IDnomic Security Server

Securing the Value of the Internet of Things

Trusted partner for your **Digital Journey**

Atos

Secured identity management is at the core of digital world security. The growing number of entities connected to the Internet of Things (IoT) results in increasingly complex systems to be managed. With its IoT Security Server securing connected objects, their communications and the exchanged data, Atos provides a secure, compliant and scalable solution to face these new challenges. We support your enterprise in this digital journey, allowing you to focus on growing your IoT business

Securing digital transformation

Identity Management for IoT

The IoT Security Server provides functionality for the whole IoT device security management, paramount to control the lifecycle of your devices and networks.

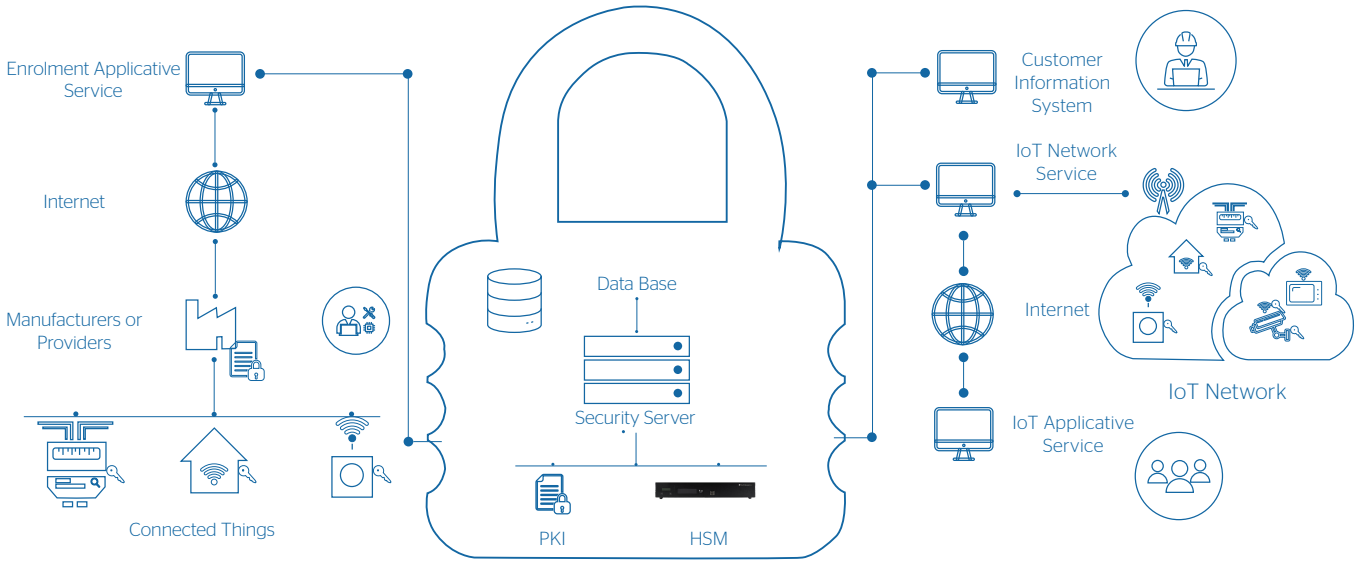
Manufacturers can rely on it to securely distribute devices' keys and certificates, while the inner database mechanisms coupled with Atos HSM product makes it easy to store device related information in a secure way. Such information is vital to provide full protection of data at rest, and to guarantee secure device communications.

Accompanying Growth

Atos IoT Security Server's modularity enables the smooth deployment of a solution tailored to your organisation's needs. The IoT Security Server can also be integrated with different partners to build a complete end-to-end IoT security solution to deploy and monitor security in infrastructures, networks and applications (e.g., through an IoT SOC).

A Leader in IoT Security

As a cybersecurity leader, Atos provides consultancy, along with training and support services, to define the best way to integrate and operate the IoT Security Server into your Information System or IoT platform. The IoT Security Server can be deployed on premise or in SaaS mode, and may be hosted in secure data centres managed by Atos.



End-to-end Security for LoRaWan

IoT Security Server Features

- Enrolment of connected devices to obtain keys associated with their use and management of their lifecycle (creation, consultation, suspension and deletion). Import of keys provided by the manufacturers or generation by the Security Server.
- Computation of connected device keys on demand for specific use for maximum security guarantee Processing of applicative session exchanged business applications (session key can be encrypted).
- Symmetric encryption (3DES/AES) and asymmetric encryption (RSA/ECDSA).
- Signature and/or encryption of exchanges with manufacturers and/or operators.
- Flexible and evolving solution managing the routing of commands and the various available exchange protocols (HTTP(s), SFTP, SOAP, RESTFul, Web Socket).
- Graphical interfaces provided for HSM and IoT Security Server administration, master key management in HSMs and devices keys, management of manufacturers and/or operators allowed to manipulate devices data, and configurations specific to LoRaWAN.
- Support of communication with a PKI service to obtain certificates Support of load balancing mode to address several HSMs.

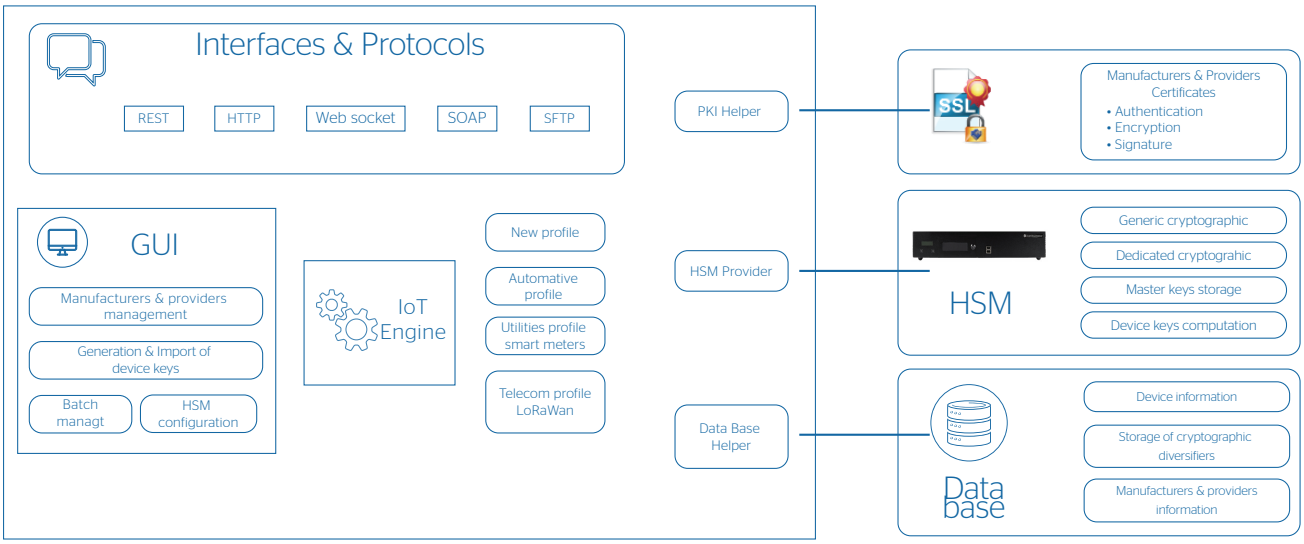
Scalability and Performance

The IoT world is constantly growing and experts are predicting the number of connected devices to reach tens of billion by 2025 (e.g., 40 billion according to IDC). The solution made by Atos is designed to be highly scalable (multiple active instances within a possible redundant architecture) to meet this significant upcoming growth.

Atos Digital Identity

The IoT Security Server is fully integrated to Atos IoT security solutions, which include:

- IDnomic for Objects to distribute certificates to connected devices and to the different entities of the IoT solution,
- Trustway HSM for IoT,
- CardOS Secure Elements for IoT device embedded security.



Supported LoRaWAN features

Network Services	Join/Rejoin and VeryMIC Requests
Applicative Services	GetAppSKey Requests
Device Management	Device enrolment, life cycle management Manufacturer management
Compliant	With LoRaWAN 1.0 and LoRaWAN 1.1

Multiple deployment models

As a Service on shared or private instances (Atos or public cloud hosting
On-premise hosting

Environments

Hardware and Software for IoT Security Server Hosting	
Physical Servers	32/64 bits platform with at least 4 Go of RAM, 10 Go of available disc memory, 2 Ethernet ports
Virtual Machines	VMWare or Hyper-V
Operating Systems	Red Hat 6 or 7 (32 or 64 bits)/SUSE SLES 10 or 11 (32 or 64 bits)
Data Base	Cassandra (external base in 3-tiers architecture)
Workstation for Administrators	
Browsers	Firefox or Chrome
Operating Systems	Windows 10
HSM	
HSM with LoRaWAN dedicated functions for performance optimization: Trustway HSM for IoT	

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

Let's start a discussion together

CT-201105-AS-Fs-IDnomic_Security_server_LoRa_en2