IDnomic metasign

A non-repudiable signature creating and verifying secure transactions

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 metasign, 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 (e.g. a user or an application) uses a signature key pair (a public key and a private key) and a certificate generated by a Certification Authority.

Metasign can use signature certificates generated by the Atos's solution metapki or other PKI products.

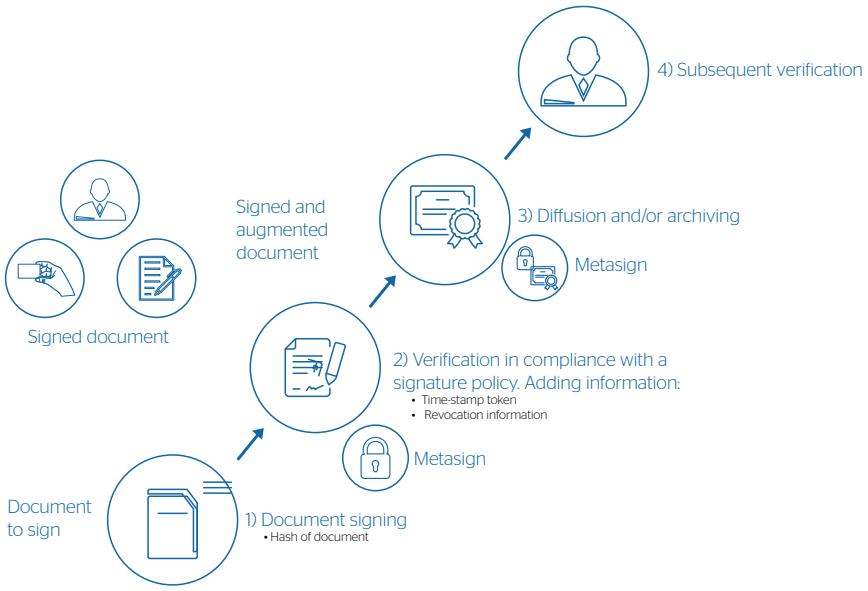
For users, the signature private key and the signature certificate may be stored in a smart card or in a USB token protected by a PIN, or alternatively in a file in the PKCS#12 format. Private keys and certificates are accessible either through a PKCS#11 interface or a MSCAPI interface.

For applications, Hardware Security Modules (HSM) are used for the same purpose.

Metasign creates and verifies electronic signatures using the following formats: CMS, CAdES, XAdES or PAdES, and in conformance with declared signature policies. Metasign supports time-stamping tokens generated by Atos metatime or by other time-stamping solutions.

Metasign 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.



Trusted partner for your **Digital Journey**

Metasign offer and its functionalities

Metasign-server

Metasign-server is a “web service” server that signs and verifies documents. Its administration interface is provided for configuring applications and signature policies.

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 centralised and secured management of signature keys.

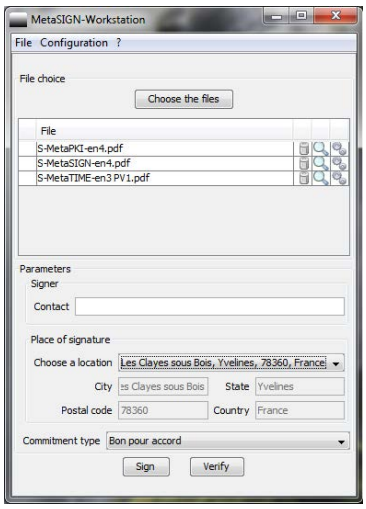
Metasign-api

Metasign-api is a full set of Java programming interfaces allowing different integration scenarios:

- Java applets for web browsers
- standalone applications for personal computers
- server-based applications.

Metasign-workstation

Metasign-workstation is a standalone application running on a PC. Users can sign multiple documents in a one step process. The main goal of the application is to simplify the usage and the deployment of digital signatures.



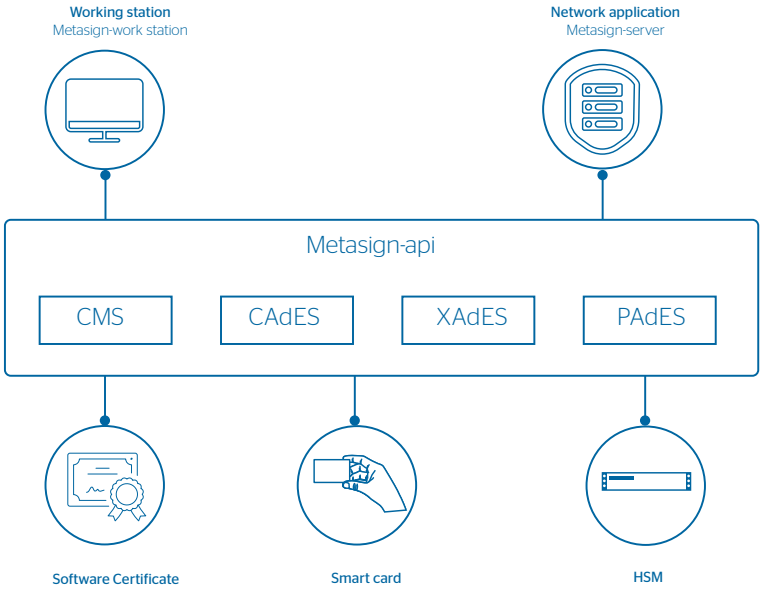
Vericert

Vericert is an optional “web service” server component. It verifies certification paths against verification policies that can be configured in the administration interface.

Verification can take place with reference to the current time or to a time in the past. Trusted Certification Authorities can be extracted from European trusted lists (TSL).

Signature formats

Metasign supports advanced electronic signatures conformant with the CMS, CAdES (CMS Advanced Electronic Signatures), XAdES (XML Advanced Electronic Signatures) and PAdES (PDF Advanced Electronic Signatures) technical specifications as defined by ETSI (European Telecommunication Standardisation Institute).



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 • PKCS#11 and MSCAPI for interfacing with smart cards. Support of IAS cards and pinpad readers • PKCS#11 for interfacing with a Hardware Security Module (HSM) • PKCS#12 for the storage (in the file case) of the signature private key and the certificate

Conformity
Conformance with European directive 1999/93/CE and eIDAS regulation
✓ VISA DE SECURITE — Atos received on 25/03/2016 the ANSSI Security Visa for Common Criteria certification at level EAL 3 augmented with its products MetaSIGN-API and MetaSIGN-Applet version 3.3.5.

System requirements
Metasign works in a Java 8 runtime
The metasign implementation of norms and standards is validated throughout the frequently participation to ETSI interoperability plugtests
Server solutions metasign-server and Vericert are running on Linux platforms (e.g. Red Hat or SUSE). These solutions are fully integrated and delivered with Open Source international components Apache, PostgreSQL, PHP and Tomcat

Find out more about us
atos.net/en/products/cyber-security/digital-identities/metasign

CT-201015-AS-F-IDnomic_metasign-en7