keynetic

Smart Grids
Our solutions to secure them

The highlights

- Cybersecurity in **Industrial Control Systems (ICS)** is essential, since cyberattacks can affect not only he production system but also the integrity of operations.
- Attackers are highly attracted to these kinds of attacks and **numerous infrastructures have already been assaulted in recent years**, such as systems for electric power grid and water treatment.

The electric power industry, which includes the generation, transmission and distribution of electric power, is a highly regulated and standardized industry. In this regard, the International Electrotechnical Commission (IEC) has published the **IEC 62351** standard for **data and communications security** in the context of power systems management and associated information exchange.

Keynetic is committed to the development of tools compliant with IEC standards to provide solutions to **secure Smart Grids** and **protect critical infrastructure** from cyberattacks. We build IEC 62351-9 compliant agents for Intelligent Electronic Devices (IED), and Public Key Infrastructure (PKI) and Key Distribution Center (KDC) servers for power management equipment, aware of how critical it is to ensure the root of trust infrastructure of our customers.

Electric Power Grid systems are under attack

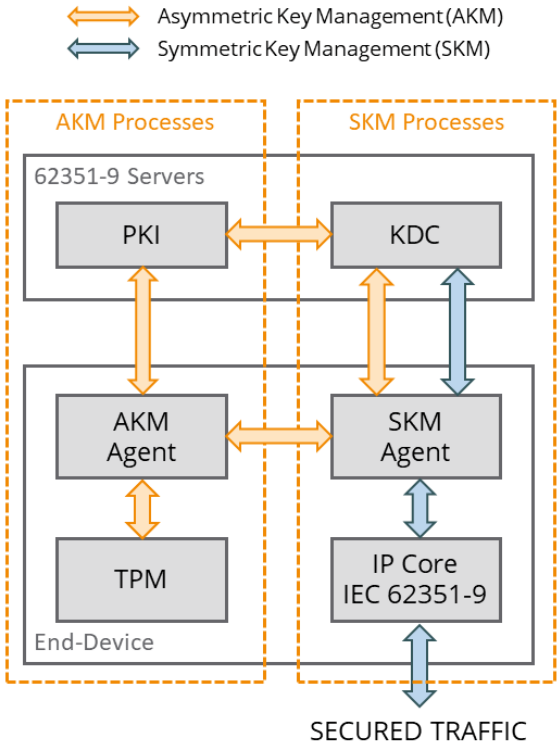
During the last years, critical infrastructures worldwide have suffered several cyberattacks, such as the electric power grid or water treatment systems. The impact of this type of attacks is critical, since it not only affects the production and the integrity if operations, but also directly affects citizens' quality of life.

Attackers are very attracted to these systems due to the impact and consequences, which makes them highly valuable. Thus, cybersecurity is essential for these infrastructures and, in general, in any Industrial Control Systems (ICS).

IEC 62351-9 standard

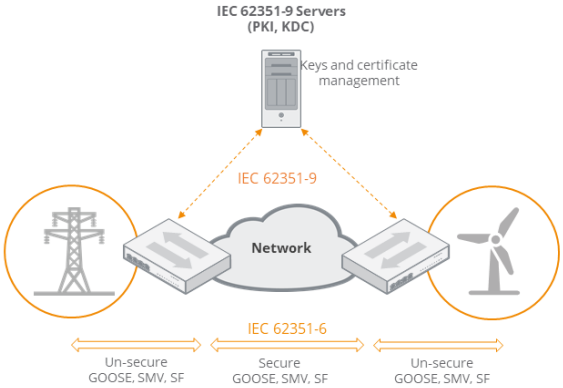
In order to secure critical infrastructures, the International Electrotechnical Commission (IEC) published the **IEC 62351 standard** to increase the security of interconnected power systems. This standard, developed by WG 15 of IEC TC57, includes a set of technical specifications that covers different aspects for handling the security and protection of communications in this sector, suchas communication network and system security (profiles including TCP/IP and MMS), security for IEC 60870-5 and IEC 61850, role-based access control, and key management for power system equipment. It also covers more general aspects, such as security architecture guidelines, and resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems.

Specifically, the **IEC 62351-9** specification deals with the **cryptographic key management** for the IEC 61850 power utility automation. It proposes a hybrid approach where an **asymmetric part** deals with the generation, distribution, revocation and handling of public-key certificates, and a **symmetric part** responsible for group key distribution (based on GDOI protocol, RFC 8052) of symmetric keys.



We build IEC 62351-9 compliant solutions for you

Keynetic can help you with the adoption of the IEC 62351-9 standard. We can provide you with **IEC 62351-9 compliant agents for IEDs**, and **PKI and KDC** servers for power management equipment to deal with the key and certificate management necessary to secure your Smart Grid. The **key management** involves the generation, distribution and revocation of public-key certificates and cryptographic keys.



About us

Keynetic is an innovative cybersecurity SME that develops their own products for network security and intelligence by leveraging the most advanced Software-Defined Networking and Network Functions Virtualization (SDN/NFV), Network Automation and Machine Learning technologies.

We envision network security as an iterative process – visualization & control – that begins with the understanding of the network dynamics and the interactions between your devices. The actual data extracted from the network devices guides this procedure. Thanks to ML technology the time and effort invested in this process is drastically reduced.