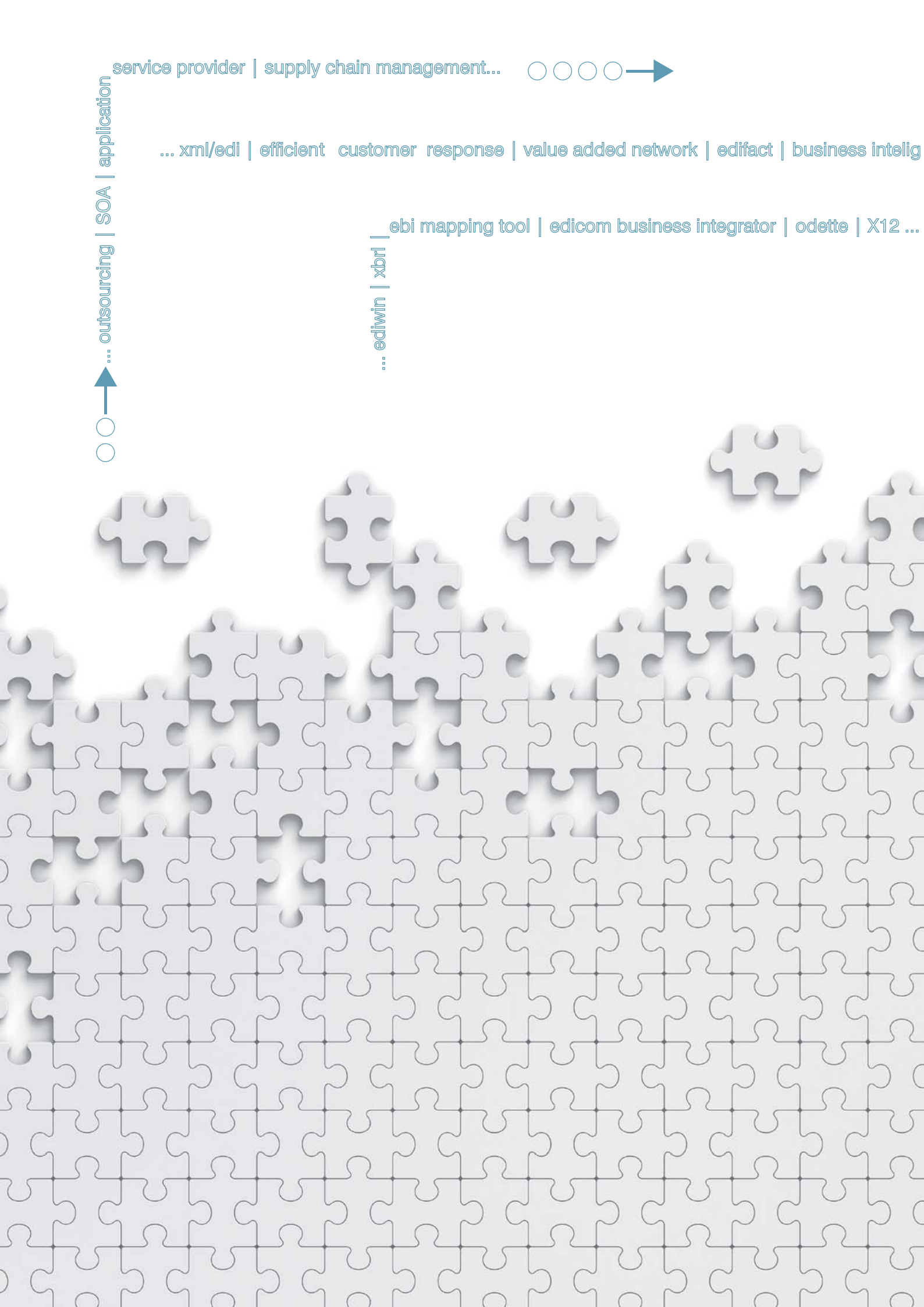
# CA · edicom

certification authority

OUR SUCCESS BEGINS WITH YOU

edicom

connecting business


service provider | supply chain management...
... xml/edi | efficient customer response | value added network | edifact | business intelig
ebi mapping tool | edicom business integrator | odette | X12 ...
... ediwin | xbrl |
... outsourcing | SOA | application

edicom
connecting business

## OUR SUCCESS BEGINS WITH YOU

For us there is only one way to understand our work, and that is by putting ourselves in the shoes of our clients and users.

Specialists in data transmission and integration software consulting and development, at EDICOM we design high performance transactional systems designed to cover the needs of B2B e-commerce projects. After over a decade, our own development solutions are now positioned as a reference that has increased the value of the transactions of thousands of clients worldwide.

To achieve this, we have specialized in you, your needs, your expectations and your business... so that you don't have to worry about the installation, management and updating of advanced systems. At EDICOM we develop, implement and maintain our systems under strict service policies with a total focus on the client.

The success of each of our projects begins with you. With your suggestions, your ideas, but mainly with your decisions. Decisions driving your business towards advanced models, which constitute a full commitment to achieve the highest levels of excellence in your management.

OFFICES EDICOM

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

## some of our customers...

**Retailers**
El Corte Inglés, Carrefour, Harrods, Leroy Merlin, Toys 'R' Us, Delhaize, Dia, Douglas, Alcampo, Aki, Intersport, Sephora, Consum, Eroski, Makro, Cortefiel, Mercadona, Fnac, Media Markt, Conforama, The Singular Kitchen, Gruppo Pam, Esselunga, Cisalfa, Grupo Expert...

**Manufacturers**
Unilever, Bonduelle, Energizer, Red Bull, Heinz, Saint Gobain, Schweppes, Bic, Bandai, L'Oreal, Kellog's, Kimberly Cark, Reckitt Benckiser, Procter & Gamble, Tommy Hilfiger, Guess, Arbora & Ausonia, Valentino, Nintendo, MaxMara, Ferrero, Giochi Preziosi, BioCentury, Adolfo Dominguez, Vodafone, Tod's, Rip Curl, Aubade, Nutrexpa, Loewe, Samsonite, Microsoft, Danone, Hans Grohe, Coronel Tappioca, Kraft, Bourjois, Sony, Billabong, Riso Gallo, Replay, Star...

**Logistic & transport**
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 Entreposage, ID Logistics, Transcommerce Net , Hermes, Logicargo, Rhenus Tetrans, Snatt Logistica, SDF Iberica, TNT Express, Transnatur...

**Automotive**
Norauto, Feu Vert, Midas, Daimler Chrysler, Nissan, Arcelor Mittal, Pirelli, Gestamp, Ficosa,Durex, Showa Europe, Rubi, Kayaba, Ruffini, Fujitsu Ten, Good Year, Michelin, Magna Electronics, Denso...

**Health**
**Spanish Public Health Services:** Servicio Valenciano, IB-Salut, Osakidetza, SAS...

**Vendors:** 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...

**Tourism**
El Corte Inglés, Marsans, Viajes Barceló, Carlson Wagonlit España, Halcón, Air Europa, Logitravel, Catai, Beds Online, Costa Crociere, Avis, Ibero Cruceros, Pullmantur Cruisses, NH, Europcar, ABBA Hoteles, Atesa, Hertz, Marina D'Or...

**Mass media & Advertising**
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...

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

**Public Administration**
Ministerio de Economía y Hacienda, Generalitat Valenciana, INVASSAT, I.V.E...

## WHY A CERTIFICATION AUTHORITY?
### TRUST AS KEY ELEMENT IN ELECTRONIC TRANSACTIONS

The electronic transactions of every type that we engage in with clients, banks, suppliers or public administrations are a reality involving millions of communications daily with trading partners worldwide.

Purchase orders, invoices, despatch advices, delivery notes, contracts, etc., are often sensitive and highly important transactions calling for the rollout of different technologies for the appropriate creation, sending and reception of messages.

It is precisely the sensitivity and importance surrounding these communications that makes the adoption necessary of systems which also guarantee their security, confidentiality and integrity. The response to these issues is achieved by means of encryption techniques implemented by the standardised Electronic Signature processes managed through the Certification Authorities.

The EDICOM Certification Authority (ACEDICOM) provides physical and legal persons with the secure electronic identification mechanisms that enable them to engage in activities where electronic signature replaces the handwritten, with identical legal guarantees.

ACEDICOM is an integral part of the service infrastructure provided by EDICOM. In this way, we add mechanisms to our mail and communications solutions that enable our users to interchange electronic messages securely in complete confidentiality.

The certificates issued by the EDICOM Certification Authority comply with EU Directive 1999/93/CE of 13th December, so enjoy widespread recognition to operate throughout the European Union.

SAS70 Completed TypeII Audit

edicom certification authority

Webtrust

*certification authority*

- Issuing qualified certificates on secure device
- Issuing qualified certificates on software support
- Certificate and CRL repository.
- TSA (Time Stamping Authority)
- Certified Storage Service

edicom

*connecting business*

- VAN (Value Added Network).
- XML/EDI transactions.
- Electronic Invoicing
- Secure electronic document publishing.
- CRP/VMI software.

## ELECTRONIC SIGNATURE: WHAT IS IT AND WHAT IS IT FOR?

DIGITAL SIGNATURE

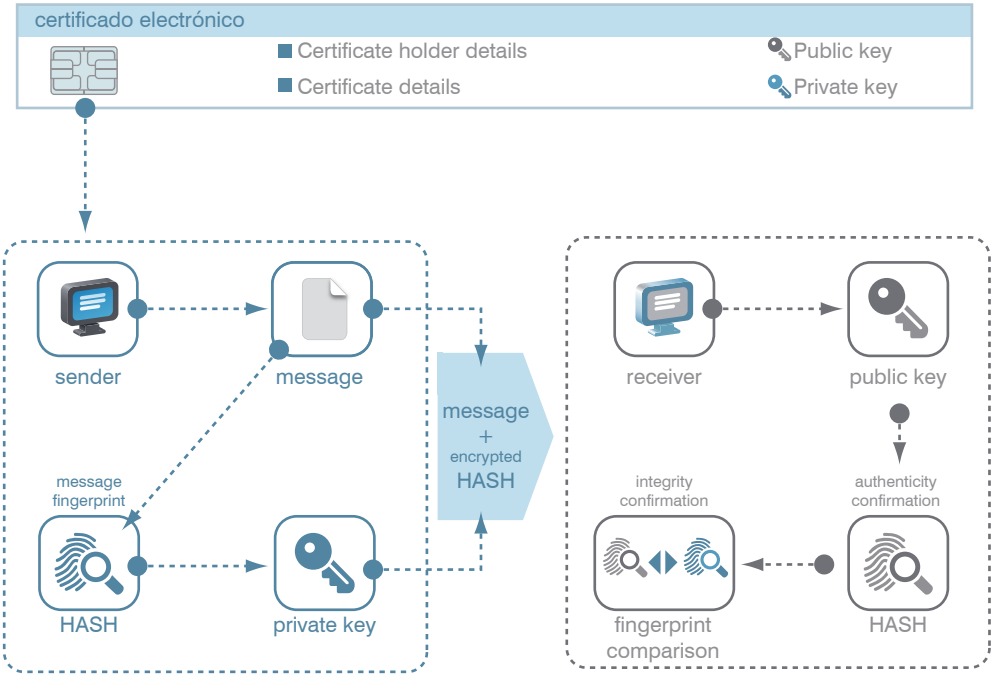
Electronic messages are affected by 3 main issues: **Confidentiality, integrity and authenticity.**

- Confidentiality: Refers to the capacity to keep an electronic document inaccessible to everyone except the receivers to whom the message is addressed.
- Integrity: Guarantees that the received document coincides with the document sent, with no possibility for change.
- Authenticity: Refers to the capacity to determine if a person has established their recognition and commitment regarding the content of the electronic document.

The issue of authenticity in a traditional document is resolved by means of the handwritten signature. To this end, one or several individuals show their will to acknowledge the content of a document, and where indicated, the commitment to fulfil the obligations and agreements set out in the same.

In the framework of electronic messages, the response to confidentiality, integrity and authenticity issues is through cryptography:

- The question of **confidentiality** is resolved by means of encryption techniques.
- **Integrity** and **authenticity** issues are covered by digital signature techniques.




- The sender obtains a summary or HASH of the document that establishes a unique fingerprint of the message. If the message is even slightly modified, this fingerprint changes.
- This HASH is encrypted with the sender's private key.
- The receiver receives the message and the encrypted HASH.
- It is then decrypted with the sender's public key. If the process is carried out successfully, it can guarantee the message source (the message is authentic)
- In parallel, the receiver applies the same HASH algorithm to the message as the sender. The fingerprint obtained is compared with the "decrypted" one and if they are the same, it is verified that the message has not been modified (the message is intact)

# digitalCertificates

A digital certificate is a document signed electronically by a certification services provider that links signature verification data to a signer and confirms their identity. The signer is the person who has a signature creation device and acts in their own name or on behalf of a physical or legal person that they represent.

To this end, the applicant's credentials are rigorously checked by the Certification Entity and univocally bound to the Certificate, so providing a unique electronic identifier which will allow them to carry out every type of electronic transaction requiring authentication.

The certificates must be issued by an Accredited Certification Authority, integrated in a PKI (Public Key Infrastructure).

## DIGITAL CERTIFICATE USES

### Digital signature

The certificate is used to sign all type of digital documents, from simple e-mails to the most complex mercantile contracts. This involves a non-rejection guarantee of unequivocal acknowledgement of who the document sender is and the integrity of the document.

### Security in communication

The certificate serves to codify a communication between two people, keeping all the transmitted information confidential. In this way, it is guaranteed that any document sent by one person to another will be closed and may only be opened by the legitimate addressee.

### Registered digitalisation

In some countries, the legislation allows replacement of the original on paper by its digital equivalent, preserving identical legal guarantees whenever certain procedures, generally linked with electronic signature, are followed.

### Personal identification

Lets you know the identity when entering a physical or digital space, allowing or denying accesses and making a record of the same.

### Software signature

The digital certificate is used to sign software. This enables the organisation that is going to use the software to ensure that it is original, know who has created it, and, most importantly, that nobody has modified it once it has been signed.

*Edicom is constituted as a Certifying Entity with the mission of providing our clients with the identification elements for the specific activity to be carried out, avoiding generalised certificates and guaranteeing compliance with legality in its strictest interpretation, as in the case of secure devices, which are covered by the CWA 1416 certification.*
*ACEDICOM issues qualified certificates for use in secure devices as well as software certificates.*

# digitalCertificates

### QUALIFIED SIGNATURE CERTIFICATES ON CENTRALISED SECURE DEVICE

The qualified secure device signature creation certificates issued by the Edicom Certification Authority are not physically delivered on any support, since by their very nature they are generated in the same device that will house them and through which the signature services are provided.

EDICOM centralised signature creation devices hold the CWA 14169 certification, guaranteeing compliance with the strictest legal interpretations.

### QUALIFIED SIGNATURE CERTIFICATES ON "SMART CARD" OR USB TOKEN SECURE DEVICE

These certificates are delivered on the cryptographic card, which keeps the sensitive cryptographic material within the card and protects its use by access control, so that extracting the private key is impossible in any case. Additionally, a SIM card reader device is provided with a USB for smart cards with plug-in (SIM card) format.

As in centralised systems, they are secure devices with CWA 14169 accreditation.


### QUALIFIED SIGNATURE CERTIFICATES ON SOFTWARE SUPPORT

Electronic signature creation certificates on software support are delivered in electronic files that can be downloaded to hard disks or USB memories, with no need to use external devices for the generation of signatures from them. They are therefore certificates with a different security level, although they may be valid for use in a multitude of transactions.


### CLIENT AND SERVER TLS (Transport Layer Security) CERTIFICATES

Unlike the former, these are "Non Qualified" certificates, so the presence of the holder is not required by the Edicom Registration Authority for their issue. They may be of two types:

Client certificates: Issued to physical persons and can serve for authentication in operating systems (optional in smart card or USB token support) and security in e-mails.

Server certificates: Issued to domain names for server authentication in SSL services (https) and can also be used for security in IPSEC tunnels.

| VIGENCIA DE LOS CERTIFICADOS | No usage limitation | With usage limitation | ...limitations... |
|---|---|---|---|
| Qualified certificate on centralised secure device | 4 YEARS | 4 YEARS | ›Signing electronic invoices<br>›Signing documents with certified storage |
| Qualified certificate on "smart card" secure device | 2 YEARS | | |
| Qualified certificate on software support | 2 YEARS | 2 YEARS | ›Access controls<br>›Signing commercial and tax documents<br>›Other limitations |
| Client and server TLS certificates | 2 YEARS | | |

■ For the issue of EDICOM Qualified Certificates, the holder must appear in person before the Edicom Registration Authority to guarantee the identity of the physical or legal person in whose name the certificate will be issued.

# Remote signature

## EDICOM CRYPTO SERVER REMOTE SIGNATURE SERVICE

The EDICOM Remote Signature service “EDICOM CRYPTO SERVER (ECS)” lets you use the qualified Electronic signature with certificates stored in secure signature creation devices (SSCD) housed in the EDICOM facilities, through a WebService interface on HTTPS.

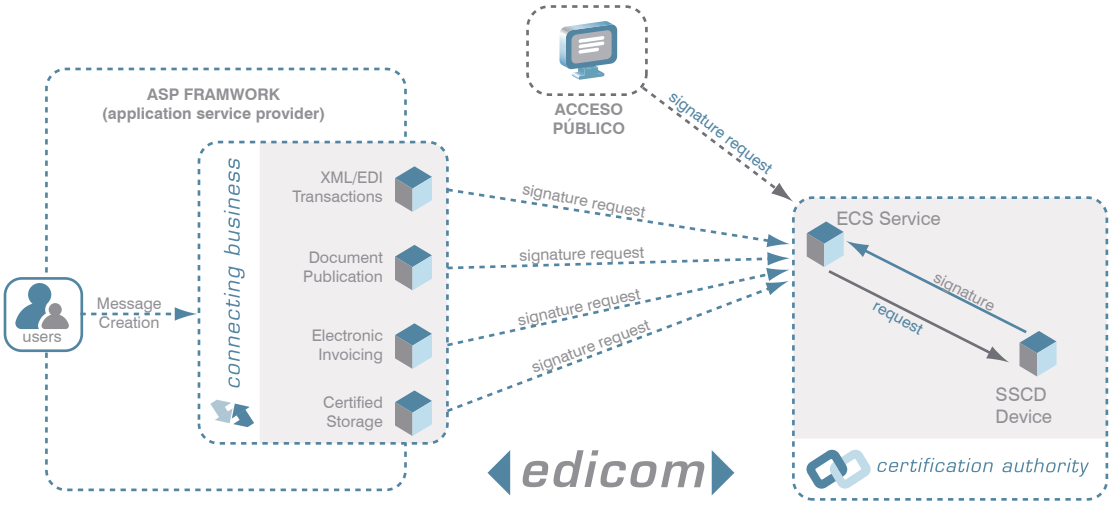
The ECS service in turn uses the following EDICOM electronic security and signature-related services:

- ACEDICOM certification entity for qualified certificate generation.
- TimeStamp service (TSA) for time stamping.
- OCSP service for certificate revocation information.


By means of ECS, the technological issue of qualified electronic signature by means of secure smartcard or HSM type devices is totally resolved, with no added complication for the client software, as the responsibility for management or access to these devices is passed on to the ECS, with all the administration advantages that it entails for the client, since they do not have to worry about the physical security of the signature device.

This service also relieves them of the technical complexity of concurrent access to the signature device from multiple sites.

- ECS (Edicom Crypto Server) service allows cryptographic signature operations in client-server architecture, either from within the EDICOM ASP framework (private intranet) or via Internet (public access).
- All the pairs of keys are stored in the secure centralised SSCD device. Generation of these keys is a process totally unconnected to ECS and follows the corresponding operating procedures of the ACEDICOM Certification Authority.
- There are 2 authentication levels: One at service level allowing access to EDICOM CRYPTO SERVER, and another with the SSCD secure signature device including the PIN associated with the private key.




Additionally, in electronic document signature processes the users may, where indicated, opt for the Delegated Signature Service.

This service differs from Remote Signature in that the documents generated by the user are signed with a certificate issued in the name of EDICOM. In this way, the issuer authorises Edicom to sign these documents on their behalf, relieving them of the maintenance and management of electronic certificates in their own name.

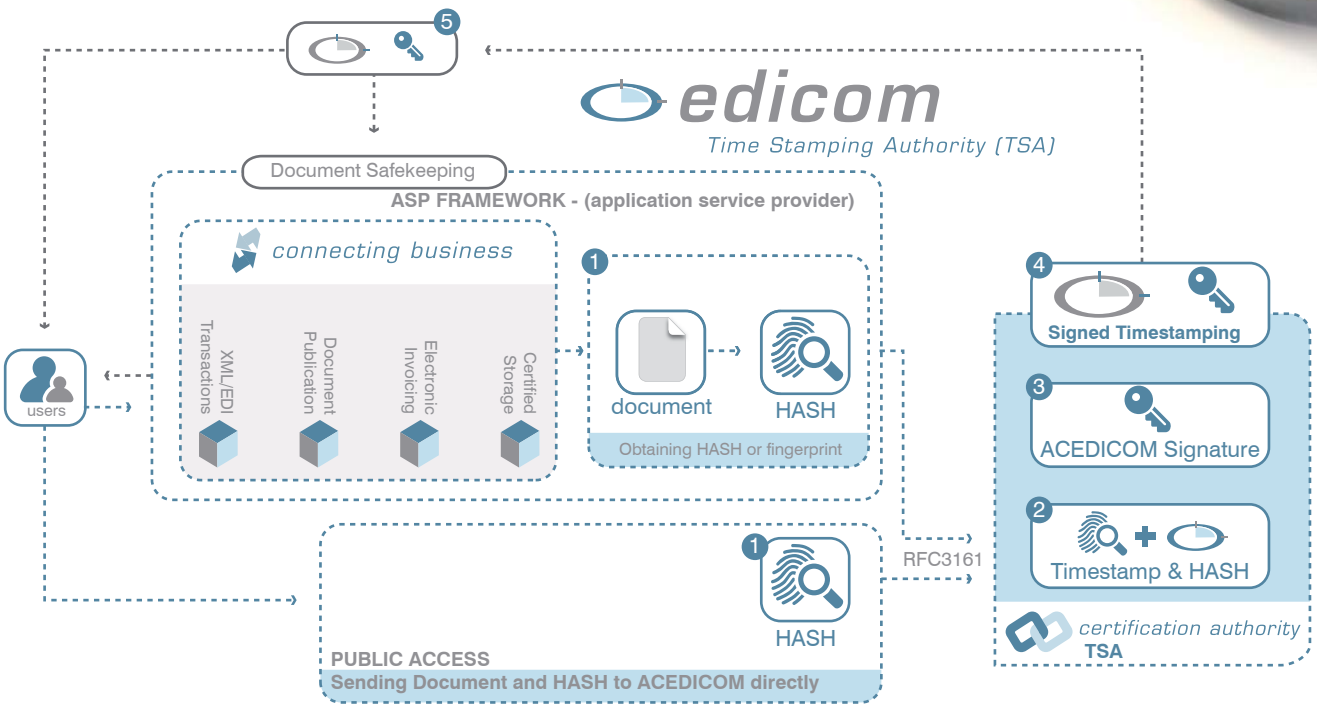
edicom
connecting business

TSA
edicom time stamping authority

## TIME STAMPING SERVICE

With Timestamping it is possible to demonstrate that a series of data exists and has not been altered as of a specific point in time. A Timestamping Authority such as Edicom acts as a trusted third party testifying the existence of these electronic data at a specific date and time.

Service operation:




The process is initiated by the client who wishes to obtain the timestamp for a particular document:

1. The client application must obtain the "summary", "fingerprint" or HASH of the document, and makes a timestamp request according to the RFC3161 protocol. This request can be made automatically through the EDICOM integration and transformation, HASH calculation or Web Services communications solutions, accessed through our ASP framework.
2. The timestamp is applied when receiving the message (with the document HASH). To this end, the service has a synchronous time source with the Universal Time Scale (UTC).
3. The EDICOM signature as Certification Authority is added, as well the certificate.
4. The signed timestamp is returned to the client. In this point, EDICOM offers document
5. safekeeping service for the storage of originals in high availability platforms.

- The protocol for Timestamping is described in RFC 3161and is in the Internet standards registry.
- The Time Stamp is verifiable by anyone and certifies the existence of a document at the time indicated by the stamp.
- The presence of a time stamp verifies that the original document has not been altered since its presentation.

# certified Storage

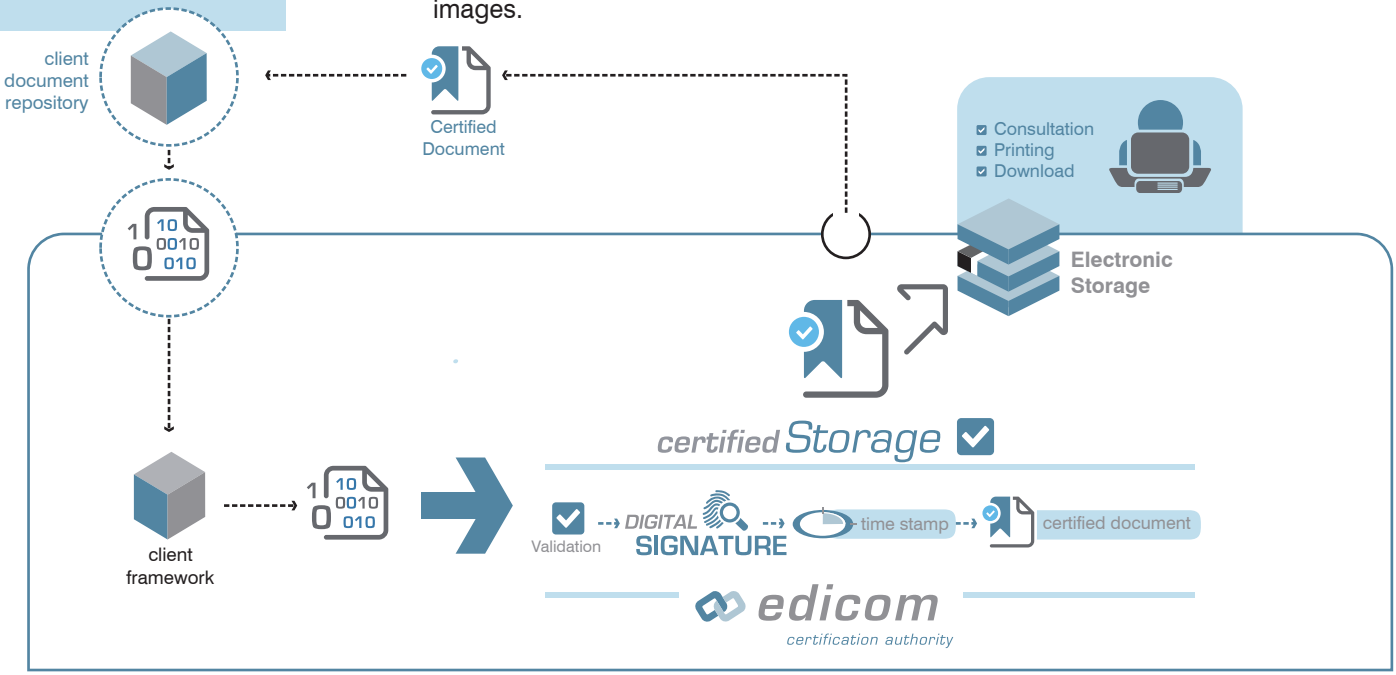
## CERTIFIED STORAGE SERVICE

In any type of company, large amounts of documents are received and produced on a daily basis. Invoices, receipts, despatch advices and correspondence, among others, pile up in offices, taking up unnecessary space, while too much time is wasted on their search and retrieval.

This translates into increasing demand calling for a digital receipt for documents that can be made without reducing the security and documentary guarantees which, as receipts, are provided by the original documents which they aim to replace.

These documents stored by electronic means could be originals created from the outset in electronic format, but also documents on paper having undergone a digitalisation process to allow their substitution by the corresponding files containing the equivalent graphic images.

- In some countries, the legislation allows substitution of the original on paper by its digital equivalent, preserving identical legal guarantees whenever certain procedures are followed, generally linked with electronic signature.
- Once this process is complete, the destruction of the original physical document file can take place, as the EDICOM Certified Document Repository file is legally equivalent.




### INFORMATION SECURITY

EDICOM has an information security system in compliance with UNE-ISO/IEC 27001:2007 standards, and control mechanisms audited by outside consultants under SAS70 Type II.

- The user makes a storage request, sending the documents to be processed to EDICOM through the working framework in our Technological Platform.
- The EDICOM Certification Authority receives the request and checks that it is complete. Access control based on the client's user name and password is implemented and the request verified.
- The Certified Storage Service of the Certification Authority signs the document and includes a timestamp. In this way, anyone who consults the document as of this point can check its integrity from the exact moment that the certification process was carried out.
- After the verification, signing and timestamping process, the document is placed in the repository for safekeeping and later consultation.

**SPAIN**
Parque Tecnológico de Paterna
Ronda de Auguste y Louis Lumiere, 12
46980 Paterna (Valencia)
Tel. +34 961 366 565 | U.K. Phone. +44 871 277 0028
Fax. +34 961 367 117
marketing@edicomgroup.com
edicomgroup.com/es

**FRANCE - PARÍS**
23-25 Rue de Berri
75008 Paris
Tel. +33 (0) 820 360 330
Fax. +33 (1) 53 76 26 87
edicomfr@edicomgroup.com
edicomgroup.com/fr

**FRANCE - LA CIOTAT**
Espace Mistral, Bat A
297 Avenue du Mistral Zone Athelia 4
13600 La Ciotat
Tel. +33 (0) 0820 360 330
edicomfr@edicomgroup.com
edicomgroup.com/fr

**ITALIA**
Centro Direzionale Milanofiori
Viale Milanofiori
Strada 1 Palazzo F1
20090 Assago. Milano
Tel. +39 02 0064 0402
Fax. +39 02 0064 0410
marketing@edicomgroup.com
edicomgroup.com/it

**USA**
152 Madison Avenue Suite 1900
New York NY 10016
Tel. +1 212 889 1909
Fax. +1 212 889 1947
marketing_us@edicomgroup.com
edicomgroup.com/us

**BRASIL**
Rua Frei Caneca 1380 - 8º andar.
CEP.01307-002 | São Paulo
T. +55 (11) 3154-5100
F. +55 (11) 3154-5102
info_brazil@edicomgroup.com
edicomgroup.com/br

**MÉXICO**
Torre del Ángel
Paseo de la Reforma No 350 Piso 16-B
Colonia Juárez
06600 Cuauhtémoc | México D.F.
Tel. +52 (55) 52 12 15 66 (ext. 2003)
Fax. +52 (55) 11 62 04 04
ventas@edicomgroup.com
edicomgroup.com/mx

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

edicom
connecting business

www.edicomgroup.com