

A person wearing a white lab coat is shown from the chest down, holding a tablet computer with both hands. The person is in a clinical or hospital setting, with a dark blue or teal background that appears to be part of a medical device or control panel. The lighting is soft and focused on the hands and the tablet.

 Horus Trust Infrastructure
Appliances

Simplify the
deployment of your
trust infrastructures

Trusted partner for your Digital Journey

Atos

Digital identities allow applications to support security services such as user authentication, non-repudiation of transactions, and confidentiality of data exchanges. Atos, a European actor in Information System security, provides trust infrastructure appliances that can be deployed simply and securely.

Simplify your product deployment using appliance

With Horus ready-to-use appliances, organizations can deliver their projects quickly and cost-effectively. The product functionalities and the database instantiation are already pre-configured, reducing the project timeline from several months to a few weeks, and avoiding the burden of acquiring and configuring additional materials such as servers.

The system maintenance and support is simplified through bundle building avoiding complex and time-consuming tasks. Learning time is also reduced as organizations have less features to handle.

The Horus Trust Infrastructure appliances are loaded on the state-of-the-art Trustway Proteccio HSM, providing appliances in a high-performance, highly secure environment for performing their most sensitive cryptographic operations.

The range of Horus Trust Infrastructure appliances includes:

- Horus PKI
- Horus Signature
- Horus User Explicit Consent
- Horus Time Stamping
- Horus Blockchain

Keep control of security with PKI

With the Horus PKI appliances, digital certificates can be easily integrated and used to support different purposes.

Different configurations are available:

- Horus Root CA: for the delivery of Subordinate CAs to build a trusted CA hierarchy. The CA certificate profiles are created from defined models and can be associated with RSA or ECDSA asymmetric keys. The production of CA certificates complies with the certification policy defined by the customer and is compliant with supervisory body requirements. Typical usages include creation of new requested delegated CA and production of Certificate Revocation Lists (CRLs).
- Horus Simple Certificate Enrolment Protocol (SCEP) CA: allowing the automatic delivery of final certificates for strong authentication. Certificates are dedicated to different types of holders, i.e., people or equipment. This appliance can be integrated as part of a global Information System to deliver digital identities for each component of this system.
- Other instances of Horus PKI appliance can be done according to customers' requirements.



Use case - Telecom

A telecom network provider for IoT needs to secure its ecosystem. The Horus SCEP CA appliance can provide X509 certificates to the gateways and all certificate requests are processed through the SCEP protocol. Control of certificate revocation can also be done using the Online Certificate Status Protocol (OCSP) protocol.

This way, it becomes possible to deliver the security features for IoT infrastructure and manage million of devices connected through gateways.



Bring confidence to your exchanges with electronic signature

The Horus signature appliances can be securely deployed in the organization's infrastructure, providing trust and integrity of signed documents and bringing proof of non-repudiation by the signer. Users can keep on using their existing document workflow management application and add electronic signature processes without any discontinuity. The following functions are supported by Horus Signature appliances:

- **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.

Different configurations are available:

- Horus Seal signature: for the delivery of seal signatures on behalf of a company or a legal entity.
- Horus People signature: different people can request personal signatures when they have been previously registered and at least, a signature digital identity has been enrolled for them. A GUI web application is deployed to be interfaced with the signatories.

The Horus signature appliances are fully compliant with the eIDAS regulation for creation of qualified digital signatures. In that case, Horus people signature appliance is also connected to the User Explicit Consent appliance to ensure the sole control of signature key by its owner.



Use case - Healthcare

A hospital wants to deploy a system to centrally sign documents (blood analysis, tests results...) in order to have a fully dematerialized process and to ensure authenticity, integrity and signer identity for the documents. It benefits from a central signing service to mutualize the signing process and the signature policy for all existing medical applications, while remaining easy to use.

Why choosing Appliances for trust infrastructure?



Speed of deployment

Reduce your deployment time from several months to a few weeks



Flexibility

As you grow, adapt the appliances required to your needs



Cost-efficiency

By simplifying the integration of trust infrastructure applications you avoid further development costs

Enable the sole control of digital key by its legitimate owner

Many sensitive applications require strong authentication to access a service for data encryption or/and signature. In a centralized environment system, a mechanism has to be set up to control that only the owner of a sensitive key will activate cryptographic operations on that key.

The Horus User Explicit Consent appliance defines secure mechanisms attached to the digital keys that have to be activated and controlled before the key usage approval.

The Horus User Explicit Consent appliance provides the following mechanisms:

- One Time Password (OTP) authentication: usage of key is conditioned by the providing of an OTP to execute the cryptographic operation. The key activation request generates a challenge which is transmitted to a broker service in charge of relaying the information to a trusted application (like a mobile application) able to calculate the OTP from an initial secret and this challenge. The OTP will have to be transmitted to the appliance to validate the usage of key. The OTP can be used for a limited time and a limited number of operation.
- FIDO authentication: when the user owns a FIDO hardware token, this token can be enrolled in the application before the creation of a digital key to be associated together. In that case, the usage of the digital key is controlled by the signature of challenges done by the FIDO hardware token. This signature will be verified by the appliance to validate the usage of key. When the key is correctly activated, a limited number of cryptographic operations can be done in a given timeframe.



Use case - Utilities

An electricity provider needs to check the identity of its technicians when they are operating on smart meters in order to comply with the distribution system operators' regulations. As they are mobile, the technicians cannot use a laptop but they have their mobile phones with them.

Whenever they want to access the smart meters' data, they receive a notification on the trust authentication mobile application provided by the Horus appliance for User Explicit Consent Application. They just need to authenticate themselves to validate their identity and quickly access the smart meter's interface in complete trust.

Prove timestamping of transactions

The Horus timestamping appliance provides time-stamp tokens which guarantee a trusted date and time associated with the footprint of a document. It constitutes a proof element preventing the modification of the document without detection.

A time-stamp token is a signed piece of data including:

- a date and time (UTC time)
- a hash value computed using a hash function (e.g., SHA 1 or SHA 256)
- the identifier of the time-stamping unit (TSU) which produced the time-stamp token

The Horus timestamping appliance is preconfigured to manage two TSU with different timestamp policies. The access to the TSU can be secured by strong authentication. Addition of TSU is possible through a personalized appliance building.

This appliance is compliant with the eIDAS regulation.



Use case - Public Sector

A national institution wants to set up new digitalization services within its administration, including digital signature. It should be used internally and externally.

Along with fully dematerialized procedures, organizations can set up a timestamp appliance either for their internal needs or for external services acting as trust service providers. The time token can be generated for external usage in an as-a-Service approach with no limitation in the number of tokens and with a highly scalable solution.

Manage decentralized multi-actor confidence through blockchain

Through the Horus Blockchain appliance, organizations can form a blockchain consortium while keeping the sovereignty of their data with regards to companies' customers. By relying on the blockchain technology, it is possible to reduce fraud, increase transparency in supply chains and build or reinforce trust in nascent relationships. With the Horus Blockchain appliance, organizations can:

- manage governance using consortium blockchains
- control trust levels, ensuring privacy and confidentiality through electronic signature and encryption
- reinforce access control to Blockchain data with the right authentication factors.



Use case - Automotive

A consortium of car manufacturers, garage owners and insurances is looking to reduce fraud and increase transparency in automotive transactions.

They set up a private blockchain network which can eliminate the potential for fraud with a blockchain appliance. When a car owner takes a vehicle into a garage for service or maintenance, all relevant information for traceability about the car - including the distance it has travelled - will be entered into the shared, distributed ledger using blockchain. This cannot then be changed. Any potential buyer will just have to check the network to make sure that the information on the odometer and in the maintenance book corresponds with the reality recorded using blockchain. Fraud risks will be mitigated and all these actors will reinforce trust in their relationships with consumers and suppliers.

A model tailored to your needs

Horus offers three different models of appliances according to the needs of the infrastructure:

- **A basic model** with only one service embedded in a HSM. This simple model is autonomous and does not require management of high volume of data. As it is not depending on the infrastructure, it can be deployed in a short time. As an example, this model is fully adopted for Horus Root CA appliance.
- **A high-availability model** with 2 appliances sharing live database for one service embedded in each HSM. This model can be adopted to generate high volumes of certificates or signatures. With the high availability cluster, the business continuity is ensured through load-balancing to meet the highest requirements while keeping a simple setup.
- **A multi-services model** with several services embedded in a HSM. In this way, it is possible to combine many services such as electronic signature and timestamping.

A combination of the high-availability model and the multi-services model is possible.

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

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

Horus Root CA Appliance

- Certificate compliance with ITU-T X.509v3, RFC 5280 and RFC 3739
- Revocation information compliance with ITU-T X.509v2 CRL
- Certification request format: PKCS#10
- Algorithms: RSA 4096 and ECDSA named curves secp224r1, secp384r1, frp256v1

Horus SCEP CA Appliance

- Certificate compliance with ITU-T X.509v3 and RFC 5280
- Revocation information compliance with ITU-T X.509v2 CRL and OCSP Protocol (RFC 2560)
- Certificate enrolment protocol: SCEP
- Algorithms: RSA 2048 & 4096

Horus 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
- Signature policy:
ETSI TR 102 038 XML policy
ETSI EN 319 431
ETSI EN 319 441

Horus User Explicit Consent Appliance

- PKCS#11 to communicate with ECM module
- ETSI EN 419 241-1
- Compliance with PP 419 241-2

Horus Timestamping Appliance

- IETF RFC 3161
- ETSI TS 101 861 (a profile of RFC 3161)
- X.509 v3 or RFC 5280 for TSU certificates
- ETSI EN 319 422

Blockchain Appliance

- Hyperledger Fabric v1.1 node
- Confidentiality management (Governance Management Suite - GMS) on top of Hyperledger Fabric
- Node management admin and presentation dashboards
- Access to GMS and blockchain node using RESTful API



About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 73 countries and annual revenue of around € 12 billion. European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, the Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us

atos.net/en/products/cyber-security/digital-identities

Let's start a discussion together

