# AN13742

## Secure smart metering with NXP secure solutions

Rev. 1.0 — 7 June 2024 Application note

**Document information**

| Information | Content |
|---|---|
| Keywords | DLMS, COSEM, smart metering, secure element, EdgeLock, SE05x, A5000, EdgeLock 2GO, IEC62056 |
| Abstract | This document describes how NXP secure solutions such as EdgeLock SE05x/A5000 and EdgeLock 2GO can be integrated in smart meters to meet the security requirements mandated by smart metering standards like DLMS/COSEM and even go beyond that. |

# 1 Introduction to smart metering

The delivery of utilities like water, natural gas and electricity to end customers needs to be metered for commercial reasons. Until the late 20th century, resource metering has always been performed mechanically and locally by operators who regularly needed to read the meter's mechanical display, write down the value together with the meter number and send that data to the utility company for accounting and billing. Recently, the availability of electronic sensors as well as storage and data communication technologies makes it possible to consider automating this process.

Smart metering devices, also known as **smart meters** or **advanced meters**, play an essential role in this infrastructure. Typically installed in the consumer premises, smart meters collect and transmit data, such as energy and power consumption readings, to utility suppliers, who can then use this information to predict future demand, detect faults and leakages and get insights on customer consumption patterns. At the same time, through the infrastructure of their utility suppliers, consumers could get access almost in real-time to their consumption data and make informed decisions on how to optimize their consumption and reduce their bills. In the near future, smart meters are even expected to be able to connect to smart home networks to provide to IoT devices real-time data that can be used to trigger intelligent behaviors (e.g., turning on an appliance when electricity is cheaper).

If a household has the capability to store energy and/or feed it into the grid, a smart meter is required to correctly bill the balance between the energy received from the grid versus energy delivered to the grid. This may be the case if solar panels are generating more electricity than what they can consume, or if the electric car's battery is used for temporary grid energy storage.

Since smart meters are one of the main entry points to the utility suppliers' infrastructure, security is an essential requirement to protect smart metering equipment from unintended usage and to protect consumer privacy. In fact, attackers can leverage insecure communication protocols or hardware and software vulnerabilities to manipulate consumption readings or disrupt the normal operation of smart meters. Implementing strong security measures, supported by strong cryptographic credentials and protocols, is therefore an essential requirement in building a secure and reliable smart metering infrastructure.

## 1.1 Architecture of a smart metering system

Even though the architecture of smart metering systems might be heavily influenced by standards and regulations drafted by local governments and regulatory agencies, the architecture of most smart metering systems will be very similar to the **Advanced Metering Infrastructure (AMI)** depicted in Figure 1.

Through an AMI, utility suppliers are able to establish a two-way communication with smart meters and other third party entities with the objective of measuring, collecting and analyzing metering data and providing additional services to their customers. The **DLMS/COSEM specification**, standardized in IEC 62056, is one of the most widely accepted and globally recognized standards for metering data exchange between smart meters and other AMI entities.

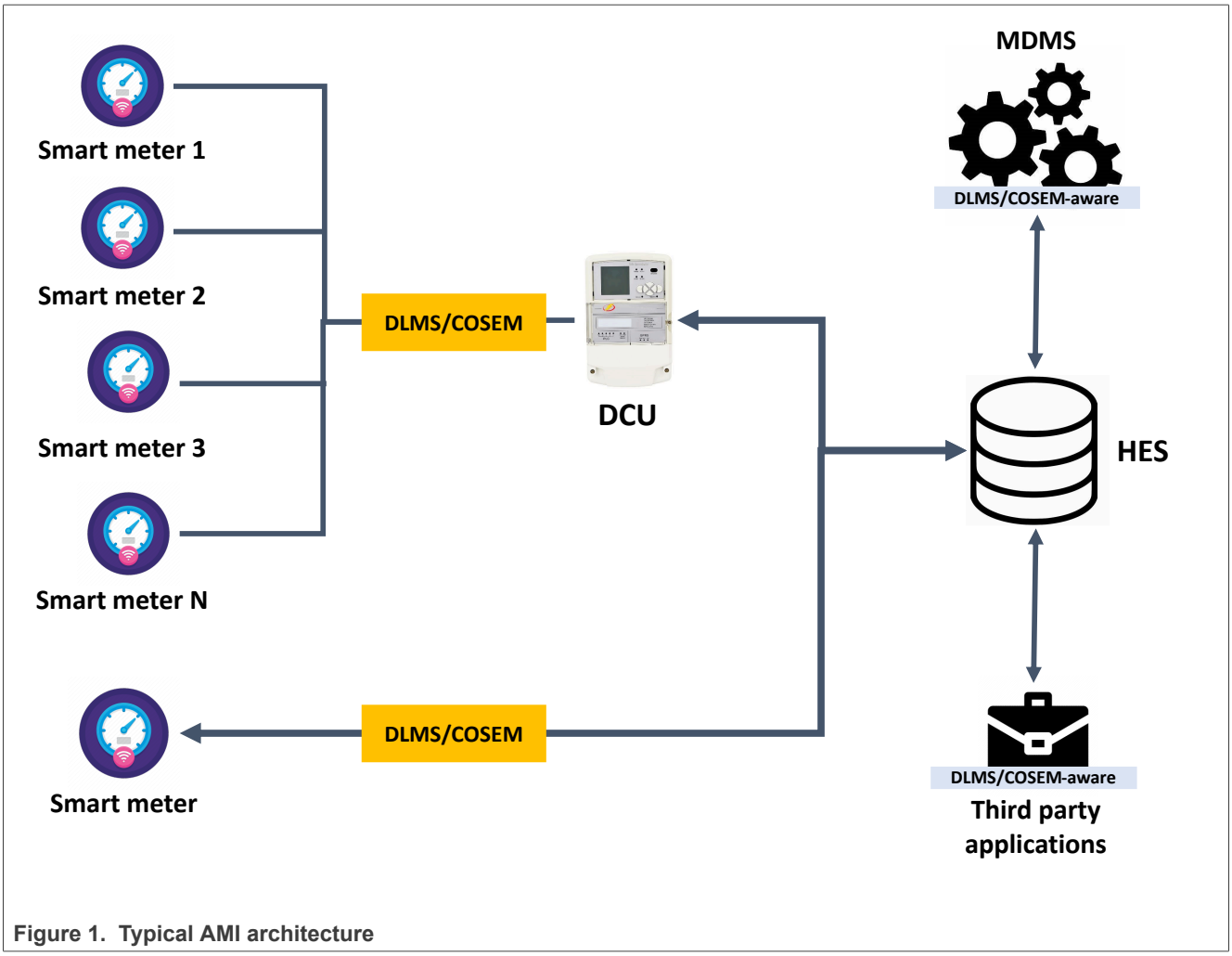


Figure 1. Typical AMI architecture

- **Smart meters** are typically installed in customer premises and through their integrated metrology unit they provide to utility suppliers detailed (real time) readings of resource consumption of a building, business or home. Smart meters can range from very simple devices with few basic functionalities to advanced IoT devices with a wide variety of connectivity interfaces (e.g., WiFi, Bluetooth, NFC, Ethernet), user interfaces (e.g., LCD touch screens) and smart features (e.g., smart home integration). Smart meters can be connected directly to a Head-End System (HES) or to a Data Concentrator Unit (DCU). Management commands and metering data are typically exchanged with other AMI entities using the DLMS/COSEM standard. In some countries like Germany, an additional component called *Smart Meter Gateway (SMGW)* plays a crucial role in the architecture as it acts as intermediary between smart meter devices and the rest of the smart metering infrastructure. For more information on SMGWs and their role in the German smart metering infrastructure, please refer to Section 3.
- The **Data Concentrator Unit (DCU)** is responsible for receiving, storing and aggregating metering data coming from a small group of smart meters (between dozens and thousands of devices) deployed in a Neighbor Area Network (NAN). It acts as an intermediate gateway that relays metering data and control messages between smart meters and higher level systems (typically an HES). DCUs typical functions also include verifying that data has been received successfully from smart meters and confirming that communication links between the DCU and smart meters are intact. DCUs are typically located in physically secure locations such as substations or transformer stations operated by the utility supplier.
- **Head-End Systems (HESs)** are large systems that collect measurement data and meter events from smart meters or DCUs for eventual submission of this data to other AMI entities such as Meter Data Management

Systems (MDMSs) or other third-party applications. Head-end systems may perform a limited amount of data validation before either making the data available for other systems to request or pushing the data out to other systems.

- A **Meter Data Management System (MDMS)** manages all the data received from one or several HESs. Through the MDMS, utility providers can analyze metering data, create valuable data reports, track deployed smart meters, detect issues and faults and forecast future demand, among many other things.
- **Third party applications**, such as smart meter maintenance applications, or utility billing systems, are generally involved in the data exchange of the AMI. DLMS/COSEM supports data exchange between *DLMS/COSEM-aware* third party applications and smart meters through intermediate entities such as DCUs or HESs.

## 1.2 Main security requirements for smart meters

Smart meters are one of the most vulnerable components of an AMI as they are typically mounted in locations where they can be easily accessed and manipulated. The following security considerations are essential to ensure the secure operation of smart meters:

- **Prevent fake or unauthorized smart meters from being installed:** fake or unauthorized smart meters can be deployed in the field by malicious actors to report wrong measurements, to steal sensitive data, or both. For this reason only authorized smart meters should be able to connect to the AMI and use its services. To achieve this, smart meters must be provisioned with unique credentials that are used to authenticate the smart meter to the backend infrastructure (e.g., the DCU or the HES) and prove that the device is indeed authentic. This requirement can be achieved by implementing one of the DLMS/COSEM authentication mechanisms (see Section 2.1 and Section 4.1.1) or other lower layer authentication mechanisms such as Transport Layer Security (see Section 5). Even so, there is also the possibility that the software running on an authentic smart meter is manipulated, modified or substituted by unauthorized actors and use provisioned credentials in an improper way. In this context, specific processes for secure boot and secure firmware update ensure that the software can be trusted when the device is operating (see Section 5).
- **Secure communication:** smart meters need to securely communicate with AMI entities over potentially unsecured networks such as the internet. It is therefore essential that data is appropriately encrypted before it is sent over the network, so only intended recipients can read the data. The DLMS/COSEM standard specifies mechanisms for data encryption at the application layer (see Section 2.1 and Section 4.1.1). Other encryption mechanisms, such as TLS, can be applied at lower layers of the protocol stack.
- **Authenticate transactions:** smart meters generate many transactions, mostly in the form of metering data, which are essential for the correct operation of the network. It is therefore essential to prevent attackers from generating fake transactions. Digital cryptographic signatures are the key enabler to ensure the authenticity of transactions: by using a device-unique private key pre-installed during manufacturing and securely stored in the smart meter, the device can sign transactions that can be later verified by any third party system using the associated public key. The DLMS/COSEM standard defines mechanisms to authenticate transactions so that they can be verified by intended recipients before being accepted (see Section 4.1.1).

## 2 The DLMS/COSEM specifications

**DLMS/COSEM** is a suite of specifications maintained by the DLMS User Association (DLMS UA) that specifies an interoperable, efficient and secure language for smart meter data exchange. It defines an object-oriented data model, an application layer protocol and several communication profiles. DLMS/COSEM has been designed to be communication media agnostic, meaning that application messages can be carried end-to-end between different entities of the system, over virtually any communication media. Since 2002, the DLMS/COSEM specification has been elevated to an international standard by the IEC as part of the **IEC 62056 DLMS/COSEM suite**.

Figure 2 shows the DLMS/COSEM stack and its main components:

- **Companion Specification for Energy Metering (COSEM):** it is an interface to model the functionalities of the smart meter equipment using an object-oriented approach. The COSEM interface models metering equipment as a physical device containing one or more logical devices. For example, a meter could consist of one logical device for electricity metering and another for a connected gas meter. Each logical device may contain a number of COSEM objects, modeling the functionality of the logical device. Objects may have several attributes (e.g., logical name of the device or a value) and also methods to perform operations on the attributes (e.g., modifying the value of a specific attribute). COSEM objects can be used to model simple use cases such as register reading or more complex ones such as tariff and billing schemes. COSEM is specified in *DLMS UA Blue Book* and it is internationally standardized in *IEC 62056-6-2*.
- **Object Identification System (OBIS):** it defines the identification codes for commonly used data items in metering equipment. It provides a unique identifier for all data within the metering equipment, including measurement values, configurations and other information. OBIS is specified in *DLMS UA Blue Book* and it is internationally standardized in *IEC 62056-6-1*.
- **DLMS/COSEM application layer:** it provides the required services to establish a connection between smart meters and other entities. It also provides mechanisms to access data held by COSEM objects stored in smart meters. The DLSM/COSEM application layer is also responsible for building the application layer messages, managing the transfer of long messages in blocks, and applying cryptographic protection when needed. There are also some built-in mechanisms available for optimizing the traffic to the characteristics of the data transmitted. The DLMS/COSEM application layer is specified in *DLMS UA Green Book* and it is internationally standardized in *IEC 62056-6-3*.
- **Communication profiles:** DLMS/COSEM specifies several communication profiles that define lower layer technologies and protocols and how they can be used together with the DLMS/COSEM application layer. Some of the most commonly used communication profiles are TCP/IP and PSTN/GSM with HDLC data link layer. The DLMS/COSEM communication profiles are specified in *DLMS UA Green Book* and are standardized in several parts of *IEC 62056* (e.g., the TCP/IP communication profile is described in *IEC 2Z056-9-7*).

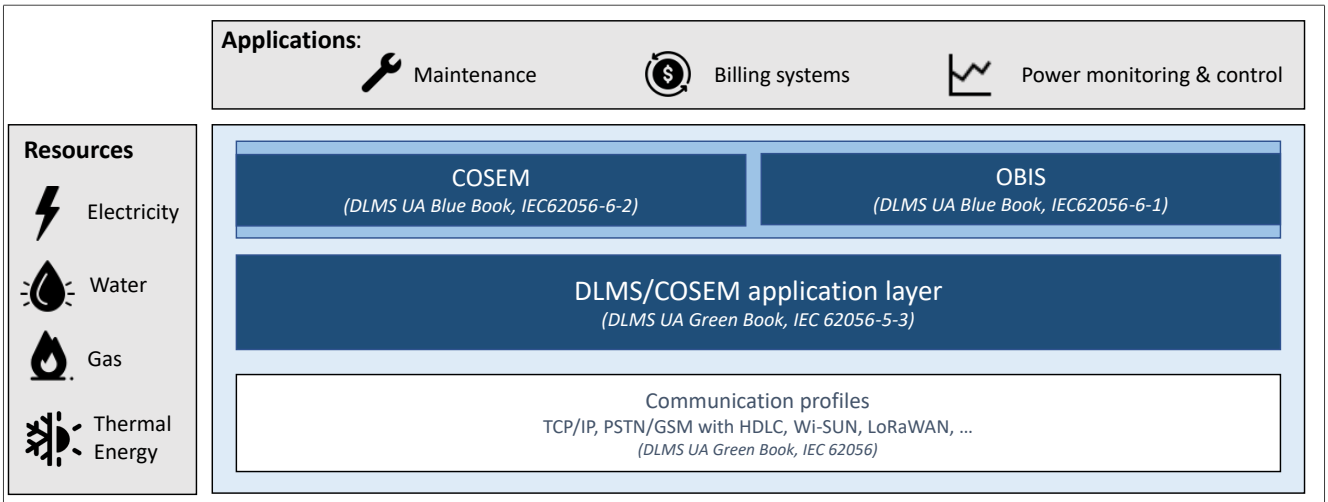


**Figure 2. The DLMS/COSEM stack**

## 2.1 DLMS/COSEM application layer, data exchange and security

The DLMS/COSEM standard uses a client-server approach where smart meters act as servers, and HESs or DCUs act as clients. Clients typically initiate the connection with servers to retrieve the attributes of COSEM objects stored in the server or to execute some methods defined by COSEM objects. The typical DLMS/COSEM communication flow is depicted in Figure 3:

1. **Establishment of a connection in lower layers:** since DLMS/COSEM is an application layer protocol, a connection must first be established between client and server at lower layers of the protocol stack. This can be, for example, a wireless or wired connection using a typical TCP/IP protocol stack. At this stage, lower layers can also establish their own specific security mechanisms to protect communication (e.g., Transport Layer Security (TLS)) which will be independent from additional security mechanisms applied by the DLMS/COSEM application layer.
2. **Establishment of an Application Association (AA):** before any data exchange can start between a DLMS/COSEM client and server, an AA must be established between the two entities. An AA is a logical connection between the client and the server whose purpose is to establish the context of all the following transactions (e.g., the security context defining the security mechanisms supported by the AA). During AA establishment, the client and the server can authenticate using any of the two application-layer authentication methods supported by DLMS/COSEM:
   - **Low Level Security (LLS):** this is the most basic level of authentication. The server only requires that the client authenticates using a password that is known by the server.
   - **High Level Security (HLS):** in this case, client and server must mutually authenticate, so that the client knows that it is communicating with an authorized server and viceversa. Contrary to LLS, HLS requires exchanging cryptographic challenges and the usage of cryptographic algorithms. DLMS/COSEM defines several HLS authentication mechanisms: some of them rely on shared secrets, such as HLS GMAC and HLS SHA-256 authentication mechanisms, others on public key cryptography such as the HLS ECDSA authentication mechanism.
3. **Message exchange with a client using xDLMS APDUs:** once an (authenticated) AA has been established, message exchange can take place. The client can access the attributes and methods of COSEM objects stored in the server through extended DLMS (xDLMS) services. For example, the GET xDLMS service is used by the client to access the value of one or more attributes stored in the server, while the ACTION xDLMS service is used by the client to invoke one or more methods in the server. These xDLMS service primitives are transported from client to server and viceversa using xDLMS Application Protocol Data Units (APDUs) that encode all the required service parameters. xDLMS APDUs can be optionally protected by applying any combination of authentication (data authenticity), encryption (data

confidentiality) and digital signature (data authenticity and integrity). Specific COSEM attributes or method parameters contained in xDLMS APDUs can additionally be protected using a different set of cryptographic keys.

4. **(Optional) Message exchange with third party applications:** optionally, *DLMS/COSEM-aware* third party applications can exchange messages with DLMS/COSEM servers using a DLMS/COSEM client as an intermediary. Communication between third party applications and servers can be protected using the same security mechanisms defined by DLMS/COSEM for client-server communication.
5. **Release of the AA:** as soon as data exchange is completed, the resources associated with the AA can be released and the AA can be closed.

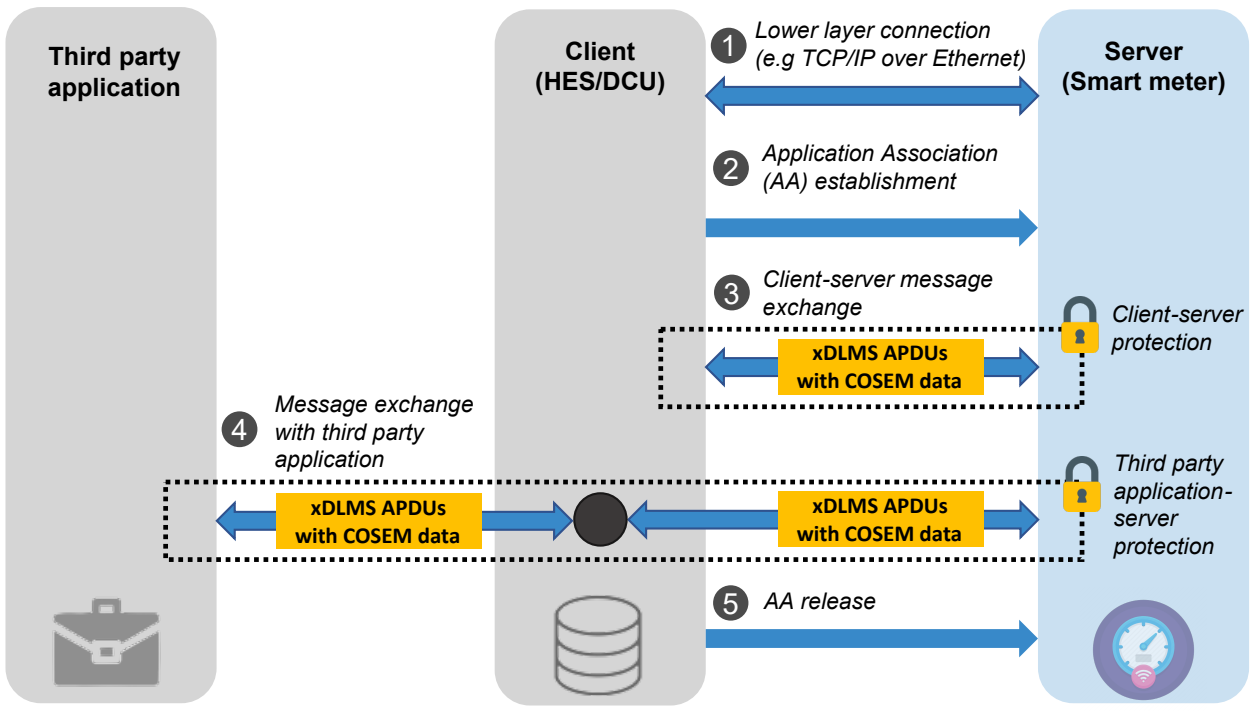


Figure 3. DLMS/COSEM end-to-end data exchange

## 3 Local smart meter regulations: the German case

In the past few years, governments have been moving towards introducing laws and regulations for the safe and secure deployment of smart metering devices. These regulations might force OEMs to implement in smart meters certain standards and protocols (e.g. DLMS/COSEM standard), some of their security provisions or even stricter or different security requirements, configurations and architectures.

With the **Measuring Point Operating Act ("Messstellenbetriebsgesetz", MsbG)**, Germany became one of the first countries to lay out a strict set of operational guidelines and requirements for the roll out of smart energy meters to all consumers with an energy consumption of more than 6000 kWh/year. The technical requirements of a smart metering system complying with the legislation have been drafted by the German Federal Office for Information Security (BSI) which put a particular effort on the definition of strong security provisions that relies on hardware protection and hardware-backed credentials.

The architecture proposed by the BSI, to which all smart metering systems deployed in Germany must adhere to, relies on a centralized component, called **Smart Meter Gateway (SMGW)**, which acts as intermediary between smart meters in the Local Metering Network (LMN) and other entities of the Home Area Network (HAN) or of the Wide Area Network (WAN). The SMGW is responsible, among other things, for collecting, processing and storing the records from smart meters and ensuring that only authorized parties have access to them. In order to protect metering data stored by the SMGW, it is mandated by the regulation that the SMGW implements the security requirements described in the *Protection Profile for Smart Meter Gateways*. In particular, the regulation mandates the usage of a **hardware Security Module (SecMod)** which supports the SMGW for specific cryptographic needs and is responsible for certain cryptographic services that are invoked by the gateway, such as:

- **Secure key pair generation and storage**
- **Digital signature generation and verification**
- **Key agreement for Transport Layer Security (TLS) and data encryption**
- **Random number generation**

Through the services offered by the SecMod, the SMGW must be able to:

- Establish an encrypted and mutually authenticated channel with smart meters and/or other entities as needed;
- Verify both the authenticity and integrity of the metering data received to ensure that data has been sent from an authentic smart meter and has not been altered during transmission;
- Verify the authenticity and integrity of data received from an external entity;
- Apply authenticity and integrity protection measures when sending processed metering data to external entities;
- Protect sensitive data that is permanently or temporarily stored in the SMGW.

All the security requirements of the Security Module, listed and described in the *Protection Profile for the Security Module of Smart Meter Gateways*, can be easily met by integrating a discrete **Secure Element (SE)** in the SMGW. The SE can not only provide a secure, tamper-resistant storage for cryptographic credentials, but also a secure environment for executing cryptographic algorithms for data encryption, signature generation and verification and other cryptographic operations. In this context, NXP provides an SE solution specifically designed to meet all the SecMod security requirements listed in the latest version of the *Protection Profile for the Security Module of Smart Meter Gateways* (version 1.03 at the time of writing).

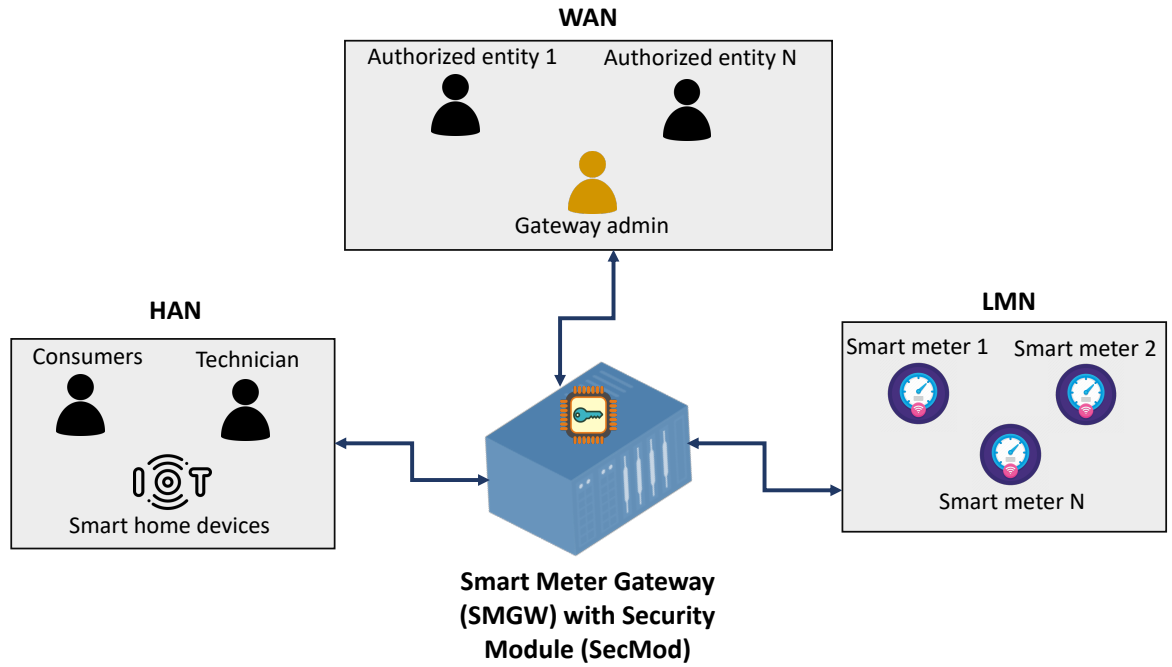


Figure 4. German Smart Metering System

# 4 Introducing NXP secure solutions for smart meters

NXP provides scalable, flexible and secure solutions to develop future-proof smart meters that fulfill the security requirements mandated by DLMS/COSEM and even go beyond that.

Enabling top-notch security on smart meters is as easy as integrating the **NXP EdgeLock SE05x/A5000 secure element**: a ready-to-use SE solution tailor-made for the IoT that provides a secure, CC EAL 6+ certified tamper-resistant hardware to protect mission critical cryptographic credentials as well as a secure environment to offload cryptographic operations. EdgeLock SE05x/A5000 is pre-provisioned with keys and credentials in a highly secure and controlled environment, therefore relieving device manufacturers from setting up a complex and expensive Public Key Infrastructure (PKI). It also comes with a pre-installed applet and a Plug & Trust middleware package that ease the integration of the secure element in the device MCU/MPU. EdgeLock SE05x/A5000 serves the generic market and can help meet the security requirements of the DLMS/COSEM specification. Tailor-made NXP SE solutions are also available to meet the security requirements mandated by specific market and country regulations (e.g., for German, France and UK markets).

To abstract the complexity of key and certificate management in secure elements and authenticators, NXP offers **EdgeLock 2GO**: a fully managed cloud platform that allows customers to create and manage secure objects, such as symmetric roots of trusts, key-pairs and certificates, which are then securely provisioned (either remotely or locally) into the secure elements of IoT devices. This gives customers the flexibility to securely manage the credentials of smart meters already deployed in the field and to quickly and easily update them to meet new security requirements or react to security incidents.

The following sections list the security requirements mandated by DLMS/COSEM that can be met by integrating in smart meters NXP solutions such as EdgeLock SE05x/A5000 and EdgeLock 2GO.

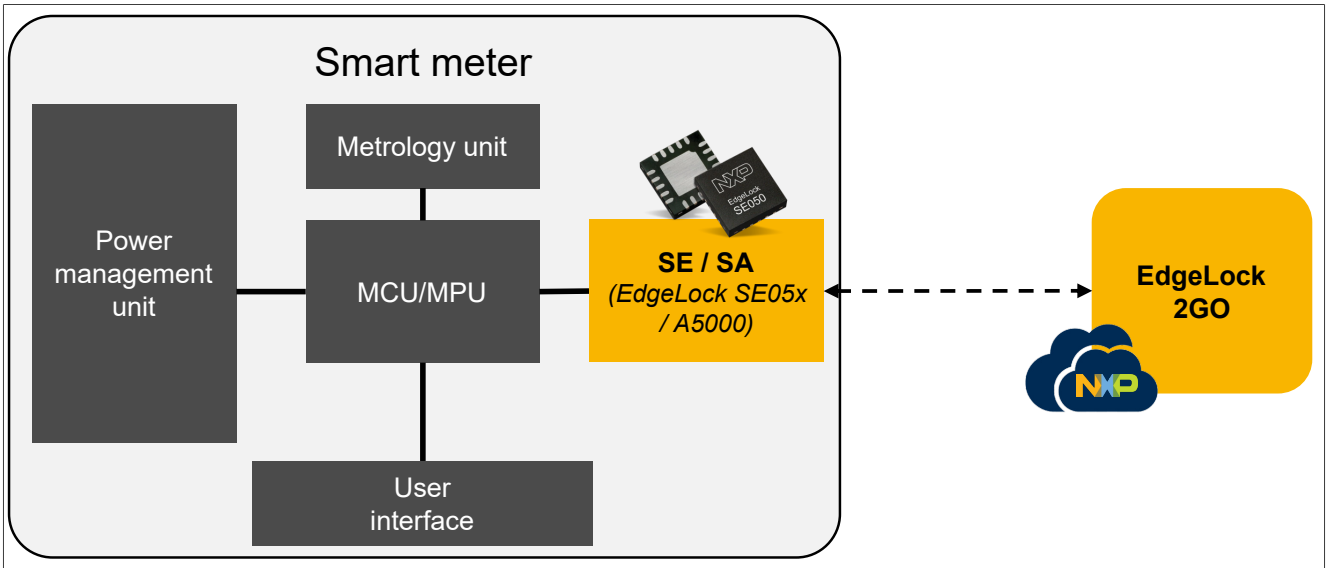


**Figure 5. High level architecture of a smart meter**

## 4.1 Meet DLMS/COSEM security requirements with NXP solutions

The security requirements of the DLMS/COSEM standard can be grouped in the following categories:

- Cryptographic algorithms and keys
- Cryptographic certificates
- Cryptographic random number generation

For each category, the specific requirements of the standard are listed and we will explain in detail how to meet those requirements by integrating NXP secure solutions in smart meters. A list of relevant demos, examples, APIs and documentation will be provided to help meet the requirements using NXP secure solutions.

***Note:*** *only security requirements that can be fully or partially met with NXP solutions are listed in the next sections. For a complete list of requirements, please refer to the DLMS/COSEM application layer specification (DLMS UA Green Book or IEC 62056-6-3).*

### 4.1.1 Cryptographic algorithms and keys

The DLMS/COSEM application layer relies on a set of cryptographic keys and algorithms to implement the security mechanisms described in Section 2.1 (mutual authentication, data integrity and authenticity, data encryption). Table 1 lists the requirements mandated by DLMS/COSEM for cryptographic keys and algorithms that can be used in smart meters (DLMS/COSEM servers).

**Table 1. DLMS/COSEM cryptographic keys and algorithms requirements**

| Category | Requirement | IEC 62056-5-3 sections |
|---|---|---|
| **Cryptographic algorithms** | Whenever security is required for HLS authentication or for protecting xDLMS APDUs, DLMS/COSEM entities shall use one of the security suites listed in Table 2:<br>• The Advanced Encryption Standard (AES) shall be used as specified in FIPS PUB 197, with key sizes of 128 and 256 bits. AES algorithm shall be used with the Galois/Counter Mode (GCM) as specified in NIST SP 800-38 D:2007.<br>• For message integrity and authentication, the GMAC algorithm shall be used.<br>• The Elliptic Curve Digital Signature Algorithm (ECDSA) shall be used as specified in FIPS PUB 186-4:2013 and in NSA1, using the curves P-256 and P-384.<br>• Key agreement shall be done using Elliptic Curve Diffie-Hellman (ECDH) algorithm using P-256 or P-384 elliptic curves according to NIST SP 800-56A Rev.2: 2013.<br>• The Secure Hash Algorithms (SHA) SHA-256 and SHA-384 shall be used as specified in FIPS PUB-4:2012.<br>• For wrapping key data, DLMS/COSEM has selected the AES Key Wrap algorithm (128 or 256 bits) according to RFC 3394. | Section 5.3.7<br>Section 5.3.3.8 |
| **Cryptographic keys** | DLMS/COSEM defines a set of symmetric keys that can be established in a DLMS/COSEM server:<br>• Master Key, KEK<br>• Global Unicast Encryption Key (GUEK)<br>• Global Broadcast Encryption Key (GBEK)<br>• (Global) Authentication Key (GAK)<br>• Dedicated key<br>• Ephemeral encryption key | Section 5.5.1 |
| | The symmetric keys that can be established using key-wrapping may be the KEK, the GUEK, the GBEK, the GAK. | Section 5.5.4 |
| | The symmetric keys that can be established using keya-agreement may be the KEK, the GUEK, the GBEK, the GAK and the Ephemeral encryption key. | Section 5.5.5 |
| | DLMS/COSEM entities should store the following asymmetric key-pairs:<br>• Digital signature key pair<br>• Ephemeral key agreement key pair<br>• Static key agreement key pair | Section 5.6.1 |

**Table 2. DLMS/COSEM security suites**

| Security suite | Authenticated encryption | Digital signature | Key agreement | Hash | Key transport |
|---|---|---|---|---|---|
| **Suite 0** (*AES-GCM-128*) | AES-GCM-128 | - | - | - | AES-128 key wrap |
| **Suite 1** *(ECDH-ECDSA-AES-GCM-128-SHA-256)* | AES-GCM-128 | ECDSA with P-256 | ECDH with P-256 | SHA-256 | AES-128 key wrap |
| **Suite 2** *(ECDH-ECDSA-AES-GCM-256-SHA-384)* | AES-GCM-256 | ECDSA with P-384 | ECDH with P-384 | SHA-384 | AES-256 key wrap |

EdgeLock SE05x/A5000 allows smart meters to securely generate and store credentials as secure objects inside its secure CC EAL6+ certified tamper-resistant hardware. Cryptographic operations involving secure objects are always performed inside the SE protected environment using built-in cryptographic functions and algorithms implemented by the pre-installed IoT applet. Supported algorithms include:

- **ECDSA and SHA-256/SHA-384 for signature operations** as required by DLMS/COSEM *security suite 1* and *security suite 2*;
- **ECDH/ECDHE for key agreement** as required by DLMS/COSEM *security suite 1* and *security suite 2*;
- **AES-GCM** and **GMAC** for authenticated encryption as required by DLMS/COSEM *security suite 0*, *security suite 1* and *security suite 2*;
- **AES-128/256 key unwrap** according to RFC3394 as required by DLMS/COSEM *security suite 0*, *security suite 1* and *security suite 2*

Private keys will never leave the boundaries of the SE. EdgeLock SE05x/A5000 natively supports the generation of device-unique symmetric (AES, DES) and asymmetric keys (ECC, RSA) directly inside the secure environment provided by the SE. **ECC keys with high key length (up to 512 bits) and future-proof curves are natively supported, including *P256* and the more secure *P-384* curve**. All credentials stored in the SE can be protected against deletion and overwriting using policies. Through policies, credential usage can be limited as well (e.g. a key-pair can be used only for signing operations).

EdgeLock SE05x/A5000/A5000 is pre-provisioned for ease of use in NXP's secure facilities with a set of device-unique key-pairs that can be used to establish the initial root of trust of the device. In case the OEM needs to provision different credentials than the ones securely provisioned by NXP, they can be manually created and injected in EdgeLock SE05x/A5000/A5000 or remotely generated and securely provisioned through the EdgeLock 2GO platform.

**Table 3. NXP material: DLMS/COSEM cryptographic algorithms**

| NXP material | Specification |
|---|---|
| **Plug & Trust middleware APIs** | • **Get handle of (pre)provisioned keys or objects:** sss_se05x_key_object_get_handle(), sss_key_store_get_key ()<br>• **Key creation:** sss_se05x_key_store_generate_key ()<br>• **Key import / injection:** sss_key_store_set_key(), Se05x_API_WriteECKey ()<br>• **Asymmetric sign / verify:** sss_asymmetric_sign_digest (), sss_asymmetric_verify_digest ()<br>• **Asymmetric encrypt / decrypt:** sss_asymmetric_encrypt (), sss_asymmetric_decrypt ()<br>• **Symmetric operations:** sss_cipher_crypt_ctr (), sss_cipher_one_go (), sss_cipher_one_go_v2 ()<br>• **Key agreement:** sss_se05x_derive_key_dh ()<br>• **Hash operations:** sss_digest_one_go ()<br>• **Authenticated encryption:** sss_aead_one_go () |

Table 3. NXP material: DLMS/COSEM cryptographic algorithms*...continued*

| NXP material | Specification |
|---|---|
| **Plug & Trust middleware demos and examples** | • **Using policies for secure objects demo:** \simw-top\demos\se05x\se05x_policy<br>• **ECC sign and verify example:** \simw-top\sss\ex\ecc<br>• **ECDH key generation**: \simw-top\sss\ex\ecdh<br>• **Symmetric cryptography using AES example**: \simw-top\sss\ex\symmetric<br>• **Concurrent ECC example:** \simw-top\demos\se05x\se05x_ConcurrentEcc<br>• **Concurrent symmetric example:** \simw-top\demos\se05x\se05x_ConcurrentSymm<br>• **EdgeLock 2GO Agent examples:**\simw-top\nxp_iot_agent\ex |

### 4.1.2 Cryptographic certificates

The DLMS/COSEM application layer relies on cryptographic certificates to implement some of the security operations described in Section 2.1. Table 4 lists the requirements mandated by DLMS/COSEM for cryptographic certificates that can be used in smart meters (DLMS/COSEM servers).

Table 4. DLMS/COSEM cryptographic certificates requirements

| Category | Requirement | IEC 62056-5-3 sections |
|---|---|---|
| **Cryptographic certificates** | DLMS/COSEM servers shall be provisioned with one or more trust anchors (root-CA certificate, Sub-CA certificate, directly trusted key) during manufacturing using a trusted Out-of-Band (OoB) channel. | Section 5.6.3.2<br>Section 5.6.6.2 |
| | DLMS/COSEM trust anchors (root-CA, Sub-CA) can be exported, but they cannot be imported or removed. Directly trusted CA keys cannot be exported. | Section 5.6.6.2 |
| | DLMS/COSEM servers may be provisioned with their own certificates and certificates of CAs, DLMS/COSEM clients and third parties. This may happen using a trusted OoB process or through the *Security setup* object. | Section 5.6.3.2 |
| | Every DLMS/COSEM server must use X.509 v3 certificate format and contain either:<br>• a P-256 or P-384 ECDSA-capable signing key; or<br>• a P-256 or P-384 ECDH-capable key agreement key | Section 5.6.5 |
| | Every certificate shall be signed using ECDSA. The signing Certification Authority (CA) key shall be P-256 or P-384 if the certificate contains a key on P-256. The signing CA's key shall be P-384 if the certificate contains a key on P-384. | Section 5.6.5 |
| | Depending on the security suite, the X.509 v3 certificates listed in Table 5 shall be handled by DLMS/COSEM end entities. | Section 5.6.5 |
| | Subject unique IDs may optionally be used in end devices certificates. | Section 5.6.4.3.6 |

**Table 5. DLMS/COSEM certificates**

| Security suite | Certificates | Public key | CA's signature key |
|---|---|---|---|
| **Suite 1** *(ECDH-ECDSA-AES-GCM-128-SHA-256)* | Root-CA | P-256 | P-256 |
| | Sub-CA | | |
| | End-Entity Signature Certificate | | |
| | End-Entity Key Establishment Certificate | | |
| | End-Entity TLS Certificate *(Optional)* | | |
| **Suite 2** *(ECDH-ECDSA-AES-GCM-256-SHA-384)* | Root-CA | P-384 | P-384 |
| | Sub-CA | P-256 or P-384 | |
| | End-Entity Signature Certificate | | |
| | End-Entity Key Establishment Certificate | | |
| | End-Entity TLS Certificate *(Optional)* | | |

EdgeLock SE05x/A5000/A5000 allows smart meters to securely generate and store certificates as secure objects inside its secure CC EAL6+ certified tamper-resistant hardware. Moreover, all certificates stored in the SE can be protected against deletion and overwriting using secure object policies.

EdgeLock SE05x/A5000/A5000 is pre-provisioned for ease of use in NXP's secure facilities with a set of keys and certificates that can be used to establish the initial root of trust of the device. It is also pre-injected with a device-unique, read-only 7-byte UID that can be used to identify the smart meter. A custom identifier can also be injected in EdgeLock SE05x/A5000/A5000 and protected against deletion and overwriting using the appropriate policies. In case the OEM needs to provision different credentials and certificates than the ones securely provisioned by NXP, they can be **manually created and injected in EdgeLock SE05x/A5000/A5000 or remotely generated and securely provisioned through the EdgeLock 2GO platform**.

The EdgeLock 2GO platform allows users to generate asymmetric key pairs (including P-256 and P-384) and their associated certificate and provision them securely into the SE of the device from the cloud. Client certificates generated by EdgeLock 2GO can be signed by the NXP root CA using the ECDSA algorithm. Alternatively, it is also possible to use a custom root CA. In both cases, keys are securely generated by EdgeLock 2GO and stored in EdgeLock 2GO secure hardware storage so users don't have to manage their own PKI. By integrating EdgeLock 2GO in smart meters it becomes easy to rotate keys and certificates; for example to react to a security incident or to keep up with evolving standards and local regulations.

**Table 6. NXP material: DLMS/COSEM cryptographic certificates**

| NXP material | Relevant content |
|---|---|
| **Plug & Trust middleware APIs** | • **Get handle of (pre)provisioned keys or objects:** sss_se05x_key_object_get_handle(), sss_key_store_get_key ()<br>• **Key / object creation:** sss_se05x_key_store_generate_key ()<br>• **Key / object import / injection:** sss_key_store_set_key()<br>• **Read EdgeLock SE05x pre-injected UID:** Se05x_API_ReadObject( kSE05x_AppletResID_UNIQUE_ID ) |

Table 6. NXP material: DLMS/COSEM cryptographic certificates*...continued*

| NXP material | Relevant content |
|---|---|
| **Plug & Trust middleware demos and examples** | • **Inject Certificate into SE example**: \simw-top\demos\se05x\se05x_InjectCertificate<br>• **Get Certificate from the SE**: \simw-top\demos\se05x\se05x_GetCertificate<br>• **Get Info example** (retrieve SE UID): \simw-top\demos\se05x\se05x_GetInfo<br>• **Using policies for secure objects demo:** \simw-top\demos\se05x\se05x_policy<br>• **EdgeLock 2GO Agent examples**:\simw-top\nxp_iot_agent\ex |

### 4.1.3 Cryptographic random number generation

The cryptographic algorithms and keys used by DLMS/COSEM standard, require the generation of random initialization data and challenges. The requirements for cryptographic random number generation defined in DLMS/COSEM are listed in

Table 7. DLMS/COSEM security requirements (cryptographic random number generation)

| Category | Requirement | IEC 62056-5-3 sections |
|---|---|---|
| **Random number generation** | A strong Random Number Generator (RNG) shall be provided to generate the random numbers required for the various algorithms used in DLMS/COSEM. The RNG shall be preferably non-deterministic. | Section 5.3.5 |

EdgeLock SE05x/A5000 supports the generation of variable-length random numbers through the built-in **AIS20 compliant Pseudo Random Number Generator (PRNG) with DRG.3 generation capabilities**. The PRNG works on top of EdgeLock SE05x/A5000 **True Random Number Generator (TRNG) compliant to AIS31 class PTG.2**. More information on PRNG and TRNG can be found in EdgeLock SE05x Data Sheet and in EdgeLock A5000 Data Sheet.

Table 8. NXP material: DLMS/COSEM cryptographic random number generation

| NXP material | Relevant content |
|---|---|
| **Plug & Trust middleware APIs** | • **Generate a random number:** sss_se05x_rng_get_random ()<br>• **Generate random data for TLS handshake:** Se05x_API_TLSGenerateRandom () |

# 5 Other recommended enhancements

EdgeLock SE05x/A5000/A5000 is a flexible IC that can be used as an all-around solution to implement a wide range of security features and use cases. By integrating EdgeLock SE05x/A5000/A5000 in smart meters, it is not only possible to meet the security requirements mandated by DLMS/COSEM standard, but also to go beyond that and implement additional, stronger security measures and use cases. For example, a smart meter might benefit from implementing the following features / use cases:

- **Secure communication using TLS:**EdgeLock SE05x/A5000/A5000 can be used to securely store all the keys and certificates required to establish a TLS channel between a smart meter and other external entities. Moreover, all the cryptographic algorithms and operations required by TLS can be executed in the SE secure environment and easily integrated in the IoT solution using the functions provided by the Plug & Trust middleware. More information on how to use EdgeLock SE05x/A5000 for TLS can be found in AN12400.
- **Secure boot:** thanks to its anti-tamper features, policy enforcement capabilities and support of modern cryptographic algorithms with high key lengths, EdgeLock SE05x/A5000/A5000 provides all the tools required to support the verification of the integrity and authenticity of the firmware during the boot of the smart meter, thus preventing attackers from injecting in the SM a corrupted firmware. In fact, EdgeLock SE05x/A5000/A5000 can be used as a secure trust anchor for the firmware validation keys and as a secure crypto processor for carrying out related cryptographic operations. Boot security can be improved even more by binding the SE to the MCU so that the MCU can only use the services offered by that particular SE and the SE can only provide its cryptographic services to that particular MCU. More information on secure boot and binding can be found in AN13086 and AN12662.
- **Secure cloud onboarding:**EdgeLock SE05x/A5000/A5000 can be used to protect keys and certificates required for the secure authentication and onboarding of the smart meter to a public or private cloud service such as Azure or AWS. To simplify the integration even more, EdgeLock SE05x/A5000/A5000 is pre-provisioned with all the certificates and keys required to onboard the smart meter to the most important cloud services. Moreover, the Plug & Trust middleware contains several examples that showcase onboarding and connection to cloud platforms (AWS, Azure, IBM Watson, GCP). More information can be found in AN12401, AN12402, AN12403, AN12404.
- **Updatable applets**: if you integrate **EdgeLock SE051** in smart meters, you can take advantage of the **SEMS Lite technology** to update applets (e.g. the IoT applet) on-the-field, both online or offline, so as to always get the latest security patches from NXP and the latest updates required to keep up with DLSM/COSEM and other specifications as they evolve over time. With EdgeLock SE051, devices can take advantage of the latest features and security improvements as soon as they are available and always enjoy a high protection level for stored credentials. Specific variants of EdgeLock SE051 even allow you to load custom applets so you can implement custom features should they be required by your use case. More information on SEMS Lite can be found in AN12907.

Please refer to EdgeLock SE05x/A5000 website and EdgeLock A5000 website for the complete list of application notes detailing the supported use cases and how they can be implemented using EdgeLock SE05x/A5000/A5000.

## 6 References


- DLMS UA. DLMS User Association website.
- IEC 62056-5-3. Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer. Edition 3.0. August 2017.
- DLMS UA. Security in DLMS, A White Paper by the DLMS User Association. November 2019.
- BSI. Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP). Version 1.3. March 2014.
- BSI. Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP). Version 1.03. December 2014.
- NXP. EdgeLock SE050 datasheet. Version 3.7. October 2022.
- NXP. EdgeLock SE051 datasheet. Version 1.8. January 2023.
- NXP. EdgeLock A5000 datasheet. Version 1.3. November 2022.
- NXP. Plug & Trust MW Documentation. Version 2.1. March 2023.

# 7 Abbreviations

**Abbreviations**

| Acronym | Description |
|---|---|
| DLMS | Device Language Message Specification |
| COSEM | Companion Specification for Energy Metering |
| WAN | Wide Area Network |
| NAN | Neighboor Area Network |
| LAN | Local Area Network |

# 8 Revision history

**Table 9. Revision history**

| Document ID | Release date | Description |
|---|---|---|
| AN13742 v.1.0 | 07 June 2024 | • Initial version |

# Legal information

## Definitions

**Draft** — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

## Disclaimers

**Limited warranty and liability** — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

**Right to make changes** — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

**Suitability for use** — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

**Applications** — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**Export control** — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

**Suitability for use in non-automotive qualified products** — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

**Translations** — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

**Security** — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

**NXP B.V.** — NXP B.V. is not an operating company and it does not distribute or sell products.

## Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

**NXP** — wordmark and logo are trademarks of NXP B.V.

# Tables

# Figures

# Contents