Use Case

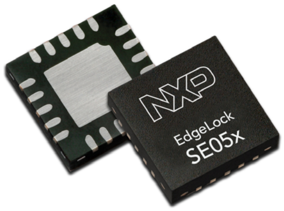
EdgeLock® SE05x secure elements and
EdgeLock A5000 secure authenticator

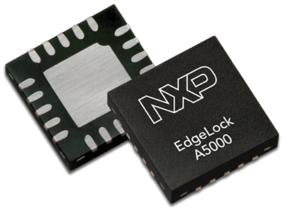
Smart, Secure Energy Management

Smart, Secure Energy Management

Smart meters are attractive targets for cyberattacks because they deal with sensitive information and connect to the broader utility and energy grid infrastructure.

NXP provides comprehensive, third-party certified and standard-compliant protection for smart meters, and even offers solutions tailored for local regulations, such as the Smart Meter Gateway (SMGW).





Applications

Residential

Commercial

Industrial

Challenge

By measuring and recording electricity, gas, or water consumption in real time, and then relaying that information to the utility company, smart meters help analyze trends, optimize grid management, and respond more quickly in emergencies. As part of the energy transition, this is becoming increasingly important as more renewable energy is used that needs to be managed in a smart way. Smart meters and smart meter gateways also lower costs by making it possible to control meters individually or in groups, from a central location, or add and disconnect consumers remotely, without dispatching a technician. Consumers benefit, too, since smart meters make it possible to view real-time usage online, making it easier to find ways to increase efficiency, and save money in residential, commercial, and industrial environments.

At the same time, though, smart meters are some of the most vulnerable components in the utility infrastructure. They're typically mounted in unguarded locations, where they can be easily accessed and manipulated, and represent a potential access point for doing damage to the broader grid.

> **"working with higher volumes of sensitive data increases the need for secure processing and communication"**

Smart meters are also being asked to do more, and this adds to the security requirements. In the electricity sector, for example, the increased use of renewable energy has more buildings being equipped with solar panels that can either direct energy to a standalone battery or to the grid. With a single building acting as a producer and a consumer of energy, the smart meter needs to track both the energy drawn from the grid and the energy sent back to it. Monitoring multiple activities and working with higher volumes of sensitive data increases the need for secure processing and communication.

In some cases, developers may need to add specific security mechanisms to meet regulatory requirements. The globally recognized IEC 62056 standard, for instance, specifies the use of certain cryptographic operations to protect data exchange in smart meters, and there are a number of regional architectures developers may need to deal with, such as the SMGW in Germany. Satisfying the requirements of these various standards and regulations can complicate the design process and make it harder to deliver market-ready products.

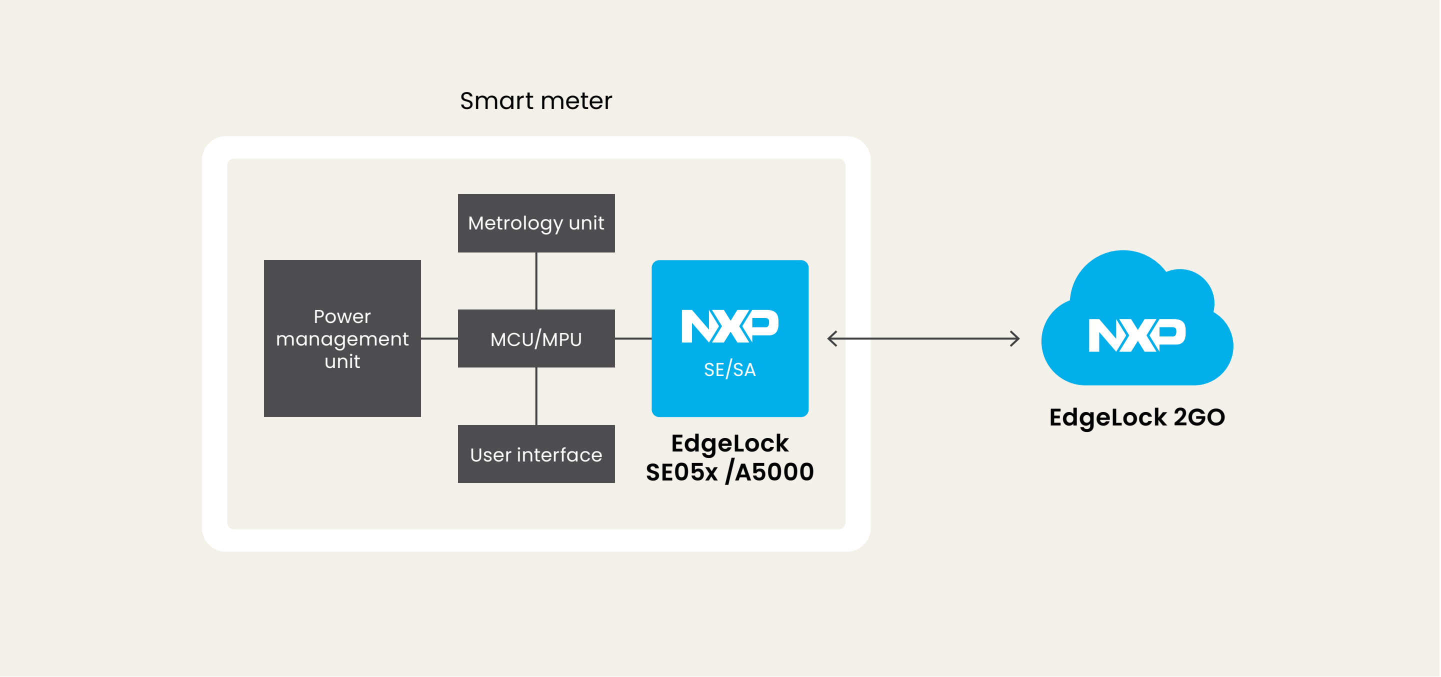
Solution

NXP's industry proven EdgeLock Secure Element and Secure Authenticator portfolio for IoT security includes a range of solutions ideally suited for smart meters. Designed to prevent unauthorized access to meter data, while ensuring secure communication and authenticated transactions, our EdgeLock solutions help developers add high-level security to all kinds of metering devices, including those intended for deployment in specific regions.

- **IEC 62056 (DLMS/COSEM)**
  For smart meters that need to use the DLMS/COSEM standard, as defined by IEC 62056, the NXP EdgeLock SE05x secure element and EdgeLock A5000 secure authenticator meet the DLMS/COSEM requirements for cryptographic algorithms and keys, cryptographic certifications, and cryptographic random-number generation. The EdgeLock SE05x/A5000 provide a secure environment to offload cryptographic operations and protects cryptographic credentials by storing them in tamper-resistant hardware certified to CC EAL 6+. (Details on how to meet the requirements of DLMS/COSEM are provided in NXP Application Note AN13742.)
- **German SMGW**
  For the German market, NXP offers the EdgeLock SE042 secure element. Same as the proven A8000, the EdgeLock SE042 also meets the SMGW requirement for using a hardware security module that supports cryptographic services invoked by the gateway, including generation and storage of a secure key pair, generation and verification of a digital signature, a key agreement for Transport Layer Security (TLS) and data encryption, and random number generation.
- **Other Regions**
  For other regions, including France and the UK, NXP offers tailor-made EdgeLock solutions that meet their specific requirements, too.

Smart meters equipped with NXP EdgeLock SE05x or A5000 work seamlessly with NXP's EdgeLock 2GO cloud service, which lets customers securely manage the credentials of already-deployed meters and update meters as needed to address new security requirements or respond to a security incident. The EdgeLock 2GO service makes it easy to create and manage secure objects, such as symmetric roots of trust, as well as keypairs and certificates, which are then securely provisioned (either remotely or locally) to the EdgeLock SE05x secure element.

Block diagram



Learn more

The NXP Design Community site offers helpful hints, easy-to-follow how to's, and detailed application notes for use with the EdgeLock SE05x/A5000, while our product pages link to detailed specs, designs tools & software, training & support, and more.

NXP Design Community

community.nxp.com/community/identification-security/secure-authentication/overview

EdgeLock SE050 Secure Element

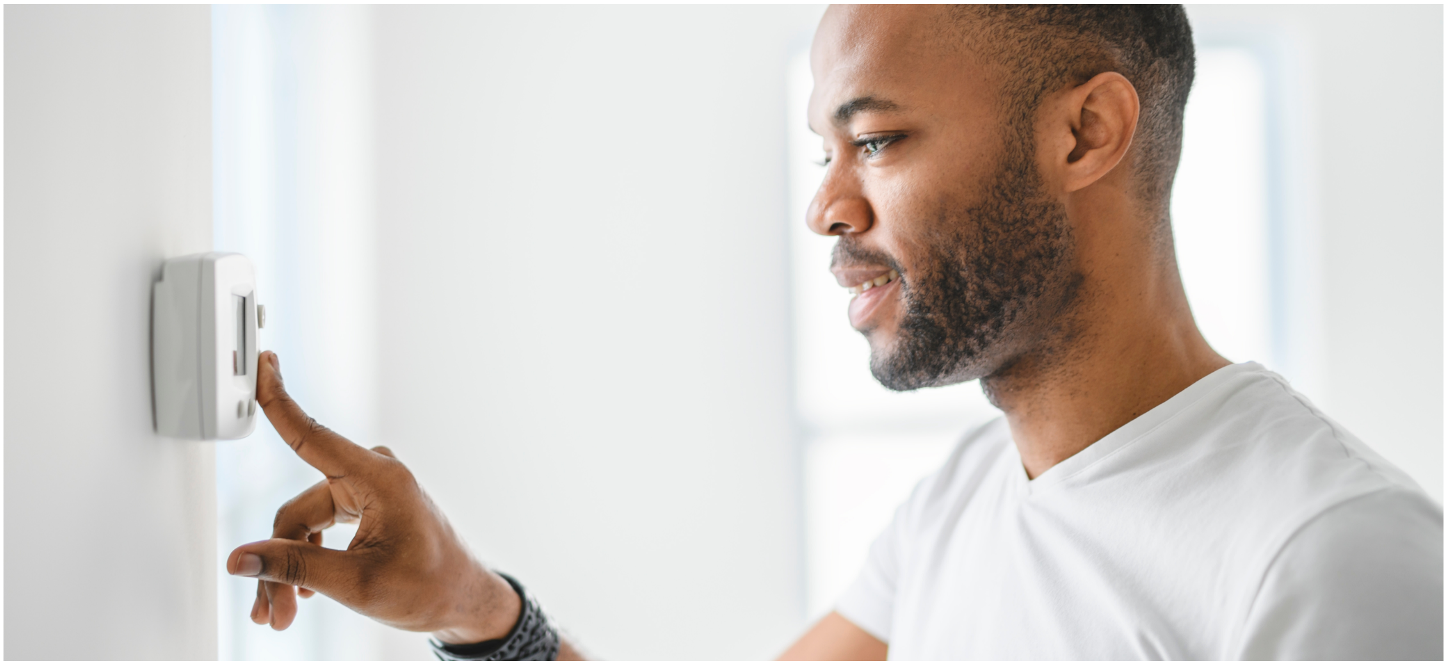
nxp.com/SE050

EdgeLock A5000 Secure Authenticator

nxp.com/A5000

EdgeLock 2GO Service Platform

nxp.com/EgdeLock2GO



Visit nxp.com/iotsecurity