IDnomic Sign

# Creation and verification of non-repudiable electronic signatures

In a context where organisations are moving to paperless transactions, it is necessary to electronically sign documents to guarantee their integrity and to be able to bring the proof of acceptance by the signer. The signature has to be verified strictly so as to detect any possible cause for invalidity. Atos, a European actor in IS security, provides **IDnomic Sign**, an overall solution to create and verify electronic signatures.

## Keep control of security

Electronic signatures guarantee the integrity of documents and identify the signers. Once a signer has produced a signature and the signature has been verified, the signature is secure and may no longer be repudiated.

Each signer uses a signature key pair (a public key and a private key) and a certificate generated by a Certification Authority.

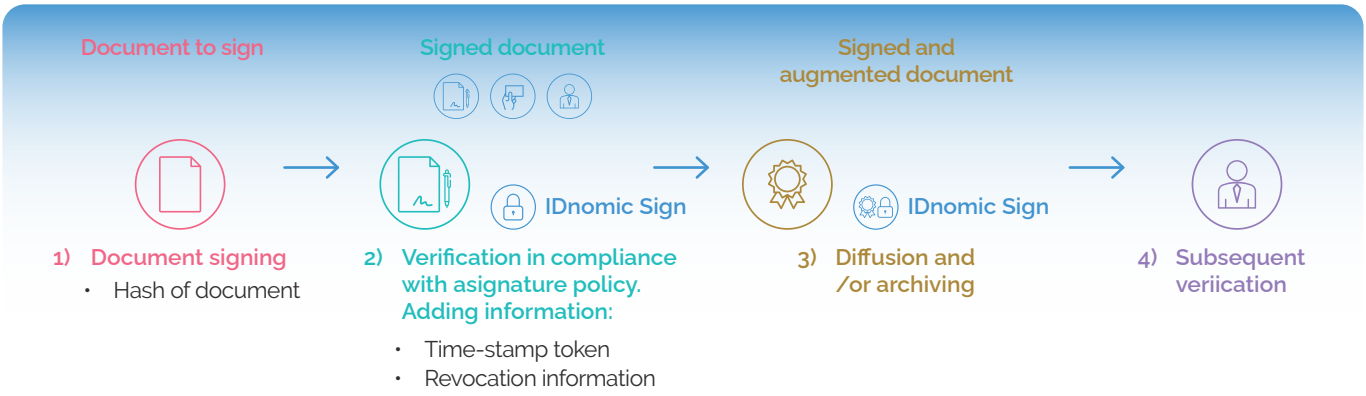
The IDnomic Sign server can use signature certificates generated by the Atos's ID PKI solution or other PKI products.

The IDnomic Sign server manages the cryptographic keys on behalf of the signers. It stores them in a secure way and allows access only to its owner. In a web application, it also allows to use keys stored locally in a smart card for example.

IDnomic Sign creates and verifies electronic signatures using the following formats: CMS, CAdES, XAdES or PAdES, and in compliance with standardized signature policies. IDnomic Sign relies on a time- stamping service such as Atos IDnomic TSP or other time-stamping solutions.

IDnomic Sign supports the following functions:

- **Signature creation:** creation with the requested format using the signature policy and the configured cryptographic token; multiple signatures and co- signatures are supported
- **Immediate verification and augmentation:** cryptographic signature verification following its creation and adding the necessary information to maintain its long-term validity with report generation
- **Subsequent verification:** verification by relying parties and generation of a report.




Atos

## IDnomic Sign offer and its functionalities

### IDnomic Sign server

The IDnomic Sign server offers a centralized implementation of a service supporting all the operations of secure electronic signatures and signature verification.

This server can be accessed in "Web services" mode (API REST) allowing the integration of the electronic signature within business applications.

It also has a signature portal function.

The server can be used to sign in the name of an entity (seal signature) or to sign in the name of a physical person with a secured management of the signer's bi-keys.

The signers can use signature certificates stored in a smart card they hold, or certificates centrally located at the IDnomic Sign server.

### Standardized signature policies

With IDnomic Sign, it is possible to define advanced signature policies. These policies will be used when the signature is built in order to control and authorize, for a given policy, an encryption algorithm, a key size, a trust authority, etc...

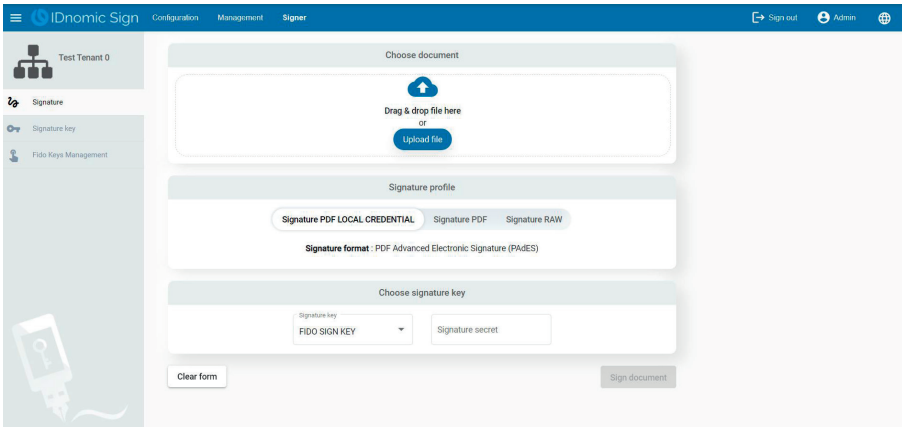
### Advanced verification of certificates

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

### Remote Qualified Signature

As an option to the IDnomic Sign server, Atos offers a dedicated appliance to perform remote qualified signatures in compliance with eIDAS the "Explicit Consent Manager". This hardware is used in addition to the IDnomic Sign server to manage the signer''s consent via an OTP or a FIDO authentication. This appliance behaves like a "Signature Activation Module (SAM)" according to the ETSI CEN 419 241-2 terminology.

Atos is engaged in a certification process with ANSSI for this appliance.




## Standards and technical specifications

### Norms and standards

- Certificate format compliance 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 visual of signature (part6)
- XML signature policy ETSI TR 102 038
- RFC 3161: Time Stamp Protocol
- Authentification Open ID Connect for the API REST
- PKCS#11 for interfacing with a Hardware Security Module (HSM)
- Local credentials

### Compliance

Compliance with the European directive 1999/93/CE and eIDAS regulation

### System requirements

IDnomic Sign works in a Java 11 runtime

The IDnomic Sign implementation of norms and standards is validated throughout the frequently participation to ETSI interoperability plugtests

Server solutions IDnomic Sign is running on Linux platforms (Red Hat or SUSE). This solution is fully integrated and delivered with Open Source international components Apache, PostgreSQL, Tomcat, Keycloak(IDP) and Ansible (install script).

Find out more about us atos.net/en/solutions/cyber-security/trusted-digital-identities/idnomic-sign