IDnomic 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 Atos 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 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 Trust Infrastructure appliances includes:

- PKI
- Signature
- User Explicit Consent
- Time Stamping

Keep control of security with PKI

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

Different configurations are available:

- 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).
- PKI Technical 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 PKI appliance can be done according to customers' requirements.

Use case – Telecom

A telecom network provider for IoT needs to secure its ecosystem. The 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 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 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:

- Seal signature: for the delivery of seal signatures on behalf of a company or a legal entity.
- 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 signature appliances are fully compliant with the eIDAS regulation for creation of qualified digital signatures. In that case, 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 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 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 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 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 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.

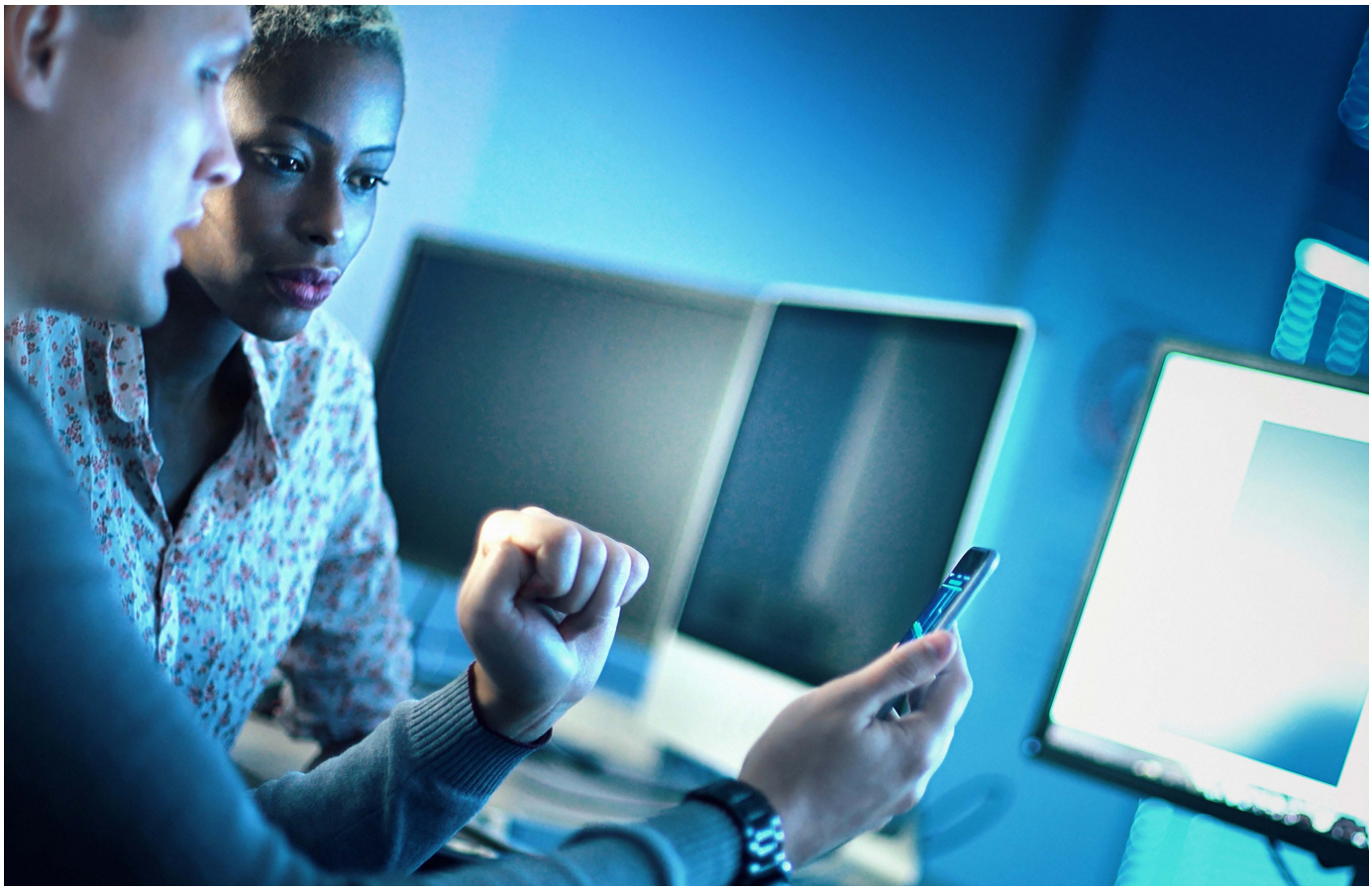
Along with fully dematerialized procedures, organizations can set up a timestamp appliance either for their internal needs or for external services acting as trust service providers. The time token can be generated for external usage in an as-a-Service approach with no limitation in the number of tokens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

A model tailored to your needs

Atos 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 adoptedfor 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

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

PKI Technical CA

- 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 and CMP
- Algorithms: RSA 2048 & 4096

Signature Appliance

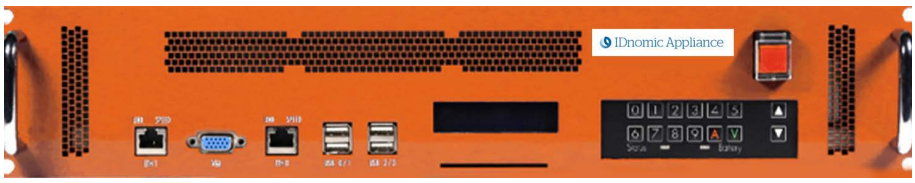
- XAdES: XML Advanced Electronic Signature
  ETSI TS 101 903 Basic profile
  ETSI TS 103 171 Baseline profile
  ETSI EN 319 132-1 Building blocks and XAdES baseline signatures
- PAdES: PDF Advanced Electronic Signature
  ETSI TS 102 778 including basic profiles (part 2), BES & EPES profiles (part 3), 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

User Explicit Consent Appliance

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

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



About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 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 space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
https://atos.net/en/solutions/cyber-security-products/digital-identities/trust-infrastructure-appliances

Let's start a discussion together

CT_J1463_201105_AS SIMPLIFYTHE