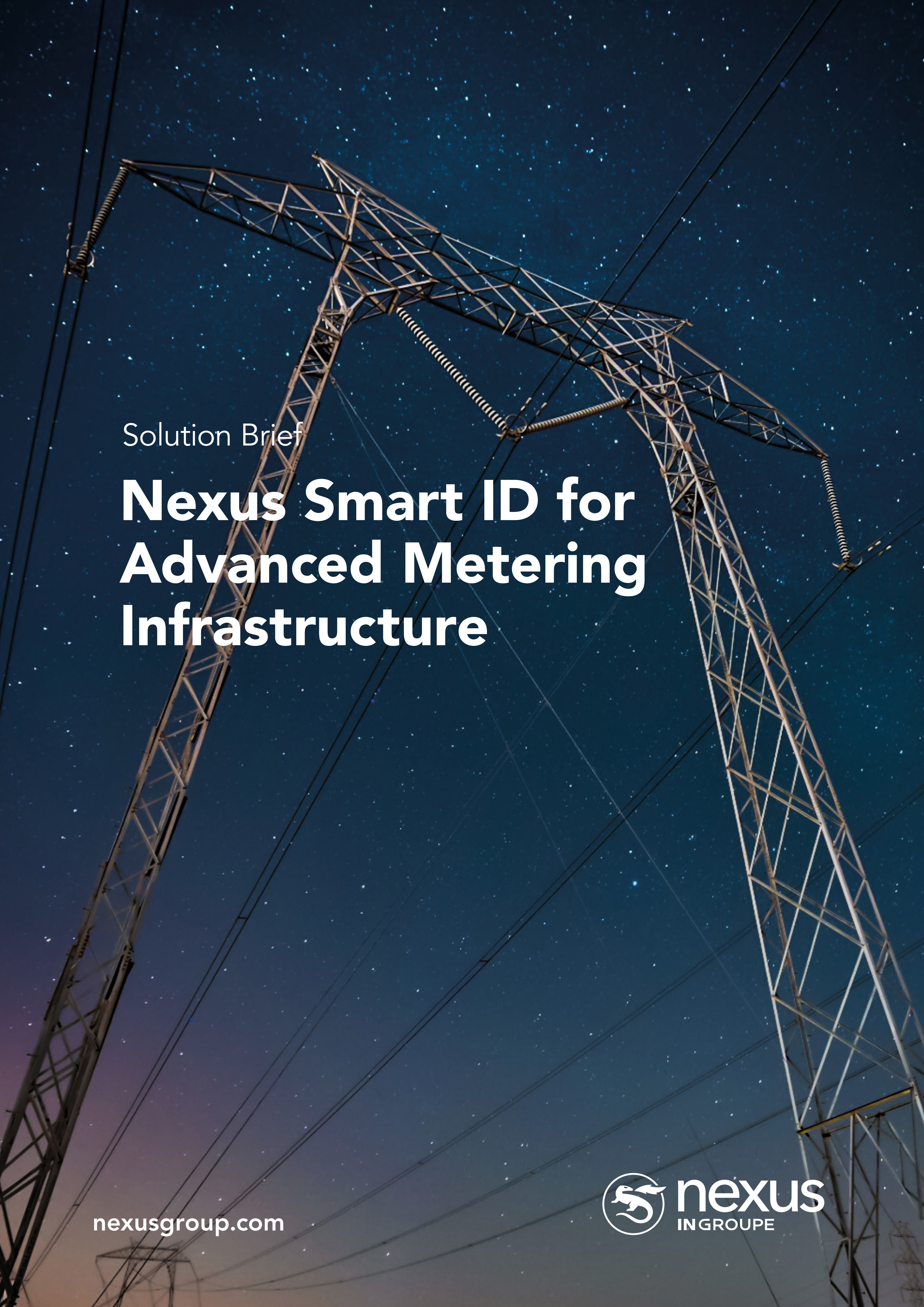


Solution Brief

Nexus Smart ID for Advanced Metering Infrastructure

nexusgroup.com

nexus INGROUPE

Introduction

Nowadays, smart metering is an Internet of Things (IoT) application for most electric power utilities. The term Advanced Metering Infrastructure (AMI) refers to systems that measure, collect, and analyze energy usage, and communicate with metering devices such as electricity meters, gas meters, heat meters, and water meters - a key building block of a smart grid.

Like for many other IoT applications, connecting electricity meters to the Internet to enable them to transmit data to a backend system, i.e., making them "smart", brings enormous benefits. It allows the electric power utility to perform remote meter reading, power outage detection and diagnostics, and much more, and is an enabler for a smart grid where business decisions are taken automatically in real-time based on analysis of the meter collected data. Also, the consumers benefit from AMI, as it brings better energy usage awareness, quicker resolution of power failure issues, improved power quality and bill accuracy, and much more.

Importance of securing the AMI

IoT brings not only benefits, but it unfortunately also comes with increased security threats and aspects to consider. Enabling smart meters and other components in the AMI to communicate with a remote backend means a more open system with a bigger attack surface and more entry points for cybersecurity attacks.

For any electric power utility implementing AMI, it is of utmost importance to protect it from malicious parties. The reasons for this are many, including:

Business value

AMIs are based on receiving accurate data from the smart meters. Analysis of the received data is the basis for intelligent decisions that drive the business. The data is used for business-critical processes including energy demand and production monitoring, grid balancing based on load shifting, customer billing, and more.

It is essential that the data is accurate, trustworthy, and protected.

Cyber attacks

There could be many different intentions with an AMI cybersecurity attack, for instance:

- Cheating the system to get cheaper or free electricity
- Blackmailing power utility for money
- State critical infrastructure terrorism

Hence, a cybersecurity breach in a smart grid can have devastating consequences, economically for the electric power utility, but also for many other parties as the power grid constitutes a nation’s critical infrastructure.

Compliance

Power utilities must comply with stringent security regulations to ensure that the critical infrastructure energy system is always protected and available. Failing to implement robust cybersecurity measures can lead to huge fines under applicable regulations, e.g., under the EU’s Network and Information Systems (NIS) directive.

Standards and regulations

There are many security regulations and standards for smart metering security for different countries and parts of the world. They are typically very thorough and include requirements on device identity authentication, device and data integrity and data confidentiality, and more.

On the international level, DLMS (Device Language Message Specification)/COSEM (Companion Specification for Energy Metering) is a suite of standards developed and maintained by the DLMS User Association (DLMS UA) that has been adopted by the International Electrotechnical Commission (IEC) into the IEC 62056 series of standards. COSEM includes a set of specifications that defines the transport and application layers of the DLMS protocol.

DLMS/COSEM provides three security suites covering e.g., public key based authenticated encryption, digital signature, key agreement, hashing and key transportation: suites 0, 1 and 2.

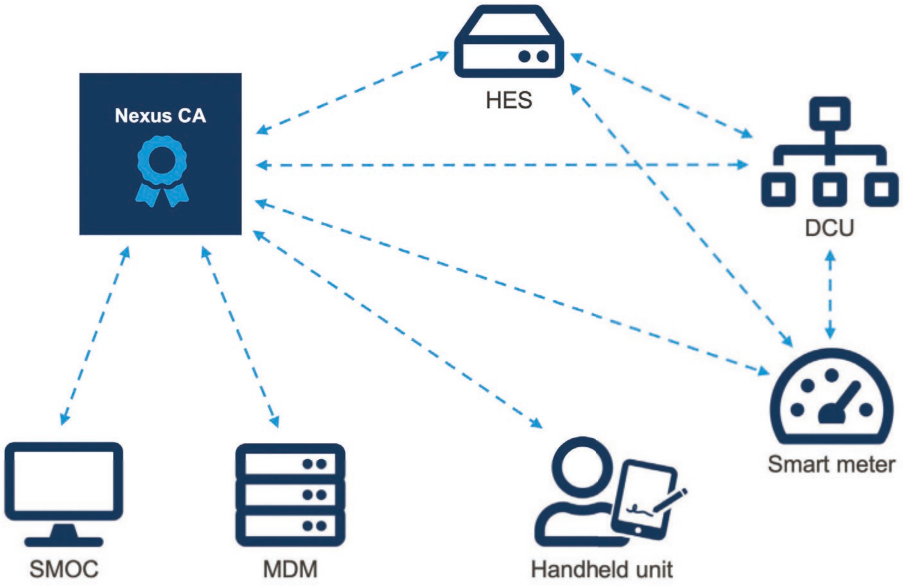
Nexus solution

Nexus Smart ID IoT is a Certificate Authority (CA) product enabling a Public Key Infrastructure (PKI) that constitutes the foundation for a trusted and secure smart grid.

Like people need trusted credentials, e.g., passport or smartcards, to prove their identity, machines use digital certificates to authenticate themselves. Trusted, unforgeable identities provisioned to each device in an IoT application, are the foundation for trusted and secure communication. PKI-based digital certificates constituting such identities enable authentication, data integrity and data confidentiality and have been used for decades to protect various systems and applications.

With a properly implemented PKI in the smart grid, the following can be guaranteed:

– each communicating device really is the device it claims to be (authentication)
– any alteration of transmitted data is detected by the recipient (data integrity)
– only the intended recipients can interpret the transmitted data (data confidentiality)

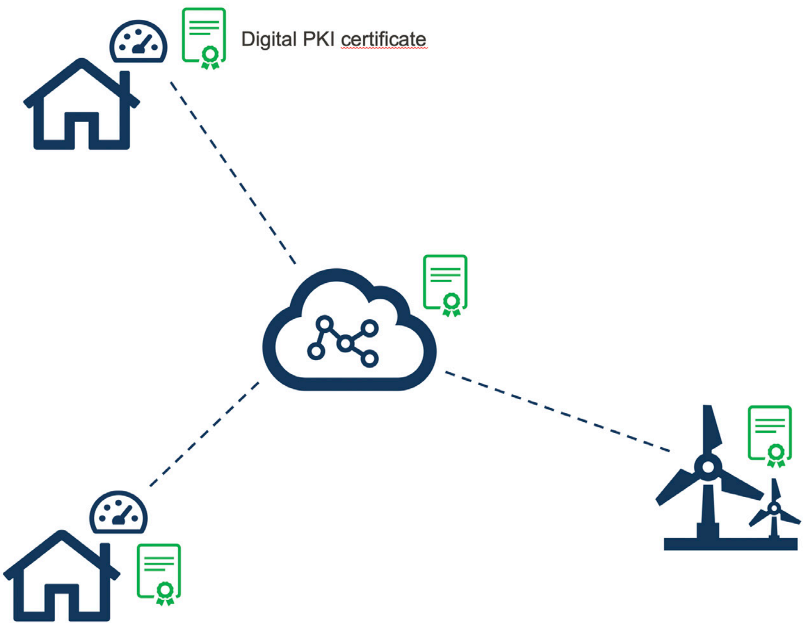


Extension to full Key Management System (KMS)
In addition to PKI, symmetric keys may be used to authenticate AMI devices and encrypt device keys at storage. Nexus partners with HSM vendors like Utimaco to provide a comprehensive Key Management System (KMS) that combines PKI with symmetric key management for generation of high quality cryptographic keys and for secure key storage.

Nexus Certificate Manager

The core component of Nexus Smart ID IoT, Certificate Manager, is a generic, mature, reliable, and high-performing CA platform. The software is serving hundreds of customers globally and has issued >1 billion certificates. It offers multi-tenancy and multi-CA possibilities and provides easy CA management and vast integration possibilities supporting multiple certificate formats, crypto algorithms and HSM vendors/ models. All standard certificate management protocols are supported, including, ACME, CMP, EST, EST-coaps, SCEP, etc., and a flexible REST API is available in addition.

Certificate Manager software is Common Criteria EAL4+ certified.



AMI integration

Nexus Smart ID IoT Certificate Manager can be easily integrated into the AMI, including Smart Meters (SM), Gateways, Data Concentration Units (DCU), Head-End System (HES), Smart Meter Operations Control (SMOC) systems and Meter Data Management (MDM) systems, for digital certificate issuing purposes. Also, Handheld units (HHU), used by e.g., operations and maintenance personnel, can be covered.

Using Nexus Smart ID IoT for issuance and lifecycle management of PKI-based trusted identities, an electric power utility can secure their AMI and comply with DLMS/COSEM (suite 0, 1 and 2).

Customer references

Nexus PKI solutions are commercially deployed with multiple power utilities on a global basis to secure Advanced Metering Infrastructure. More information about Smart ID IoT and Advanced Metering Infrastructure security is available on our web site: https://www.nexusgroup.com/smart-id/smart-meter-security/

Do you want to know more? Contact us!

https://www.nexusgroup.com/contact/

nexusgroup.com