IDnomic Signature Appliance

Secure your transactions with electronic signatures

In environments that require a high level of trust, advanced or qualified electronic signatures are highly advised. They ensure a document's integrity in paperless transactions and provide proof of acceptance by the signer.

Ensure trust in your exchanges

Electronic signatures can support organizations in their compliance journey with eIDAS regulation. While securing document and data exchanges, electronic signatures also contribute to reducing processing costs, such as printing and archiving, and to enhancing productivity with dematerialized processes.

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 public key certificate generated by a certificate authority (CA).

Quickly deploy your digital signature project with an appliance

The deployment of a digital signature project can be complex with various integration constraints to handle. The Signature Appliance facilitates the implementation of digital signature within document workflows. Users can keep using their existing document workflow management application and add electronic signature processes without any discontinuity.

The Signature Appliance uses signature certificates generated by the Atos PKI solutions or other PKI products. The signature private key and the signature certificate are stored:

- In an HSM for seal signature.
- Enciphered in the database for other uses cases. The enciphered keys are securely imported to an HSM, which provides a tamper-proof environment.

Remote signature: a solution for mobile users

Signing documents should be as easy as a hand-written signature. A remote signature functionality enables the user to electronically sign documents anywhere and from any device.

Atos offers a server-based solution where signing is done remotely with strong private key management. After a secure authentication (for instance, with a smart card), the user can apply a signature made in a tamper-proof environment.

The server is accessed by third-party software through documented Web services (SOAP or REST). For the end user, an application using these Web services can be deployed and customized to offer user-friendly interfaces, similar to a Web portal.

An administration interface is provided for configuring applications and signature policies. The server can be used to sign in the name of an entity or to sign in the name of a physical person with centralized and secure signature keys management.

Trusted partner for your **Digital Journey**

Atos

Choose the right level of digital signature

Two deployment models are available for specific use cases: basic/advanced and qualified.

Before launching a project, users need to identify which applications should have the most secure electronic signatures (qualified signatures) and the ones where a basic or advanced signature is sufficient.

The signature appliances are fully compliant with eIDAS regulation for the creation of qualified digital signatures. To achieve this compliance, the signature solution for natural persons is connected to the User Explicit Consent appliance to ensure that a signature key is solely controlled by its owner.

In a centralized environment, a mechanism must be implemented to verify that only the owner of a sensitive key will activate cryptographic operations on that key. The User Explicit Consent appliance defines secure mechanisms attached to the digital keys that have to be activated and controlled before the key usage approval.

As a "Signature Activation Module" in ETSI standards naming, the User Explicit Consent appliance offers recognized capacities of remote qualified signature. Atos is engaged in a "Qualification Elémentaire" process with the ANSSI for this appliance.

Simplify your product deployment using appliance

The Signature appliance helps organizations deliver their projects quickly and cost-efficiently, as:

1. Pre-defined configuration is implemented: the appliance model is delivered with a standard configuration that can be used in most use cases, with **no extra time** in specifications or integration,
2. The product is delivered in a **unique hardware** with **pre-configured features** and **database**,
3. Minimal configuration is done at first run to make the appliance **ready to use**.

The system maintenance and support are simplified as the appliance is an all-in-one solution facilitating the tasks that can be complex and time-consuming in a classic implementation due to tailored configurations (VMs, servers, HSM...).

Define who should be engaged

Electronic signatures are applied to cross-department applications (billing workflows, commercial contracts, payroll...) and can be adapted to different setups (decentralized/centralized; natural person/legal person, seal). With the signature of the person, the signatory personally commits to the signed data. With a seal, the signature is made on behalf of an organization or a legal person.

Different configurations are available with the Signature Appliance:

- **Seal signature:** for the delivery of seal signatures on behalf of a company or a legal entity.
  - **Centralized signature** for an application or "electronic seal"
  - Seal keys are maintained in the HSM
  - **Key Ceremony** for certificate creation
- **People signature:** different people can request personal signatures once they have been pre-registered and a signature digital identity has been enrolled for them.
  - User **centralized signature** with remote access to the server
  - Users signature private keys are managed in the HSM (enrollment phase and signature)
  - Password management to protect the user against misleading use of their private key
- **Explicit Consent Manager (ECM):** for eIDAS qualified signature, sole control by the user of a private key must be guaranteed. A specific hardware-based solution, the ECM, is used to manage the consent of the user in addition to a metasign-server. This solution does not allow the use of the private key before having activated it via an OTP or a Fido authentication. It acts as a Signature Activation Module in ETSI terminology of CEN 419 241-2 (protection profile for QSCD for Server Signing).

A model tailored to your needs

Atos provides a wide range of trust infrastructure appliances (PKI, digital signature, user explicit consent, time stamping, blockchain) and offers different models adapted to the infrastructure's needs:

- A **basic model** with only one service embedded in an HSM. This model is fully adapted to the Root CA appliance as it is autonomous and does not depend on the infrastructure.
- A **high-availability model** deploying several appliances to ensure business continuity with a centralized database.
- A **multi-services model**, enabling the combination of many services in an HSM such as electronic signature or timestamping together with PKI.

Get a greater control over the security of the information system and independence from “as-a-service” solutions with a certified hardware solution, ease and speed of implementation.

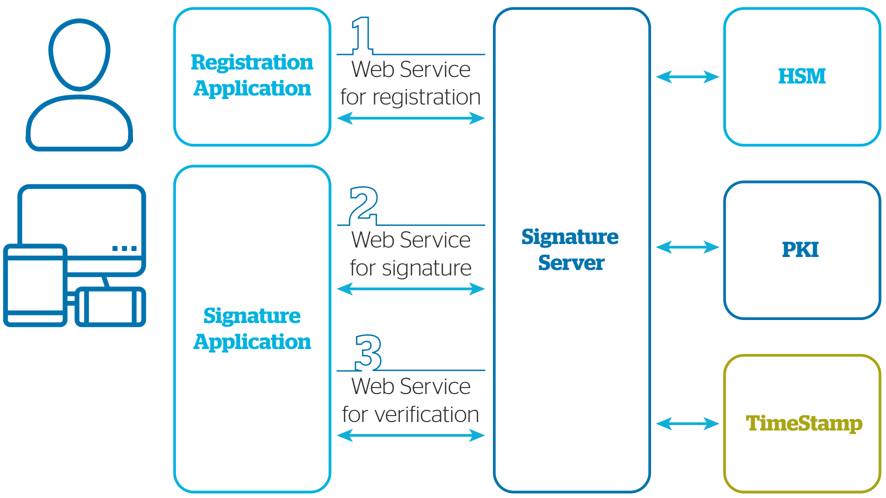
Atos signature appliance supports the following functional modules

- **Signature creation:** creation with the requested format using customized signature policies and the configured cryptographic token; multiple preconfigured signatures formats are supported e.g., PAdES, XAdES.

- **Immediate verification (and augmentation):** cryptographic signature verification and addition of the necessary information to maintain its long-term validity (i.e., connection with external timestamp server). Production of a verification report.

- **Subsequent verification:** verification of all elements which are present in the signed document and generation of a signature verification.

Signature Appliance high-level architecture


Registration Application
1
Web Service for registration
Signature Application
2
Web Service for signature
3
Web Service for verification
Signature Server
HSM
PKI
TimeStamp

Atos signature appliance supports the following signature formats

Advanced electronic signatures compliant with technical specifications as defined by ETSI (European Telecommunication Standardisation Institute):

- CMS (Cryptographic Message Syntax),

- CAdES (CMS Advanced Electronic Signatures),

- XAdES (XML Advanced Electronic Signatures),

- PAdES (PDF Advanced Electronic Signatures).

Standards and technical specifications

HSM Certifications	• Common Criteria EAL4+ compliant with CWA 14167-2-PP • NATO SECRET • Compliant with eIDAS • «Qualification Renforcée» (the highest qualification from the ANSSI) • FIPS 140-2 level 3 (in progress)
Administration	• Cryptographic profiles definition • Secure updates of embedded software • Load balancing capability
Signature Appliance	• XAdES: XML Advanced Electronic Signature ETSI TS 101 903 Basic profile ETSI TS 103 171 Baseline profile ETSI EN 319 132-1 Building blocks and XAdES baseline signatures • PAdES: PDF Advanced Electronic Signature ETSI TS 102 778 including basic profiles (part 2), BES & EPES profiles (part 3), LTV format (part 4) and visual of signature (part6) ETSI TS 103 172 Baseline profile ETSI EN 319 142-1 Building blocks and PAdES baseline signatures • CAdES : CMS Advanced Electronic Signatures TS 101 733 & EN 319 122-1 • Signature policy: ETSI TR 102 038 XML policy ETSI EN 319 431 ETSI EN 319 441
Physical Interfaces	• 2 Ethernet 10/100/1000BASE-T ports • 4 USB2 ports • 1 VGA port • Integrated keyboard and chip card reader • Redundant electrical supply • Restart button on the front • Secure RPC over SSL to Windows, Linux and AIX 32/64 servers

About Atos

Atos is a global leader in digital transformation with over 110,000 employees in 73 countries and annual revenue of over € 11 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos | Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education as well as multicultural and pluralistic approaches to research that contribute to scientific and technological excellence. Across the world, the group enables its customers, employees and collaborators, and members of societies at large to live, work and develop sustainably and confidently in the information technology space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together