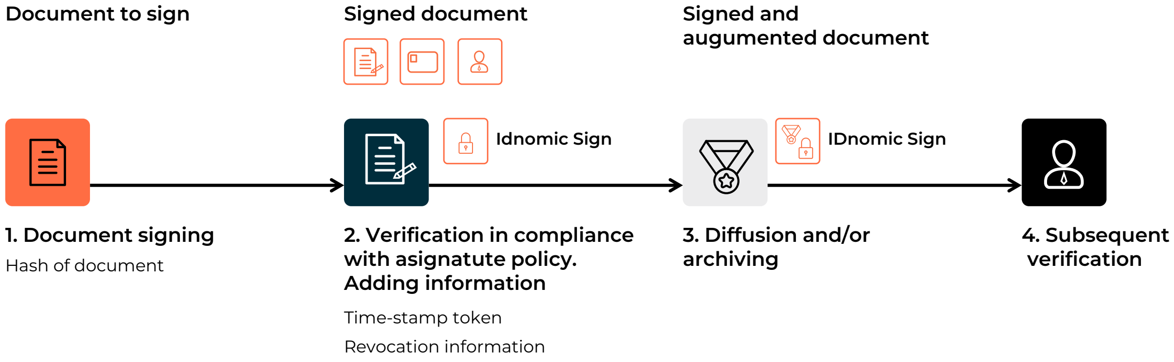
EVIDEN

IDnomic Sign

Creation and verification of non-repudiable electronic signatures

In a context where organizations are moving to paperless transactions, it is necessary to electronically sign documents to guarantee their integrity and to be able to provide a proof of acceptance by the signer. The signature has to be verified strictly to detect any possible cause for invalidity. IDnomic Sign is an overall solution to create and verify electronic signatures for various use cases.



Document to sign

Signed document

Signed and augumented document

Idnomic Sign

IDnomic Sign

1. Document signing

Hash of document

2. Verification in compliance with asignatute policy. Adding information

Time-stamp token

Revocation information

3. Diffusion and/or archiving

4. Subsequent verification

Facilitating the transformation of business processes

Electronic signatures are used to ensure the integrity of documents and identify signatories. Once a signatory has been produced and validated, it can no longer be repudiated. This is the essential property of a non-repudiation service. Each signatory uses a public and private key pair and a certificate generated by a Certification Authority.

With IDnomic Sign, Eviden provides an electronic signature platform that offers secure, high-performance and flexible services, that integrate natively with components of a trust infrastructure.

Available as software license or in SaaS mode, IDnomic Sign facilitates the digital transformation of business processes for all organizations.

The IDnomic Sign server offers companies the means to implement a secure and centralized electronic signature strategy:

- Lifecycle management of signatories' cryptographic keys, in order to carry out a remote electronic signature.
- Definition by the company, depending on degree of sensitivity, of the signature policy to be applied (formats, signature algorithm, key length, etc.).
- Creation of signatures for legal entities (electronic seal mode) or personal signatures
- Implementation of signature workflows to orchestrate the signing of a document by the various parties in a business procedure
- Enhanced, customized visual signature management for PAdES formats
- A general dashboard presenting the main operating indicators of the signature server

an atos business

EVIDEN

IDnomic Sign offers the following functions:

- Signature creation: creation in the expected format using the signature policy and the configured resource.
- Immediate verification and augmentation: cryptographic verification after creation and addition of information to maintain its long-term validity with a detailed report.
- Subsequent verification: a posteriori verification with detailed report.

IDnomic Sign generates and verifies advanced electronic signatures in CAdES, XAdES and PAdES formats in compliance with standardized signature policies.

IDnomic Sign relies on an external time-stamping service such as IDnomic TSP solution or third-party time-stamping services complying with RFC 3161.

This server is accessible in Web services mode (API REST), enabling the electronic signature to be in line with the company's business applications. The signature server also offers a signature portal which can be used directly by authenticated users on the server to sign and verify documents and to manage signature keys and preferences.

To carry out the signature, signatories can use signature certificates stored on a smart card, or certificates previously enrolled and secured centrally on the IDnomic Sign server, or short-duration certificates generated on the fly at the moment of the signature.

The interface with the PKI can be implemented using the proprietary IDnomic PKI protocol or with standardized protocols SCEP or EST protocols for any PKI respecting this protocol.

IDnomic Sign lets you define advanced signature policies, used at the time of signature construction, signature and verification to control and authorize the latter verification.

The electronic signature in PAdES format (pdf file) allows the insertion of a visual representation.

of the signature in the signed document. Each user can manage their own visuals, based on templates provided by the solution administrator.

For large companies or operators (trusted third parties), IDnomic Sign enables you to serve several single installations in a multi-tenant architecture and completely isolated. In this way users are able to serve different projects or customers without any permeability between the data used in each of the tenants.

Advanced certificate verification

Vericert is an optional server component of IDnomic Sign. It is used to build and verify certification paths against the validation policies configured in its administration. Verification services are available in web service mode. verification can be performed with respect to the present or to a date in the past. Trusted Certification Authorities can be automatically extracted from the European Trusted List (TSL).

Standards and technical specifications

Norms and standards

- Certificate format compatible with ITU-T X.509v3, RFC 5280 and RFC 3739
- XadES: XML Advanced Electronic Signature ETSI TS 101 903
- CAdES: CMS Advanced Electronic Signature ETSI TS 101 733
- PAdES: PDF Advanced Electronic Signature ETSI TS 102 778 including LTV format (part 4) and signature visual (part 6)
- XML signature policy format ETSI TR 102 038
- RFC 3161: Protocol for obtaining time stamps (timestamp tokens)
- OpenID Connect and OAuth2 authentication
- PKCS#11 for interfaces with a hardware security module security module (HSM)
- PKCS#11 for interfaces with a hardware security module security module (HSM)
- ECDSA and/or RSA signature algorithms available in the used HSM

Compliance

- Complies with European Directive 1999/93/EC and the eIDAS regulation
- Proper implementation of norms and standards is validated by frequent participation in ETSI interoperability plugtests

System requirements

- PKCS#11 for interfaces with a Hardware Security Module (HSM)
- ECDSA and/or RSA signature algorithms available in the HSM used
- Executable on the Java 11 runtime environment
- Linux (Red Hat/ CentOS 7.5 or higher).
- Integrated and delivered with Open Source components Apache, PostgreSQL, Tomcat, Ansible (installation script).
- Authentication on the IDnomic Sign server must be delegated to an Identity Provider using the authentication mechanisms OpenID Connect and OAuth2

Find out more about us: www.idnomic.com

Connect with us

eviden.com

20231010