia, que requieren la puesta en servicio de diferentes tecnologías para la adecuada creación de los mensajes, su envío y recepción.

Es precisamente la sensibilidad e importancia que rodea a estas comunicaciones, la que hace necesaria la adopción de sistemas que además garanticen su **seguridad, confidencialidad e integridad**. Cuestiones éstas a las que se da respuesta mediante las técnicas de encriptación que ponen en servicio los procesos normalizados de Firma Electrónica gestionados a través de las Autoridades de Certificación.

La Autoridad de Certificación EDICOM (ACEDICOM) proporciona a personas físicas y jurídicas, los mecanismos de identificación electrónica segura que les permiten realizar actividades en donde la firma electrónica sustituye a la manuscrita con idénticas garantías jurídicas.

La ACEDICOM se integra dentro de la infraestructura de servicio ofrecida por EDICOM. De esta forma, a nuestras soluciones de mensajería y comunicaciones, añadimos los mecanismos que permiten a nuestros usuarios el intercambio de mensajes electrónicos de forma segura, íntegra y confidencial.

Los certificados expedidos por la Autoridad de Certificación EDICOM, se ajustan a lo establecido en la Directiva 1999/93/CE de 13 de diciembre, y a la Ley 59/2003 de 19 de diciembre de firma electrónica, por lo que gozan de amplio reconocimiento para operar en toda la Unión Europea.



DIGITAL SIGNATURE

LA FIRMA ELECTRÓNICA ¿QUÉ ES Y PARA QUÉ SIRVE?

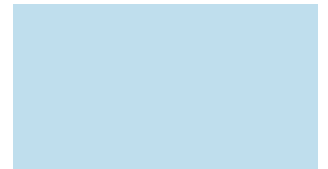
Los mensajes electrónicos se ven afectados por 3 grandes problemas: La **confidencialidad**, la **integridad** y la **autenticidad**.

- **Confidencialidad:** Se refiere a la capacidad de mantener un documento electrónico inaccesible a todos, excepto a los destinatarios a los que se dirige el mensaje.
- **Integridad:** Garantiza que el documento recibido coincide con el documento emitido sin posibilidad alguna de cambio.
- **Autenticidad:** Se refiere a la capacidad de determinar si una persona ha establecido su reconocimiento y compromiso sobre el contenido del documento electrónico.

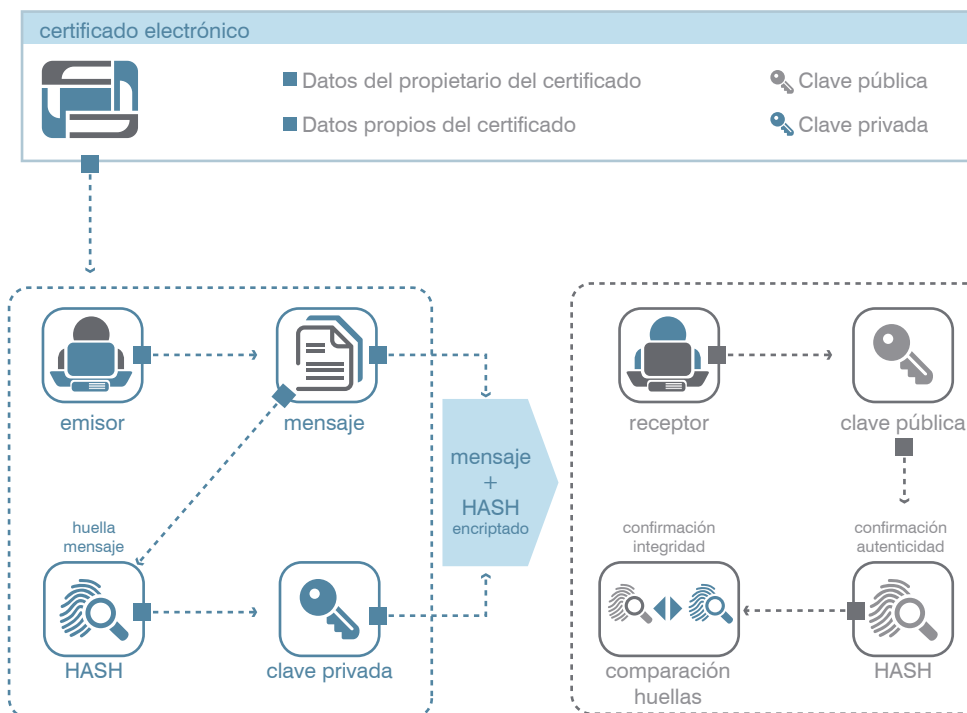
El problema de la autenticidad en un documento tradicional se soluciona mediante la firma manuscrita. Con ella, un individuo o varios manifiestan su voluntad de reconocer el contenido de un documento, y en su caso, el compromiso de cumplimiento de las obligaciones y acuerdos establecidos en él.

En el entorno de los mensajes electrónicos, a los problemas de confidencialidad, integridad y autenticidad se les da respuesta a través de la criptografía:

- La cuestión de **confidencialidad** se soluciona mediante las denominadas técnicas de cifrado.
- A las de **integridad y autenticidad** se les da cobertura a través de las técnicas de firma digital.



- El emisor obtiene un resumen o HASH del documento que establece una huella única del mensaje. Si el mensaje se modifica mínimamente esta huella cambia.
- Este HASH es encriptado con la clave privada del emisor.
- El receptor recibe el mensaje y el HASH encriptado.
- Con la llave pública del emisor lo desencripta. Si el proceso se realiza con éxito se puede garantizar el origen del mensaje (el mensaje es auténtico)
- Paralelamente el receptor aplica al mensaje el mismo algoritmo de HASH que el emisor. La huella obtenida se compara con la huella "desencriptada" y si son iguales, se verifica que el mensaje no ha sido modificado (el mensaje es íntegro)



digitalCertificates

Un certificado digital es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Para ello el solicitante es acreditado de forma rigurosa por la Entidad de Certificación quedando vinculado unívocamente al Certificado y por tanto dotándole de un identificador electrónico único, lo que le permitirá realizar todo tipo de transacciones electrónicas que requieran de autenticación.

Los certificados deben ser emitidos por una Autoridad de Certificación Acreditada, integrada en una PKI (public key infraestructure) o infraestructura de clave pública.



UTILIDADES DE LOS CERTIFICADOS DIGITALES

Firma digital

El certificado se utiliza para firmar todo tipo de documentos digitales, desde simples e-mails hasta los más complejos contratos mercantiles. Esto implica garantía de no repudio, de conocimiento inequívoco de quien es el emisor del documento y de la integridad del documento.

Seguridad en la comunicación

El certificado sirve para codificar una comunicación entre dos personas, haciendo que toda la información transmitida sea confidencial. Con ello se garantiza que cualquier documento enviado por una persona a otra estará cerrado y sólo podrá ser abierto por su legítimo destinatario.

En algunos países, la legislación permite sustituir un original en papel por su equivalente digital, conservando idénticas garantías jurídicas siempre que se observen determinados procedimientos, por lo general, vinculados a firma electrónica.

Digitalización Certificada

Permite conocer la identidad en el momento de entrar en un espacio físico o digital, permitiendo o denegando accesos y dejando constancia de los mismos.

Identificación personal

El certificado digital es utilizado para firmar software. Esto permite a la entidad que va a utilizar el software garantizar que este es el original, conocer quién lo ha creado, y muy importante, que con posterioridad a su firma, nadie lo ha modificado.

Firma de Software

Edicom se constituye en Entidad Certificadora con el objetivo de proveer a sus clientes de los elementos de identificación específicos a la actividad concreta a realizar, evitando certificados generalistas y garantizando el cumplimiento de la legalidad en su interpretación más estricta, como en el caso de los dispositivos seguros, que gozan de la certificación CWA 14169.

La ACEDICOM expide certificados reconocidos para ser utilizados en dispositivos seguros así como certificados de software.

digitalCertificates

CERTIFICADOS RECONOCIDOS DE FIRMA SOBRE DISPOSITIVO SEGURO CENTRALIZADO

Los certificados reconocidos de creación de firma sobre dispositivo seguro centralizado emitidos por la Autoridad de Certificación de Edicom no se entregan físicamente en ningún soporte, ya que por su propia naturaleza, se generan en el mismo dispositivo que los alojará y sobre el cual se prestarán los servicios de firma.

Los dispositivos centralizados de creación de firma de EDICOM, gozan de la certificación CWA 14169, garantizando el cumplimiento de la legalidad en su interpretación más estricta.

CERTIFICADOS RECONOCIDOS DE FIRMA SOBRE DISPOSITIVO SEGURO "SMART CARD" Ó TOKEN USB

Estos certificados se entregan sobre la tarjeta criptográfica que mantiene el material sensible criptográfico siempre dentro de la tarjeta, y protege su uso mediante control de acceso, no pudiendo en ningún caso extraer la clave privada. Adicionalmente se proporciona un dispositivo lector de tarjeta SIM con USB para tarjetas inteligentes con formato plug-in (SIM card).

Al igual que los sistemas centralizados, se trata de dispositivos seguros con acreditación CWA 14169.

CERTIFICADOS RECONOCIDOS DE FIRMA SOBRE SOPORTE SOFTWARE

Los certificados electrónicos de creación de firma sobre soporte software, se entregan en ficheros electrónicos que pueden ser descargados en discos duros o memorias usb, no requiriéndose el uso de dispositivos externos para la generación de firmas a partir de ellos. Se trata por tanto de certificados con diferente nivel de seguridad, si bien los mismos pueden ser válidos para su uso en multitud de transacciones.

CERTIFICADOS TLS (Transport Layer Security) DE CLIENTE Y SERVIDOR

A diferencia de los anteriores, se trata de certificados "No Reconocidos" por lo que no se requiere de la presencia de su titular ante la autoridad de Registro de Edicom para su emisión y pueden ser de dos tipos:

Certificados de cliente: Se expiden a personas físicas y pueden servir para autenticación en sistemas operativos (opcional en soporte smart card o token usb) y seguridad en Emails

Certificados de servidor: se expiden a nombres de dominio para autenticación de servidor en servicios SSL (https), también pueden servir para seguridad en túneles IPSEC



■ La expedición de los Certificados Reconocidos EDICOM requieren de la personación de su titular ante la autoridad de Registro Edicom para garantizar la identidad de la persona física o jurídica a nombre de quien se expedirá el certificado.

VIGENCIA DE LOS CERTIFICADOS	Sin Limitación de Uso	Con Limitación de Uso	...limitaciones...
Certificado reconocido sobre dispositivo seguro centralizado	4 AÑOS	4 AÑOS	<ul style="list-style-type: none"> › Firma de facturas electrónicas › Firma de documentos con almacenamiento certificado
Certificado reconocido sobre dispositivo seguro "smart card"	2 AÑOS		
Certificado reconocido sobre soporte software	2 AÑOS	2 AÑOS	<ul style="list-style-type: none"> › Controles de acceso › Firma de documentos comerciales y tributarios › Otras limitaciones
Certificado TLS de Cliente y Servidor	2 AÑOS		

SERVICIO DE FIRMA REMOTA EDICOM CRIPTO SERVER

El servicio de Firma Remota de EDICOM “EDICOM CRYPTO SERVER (ECS)” permite realizar firma electrónica reconocida con certificados almacenados en dispositivos seguros de firma (SSCD), alojados en las instalaciones de EDICOM, a través de un interfaz WebService sobre HTTPS.

El servicio ECS utiliza a su vez los siguientes servicios de EDICOM relacionados con la seguridad y firma electrónica:

- Entidad certificadora ACEDICOM para la generación de certificados reconocidos.
- Servicio de TimeStamp (TSA) para realizar sellado de tiempo.
- Servicio OCSP para información de revocación de certificados.

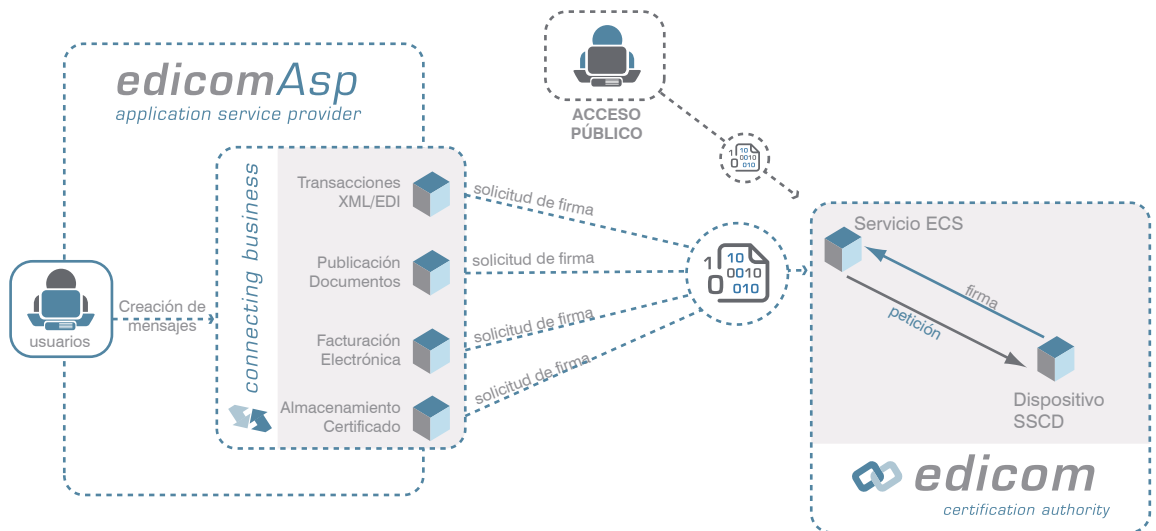
Mediante ECS la tecnología de firma electrónica reconocida mediante dispositivos seguros tipo smartcards o HSM queda totalmente solucionada y sin ninguna complicación añadida para el software cliente, pasándole por tanto la responsabilidad de la gestión o el acceso a estos dispositivos al propio ECS con todas las ventajas de administración que ello conlleva para el cliente, ya que no debe preocuparse por la seguridad física del dispositivo de firma.

Este servicio le exime igualmente de la complejidad técnica del acceso concurrente a dicho dispositivo de firma desde múltiples sitios.

■ El servicio ECS (Edicom Crypto Server) permite operaciones criptográficas de firma en una arquitectura cliente servidor, bien desde dentro del entorno ASP de EDICOM (intranet privada) o desde Internet (acceso público).

■ Todos los pares de claves se encuentran almacenados en el dispositivo seguro centralizado SSCD. La generación de estas claves es un proceso totalmente ajeno a ECS y sigue los procedimientos operativos correspondientes de la Autoridad de Certificación ACEDICOM.

■ Existen 2 niveles de autenticación: Uno a nivel del servicio que permite el acceso a EDICOM CRYPTO SERVER, y otro con el dispositivo seguro de firma SSCD que incluye el PIN asociado a la clave privada.



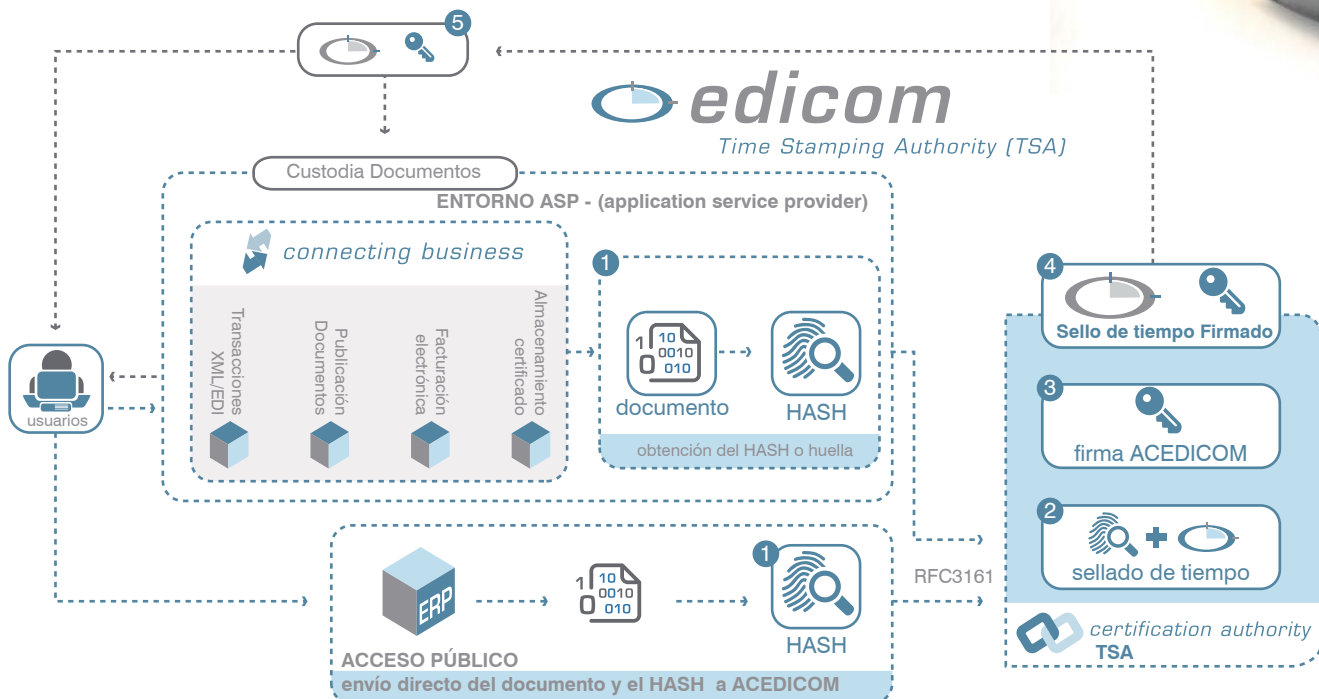
En los procesos de firma de documentos electrónicos, los usuarios pueden optar adicionalmente, y siempre y cuando sea procedente, por el **Servicio de Firma Delegada**. Este servicio se diferencia con el de Firma Remota, en que los documentos generados por el usuario son firmados con un certificado expedido a nombre de EDICOM.

De esta forma, el emisor autoriza a Edicom a firmar dichos documentos en su nombre, eximiéndole del mantenimiento y gestión de certificados electrónicos a su propio nombre.

SERVICIO DE SELLADO DE TIEMPO (Time Stamping)

Con el sellado de tiempo (Timestamping) es posible demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Una Autoridad de Sellado de Tiempo como Edicom, actúa como tercero de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

Funcionamiento del servicio:



El proceso se inicia por parte del cliente que desea obtener el sello de tiempo para un determinado documento:

- 1 La aplicación del cliente debe obtener el "resumen", "huella" o HASH del documento, y realiza una petición de sellado de tiempo según el protocolo RFC3161. Esta petición puede realizarse automáticamente a través de las soluciones de integración EDICOM, y sus servicios de transformación, cálculo de HASH o comunicaciones Web Services, accediendo a través de nuestro entorno ASP.
- 2 Recepcionado el mensaje (con el HASH del documento), se le aplicará el sello de tiempo. Para ello el servicio dispone de una fuente de tiempo sincronizada con la Escala de Tiempo Universal (UTC).
- 3 Se le añade la firma de EDICOM en calidad de Autoridad de Certificación, así como su certificado.
- 4 El sello de tiempo firmado es devuelto al cliente. En este punto, EDICOM ofrece su servicio de custodia de documentos para el almacenamiento de originales en plataformas de alta disponibilidad.
- 5

- El protocolo para el Sellado de Tiempo se describe en el RFC 3161 y está en el registro de estándares de Internet.
- El Sello de Tiempo es verificable por cualquiera y certifica la existencia de un documento en el instante que indica el sello.
- La existencia de un sello de tiempo, verifica que el documento original no ha sido alterado desde su presentación.

certified Storage

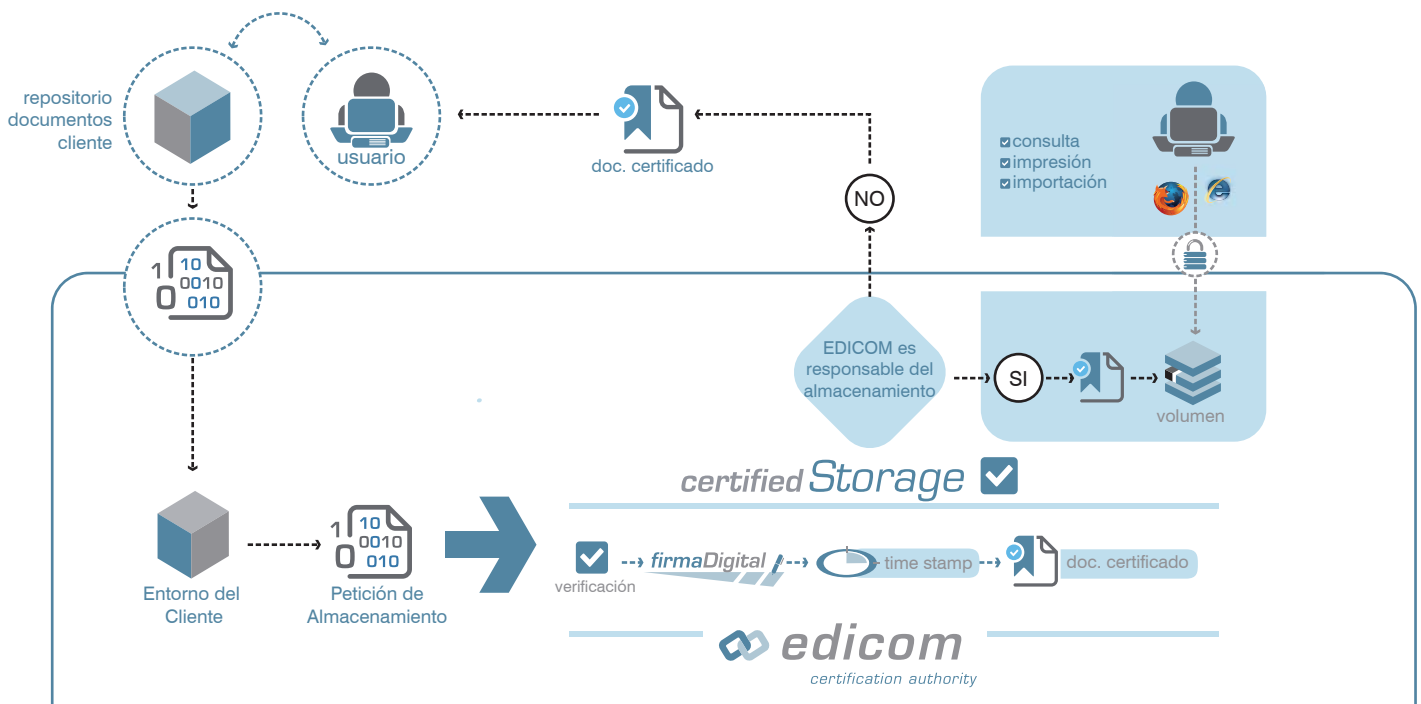
ALMACENAMIENTO CERTIFICADO

En cualquier tipo de empresa se reciben y producen a diario gran cantidad de documentos, que derivan en una demanda creciente que solicita un resguardo digital de éstos que pueda realizarse sin menoscabo de la seguridad y garantías aportadas por los documentos originales en papel.

Estos documentos almacenados por medios electrónicos podrían ser originales creados desde el principio en formato electrónico, pero también documentos en papel, sometidos a un proceso de digitalización que permitiera la sustitución de los mismos por los correspondientes archivos que contengan las imágenes gráficas equivalentes.

■ En algunos países, la legislación permite sustituir un original en papel por su equivalente digital conservando idénticas garantías jurídicas.

■ Tras la realización de procesos vinculados a la firma electrónica, en aquellos casos en los que la legislación lo permite, se puede destruir el archivo físico de documentos originales, teniendo equivalencia jurídica el archivo del Repositorio de Documentos Certificados de EDICOM.



SEGURIDAD



EDICOM se compromete a mantener las medidas de seguridad lógicas y físicas necesarias para garantizar la adecuada prestación del servicio en sus instalaciones, y a estar alineado con los estándares de seguridad vigentes en cada momento como por ejemplo ISO27001.

- El usuario realiza una petición de almacenamiento, remitiendo los documentos a procesar a EDICOM a través de su entorno de trabajo en nuestra Plataforma Tecnológica.
- La Autoridad de Certificación EDICOM recibe la petición y revisa si está completa. Realiza un control de acceso en función del usuario y password del cliente, y verifica la solicitud.
- El Servicio de Almacenamiento Certificado de la Autoridad de Certificación, firma el documento e incluye un sello de tiempo. De esta forma cualquiera que consulte el documento a partir de este momento, puede verificar su integridad desde el momento exacto en el que se realizó el proceso de certificación.
- Tras el proceso de verificación, firma y sellado de tiempo, se inserta el documento en el repositorio para su conservación y posterior consulta.



ESPAÑA

Parque Tecnológico de Paterna
C. Charles Robert Darwin 8
46980 Paterna (Valencia)
Tel. 902 119 228 | +34 961 366 565
Fax. +34 961 367 117
info_spain@edicomgroup.com

ITALIA

Centro Direzionale Milanofiori
Viale Milanofiori
Strada 1 Palazzo F1
20090 Assago. Milano
Tel. +39 02 0064 0402
Fax. +39 02 0064 0410
info_italy@edicomgroup.com

FRANCIA

23-25 Rue de Berri
75008 Paris
Tel. +33 (0) 820 360 330
Fax. +33 (1) 53 76 26 87
info_france@edicomgroup.com

USA

152 Madison Avenue Suite 1900
New York NY 10016
Tel. +1 212 889 1909
Fax. +1 212 889 1947
info_usa@edicomgroup.com

BRASIL

Rua Frei Caneca 1380 - 8º andar.
CEP.01307-002 | São Paulo
Tel. +55 (11) 3154-5100
Fax. +55 (11) 3251 3369
info_brazil@edicomgroup.com

MÉXICO

Torre del Ángel
Paseo de la Reforma No 350 Piso 16-B
Colonia Juárez
06600 Cuauhtémoc | México D.F.
Tel. 01 800 841 0241
Tel D.F. +52 (55) 52 12 15 66
Fax. +52 (55) 11 62 04 04
info_mexico@edicomgroup.com

ARGENTINA

Lola Mora 421 - Oficina 801
1107 - Puerto Madero Este | Buenos Aires
Tel. +54 (11) 5245 8410
info_argentina@edicomgroup.com
info_chile@edicomgroup.com