Guide RED Cyber assessment of smart meter products v1.0

1.CONTENTS

2. INTRODUCTION

This report has been created by a group of smart meter stakeholders, members from ESMIG, AQUA, OMS and the Ad-Hoc subgroup on Smart Meters from the CEN/CENELEC/ETSI Coordination Group on Smart Grids.

1st August 2025, the new Delegated Legislation (EU 2022/30) [2] came into force requiring most radio equipment to be compliant with Essential Articles 3.3 d, e and/or f of the RED (EU 2014/53) [1]. This legislation was introduced as a response to concerns over the resilience of some products to cyber-attacks.

By a Standardisation Request the EU Commission tasked CEN/CENELEC to develop three generic standards that set out the generic requirements that are to be demonstrated in order to presume compliance with the Essential Articles. These standards are EN 18031 -1 (Internet connected radio equipment) [4], -2 (radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment) [5] and -3 (Internet connected radio equipment processing virtual money or monetary value) [6], and they describe a set of security requirements that products need to demonstrate. There is a high degree of overlap between requirements across the three standards.

This document describes the cyber requirements contained within EN 18031 and provides a commentary on whether and how each of the requirements and the standards themselves might[1] apply to smart meters. Assumptions made are clearly documented to aid any notified bodies that may be tasked with the assessment of smart meters.

The content of this document provides a guidance to manufacturers of smart meters. It aims to assist manufacturers to assign the generic terms used in the EN18031 [4.5. 6] series standards to concrete terms used in a smart meter context. It does not provide guidance for the assessment of other components in a smart metering system.

This document cannot be used as a legal reference when performing the assessment of smart meters. It shall also be noted that the technical characteristics of the smart meters that according to this guideline, limits the scope of the products falling under (EU 2022/30) will not be the same in future legislations, such as EU 2024/2847 [3], but many of the considerations would still be applicable.

The remainder of the document is as follows:

- section 3 sets out the scope of the guide and its intended audience;
- section 4 provides a glossary of terms;
- section 5 provides references to relevant documents;
- section 6 describes how an assessment should be carried on a device under consideration including documentation to be compiled and activities to complete;
- section 7 clarifies which smart meters are in scope (and which are not);
- section 8 explains how to understand which standard or standards to apply;
- section 9 describes how to carry out the cybersecurity risk analysis as part of the overall assessment;
- section 10 clarifies the distinction of cybersecurity requirements that are needed for a general placing on the market under the RED and additional requirements that may be stipulated by a utility for operation in a particular network;
- section 11 lists the types of assets to be protected;
- section 12 sets out the Generic European smart meter architecture and highlights the differences between different types of meters: electricity, gas, thermal energy and water;
- section 13 sets out in detail how to apply the requirements in each of the 18031-x standards;
- section 14 examines each requirement and associated assessment in detail;
- Annex A sets out the typical activities that are part of a cybersecurity risk assessment;

[1] The decision as to whether each requirement applies to a particular smart meter product is ultimately the responsibility of the manufacturer.

- Annex B provides a suggested template for completion of a technical file necessary to demonstrate compliance with the standards.

2. SCOPE AND INTENDED AUDIENCE

This document intends to support manufacturers of commodity meters (electricity, gas, water, thermal energy) by evaluating the compliance of their products with EN 18031. Further on, it is supposed to structure the assessment conducted by different Notified Bodies to enable a uniform application of the requirements specified by EN 18031 [4.5.6].

There can be differences in applicability and appropriateness of requirements from commodity to commodity (see Annex A-6).

It is assumed that meter manufacturers can specify the operational environment their product is designed for and document this in manuals, safety instructions, safety statements or similar documents. These operational environment specifications can consider the different national or regional architectures defined either by customers or regulators. As an example, a meter can be designed to be protected by firewall functions integrated in a gateway which separates the meter from the Internet or other public network.

This document is intended to be used by meter manufacturers, Notified Bodies and market surveillance authorities involved in the assessment of smart meters.

GLOSSARY OF TERMS

For a glossary of terms used in this document we refer to:

CEN/CENELEC/ETSI TR 50572 - Functional reference architecture for communications in smart metering systems – Chapter 3
EN 18031-1 - Internet connected radio equipment – Chapter 3

3.REFERENCES

Nr.	Document	Description
[1]	EU 2014/53	DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment.
[2]	EU 2022/30	COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.
[3]	EU 2024/2847	REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)
[4]	EN 18031 -1	Common security requirements for radio equipment - Part 1: Internet connected radio equipment
[5]	EN 18031 -2	Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
[6]	EN 18031 -3	Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value
[7]	CEN/CENELEC/ETSI TR 50572	Reference Architecture
[8]	CEN/CENELEC/ETSI _SMCG Sec00109 / DC	Minimum security requirements for AMI components
[9]	CEN/CENELEC/ETSI _SMCG Sec00156 / DC	Protection Profile for smart meter minimum security requirements
[10]	Orgalim	Orgalim position paper, September 2022
[11]	Draft RED Guide	Draft RED guide
[12]	ISO 27005	Guidance on managing information security risks standard
[13]	EU 2014/32	Measurement Instrument Directive 2014
[14]	EU 2025/138	Commission Implementing Decision (EU) 2025/138 of 28 January 2025 amending Implementing Decision (EU) 2022/2191 as regards harmonised standards in support of the essential requirements of Directive 2014/53/EU of the European Parliament and of the Council that relate to cybersecurity, for the categories and classes of radio equipment specified in Delegated Regulation (EU) 2022/30
[15]	EN-13757-7	Communication systems for meters - Part 7: Transport and security services
[16]	Welmec 7.2 Guide	Software Guide

[17]	Blue Guide	The 'Blue Guide' on the implementation of EU product rules of 2022. (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC)

4. THE ASSESSMENT

The requirements sections of the standards contain normative text (SHALL) and so, in order to gain presumption of conformity these requirements must be satisfied if applicable.

The RED Delegated Legislation (EU 2022/30) [2] allows manufacturers to self-declare compliance with the legislation and it is recommended that the sections of the assessment highlighted in section 0 be used.

Publicly available information: information made available in the public domain such as manuals, installation and user guides and marketing information, are critically important for supporting the technical file for demonstration of compliance with the RED Cyber requirements (EU 2022/30) [2]. In particular, there should be a clear statement of the intended use of the meter setting out what capabilities the meter has and how it should be operated.

RED cybersecurity Risk assessment: setting out a manufacturer's justification as to which essential requirements apply to the product to demonstrate compliance with the various Essential Articles (3.3 d. e & f. of the RED). Additional security requirements related to specific cybersecurity risks related to the specific context of the operator of smart meters might be implemented. This cybersecurity risk assessment should take into consideration the specific smart metering architecture. See "Cybersecurity Risk Management" in section 7.

Technical file: For the RED Cyber Essential requirements (EU 2022/30) [2], a comprehensive set of documentation (referred to as ***Technical Documentation***) concerning cyber protection of the product, including a cyber security risk assessment and tests carried out in a laboratory related to the implementation of the cybersecurity requirements listed in the harmonised standards (fully cited in the OJEU), is needed to demonstrate conformance with the RED essential requirements (Articles 3.3 d. e & f.). This is the main way in which compliance with the RED Cyber legislation is demonstrated.

Declaration of conformity: standard format document needs to be included in full as an insert to the product or available on a manufacturer's website.

The CEN/CENELEC/ETSI Coordination group on Smart Meters created several documents that can be used as input for the assessment of smart meters based on the RED essential requirements 3.3 d, e & f.

- Functional reference architecture for communications in smart metering systems – CEN/CENELEC/ETSI TR 50572 – December 2011 [7]
- Minimum security requirements for AMI components – CEN/CENELEC/ETSI _SMCG Sec00109 / DC - July 2016 [8]
- Protection Profile for smart meter minimum security requirements - CEN/CENELEC/ETSI _SMCG Sec00156 / DC - July 2019 [9]

In this guideline these documents are used to define the smart meter assets and entities (section 10) and commentary for the requirements in section 11.

5. SMART METERS IN SCOPE OF (EU 2022/30) [2]

The scope of the RED Delegated Regulation (EU) 2022/30 concerning smart meters is important to understand.

From the RED Delegated Regulation (EU) 2022/30 [2], the text:

“any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment”,

has been challenging when writing the EN 18031 standards. The standardisation request M/585 prescribes technology neutral standards, and therefore it was not possible to create an exhaustive evaluation of technologies for all products which fall under this scope. Furthermore, DG-GROW has orally clarified the word “*can*” in the text above is to be interpreted as *“is capable of”*.

This view is also supported by recital (5) in the (EU) 2022/30 [2] text:

“(i) ***is capable*** *itself to communicate over the internet, regardless if it communicates directly or via any other equipment (‘internet- connected radio equipment’),”*

Furthermore, recital (5) states:

“i.e., such internet-connected equipment ***operates protocols necessary to exchange data with the internet*** *either directly or by means of an intermediate equipment;”*

Neither the RED delegate act nor EN 18031 [4,5,6] provides a clear technical definition of Internet-connected radio equipment, however, a paper by Orgalim [10] provides a technical description that could be used by manufacturers to analyse whether their product is in scope.

Manufacturers may demonstrate, through risk assessment and technical documentation, that a device is not internet-connected where public internet access is not possible due to physical, logical, or procedural design constraints aligned with intended use

Implementation of the requirements of the harmonized standards allows to demonstrate compliance to the essential requirements of the Delegated act.

However, in the following figures, technologies and architectures that have been seen prominent for solutions in the smart meter communities are elaborated on. This can give some well-argued guidance to manufacturers and authorities to assess if a product falls within the scope of the RED Delegated Regulation (EU) 2022/30 [2].

For this guidance document, only the equipment shown on the figures surrounded by the dotted lines is assessed for being in/out of scope. The legacy codes for the figures in the remainder of this section are shown in Figure 1.

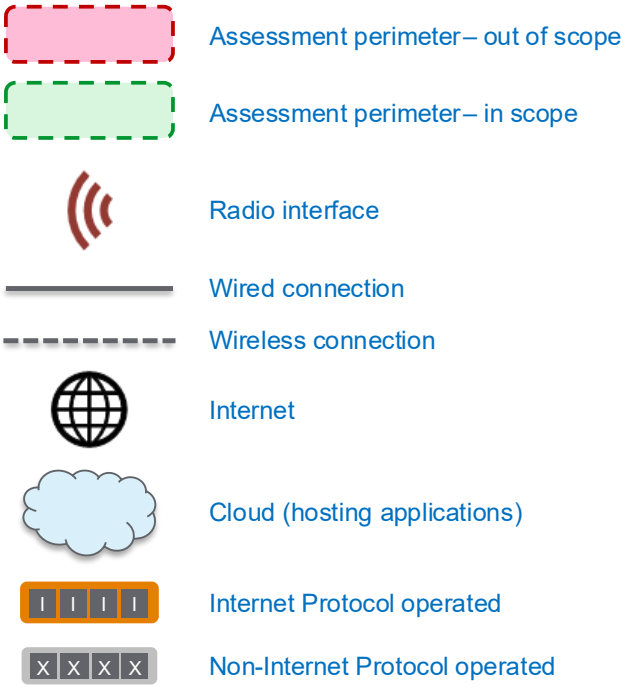

Figure 1: Legacy codes for illustrations.

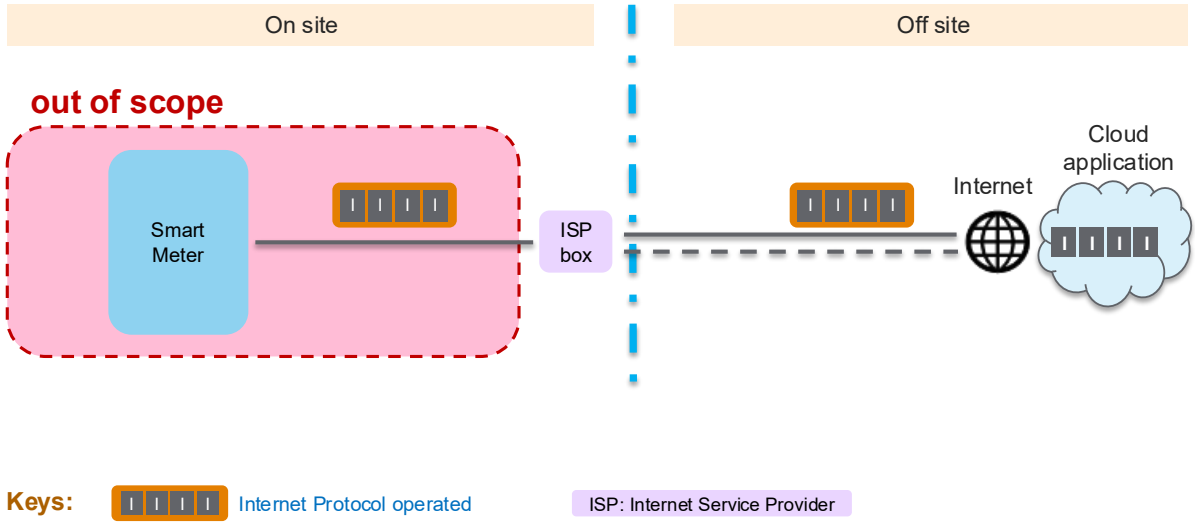

Figure 2: Example of smart meter not in scope of the RED.

The equipment shown in Figure 2 is capable of establishing an IP based communication over the Internet, via another equipment (ISP box), but it has NO radio capability and is therefore **out of scope** of the RED, and therefore also of this guidance document.

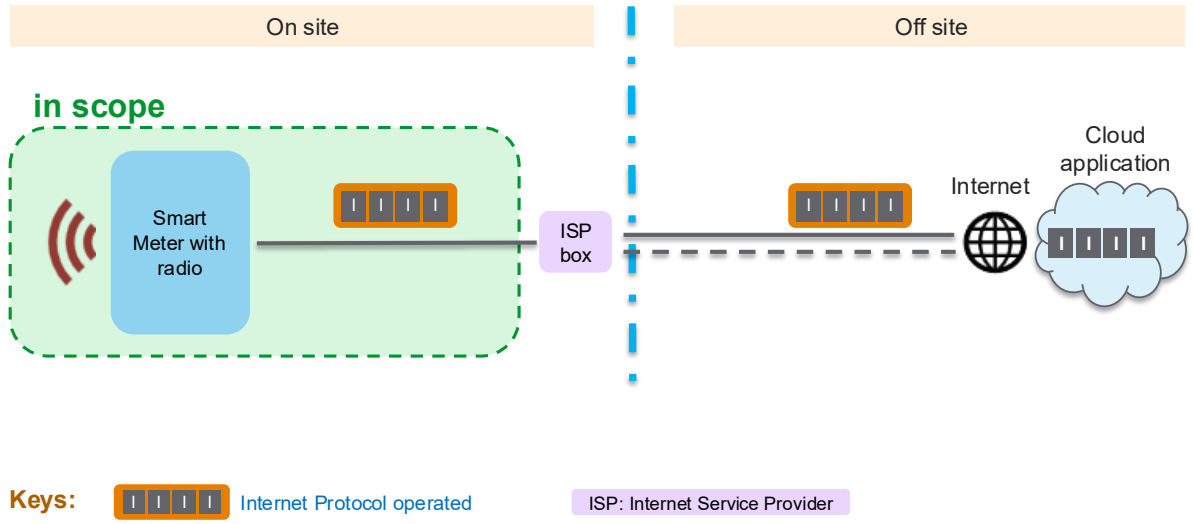

Figure 3: Example of equipment within scope of EU 2022/30.

The equipment shown in Figure 3 is capable of establishing an IP based communication over the Internet, via another equipment (ISP box), and it has a radio capability. Therefore, such equipment is **in scope** of EU 2022/30 [2] and for this guidance document.

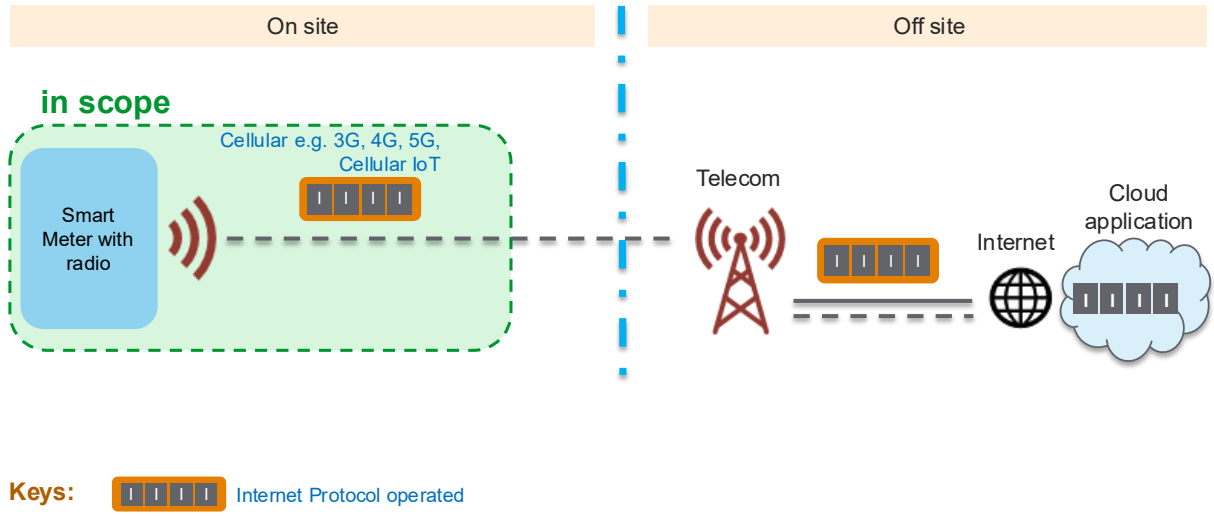

Figure 4: Example of equipment within scope of EU 2022/30.

The equipment shown in Figure 4 is capable of establishing an IP based communication over the Internet directly and it has a radio capability. Therefore, such equipment is **in scope** of EU 2022/30 [2] and for this guidance document.

A cellular product is considered '*capable to communicate itself over the internet*' even if it is configured to be communicating to a private APN. The reason is that the routing table in the mobile telecom network is configurable. Such configuration is solely dependent of the configuration of the mobile network, (typically defined in your mobile contract) and can always be modified by the mobile network operator. Hence, it cannot be argued that this is a "function" of the device.

Example: in case of IPv4, all mobile network operators assign only private IP-addresses to the devices connected to their network and it is "only" a configuration in the mobile network whether a device has access or is accessible for the internet. In IPv6 they usually assign a public IP-address, even in a private APN. However, such

IP address does not define whether you are reachable by a device from the internet or whether you can reach a device on the internet.

This viewpoint is also supported by Orgalim, providing comments to ADCO RED for updates on the draft RED guide [11]. Here it is explicitly stated that:

If a radio equipment is capable to communicate over the internet, then it is to be considered an "internet-connected radio equipment", even if the product is intended to be operated in a private network with no access to the internet.

Therefore, this interpretation is assumed to become part of the future RED guide.

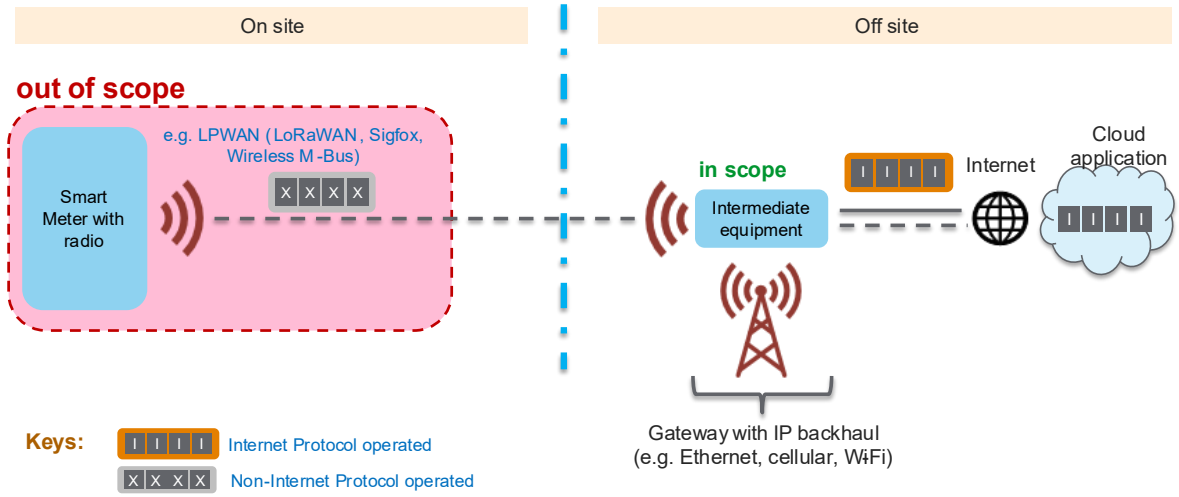

Figure 5: Example of equipment not in scope of EU 2022/30.

The equipment shown in Figure 5 is not capable of establishing an IP based communication over the Internet. Therefore, such equipment is **out of scope** of EU 2022/30 [2] and for this guidance document.

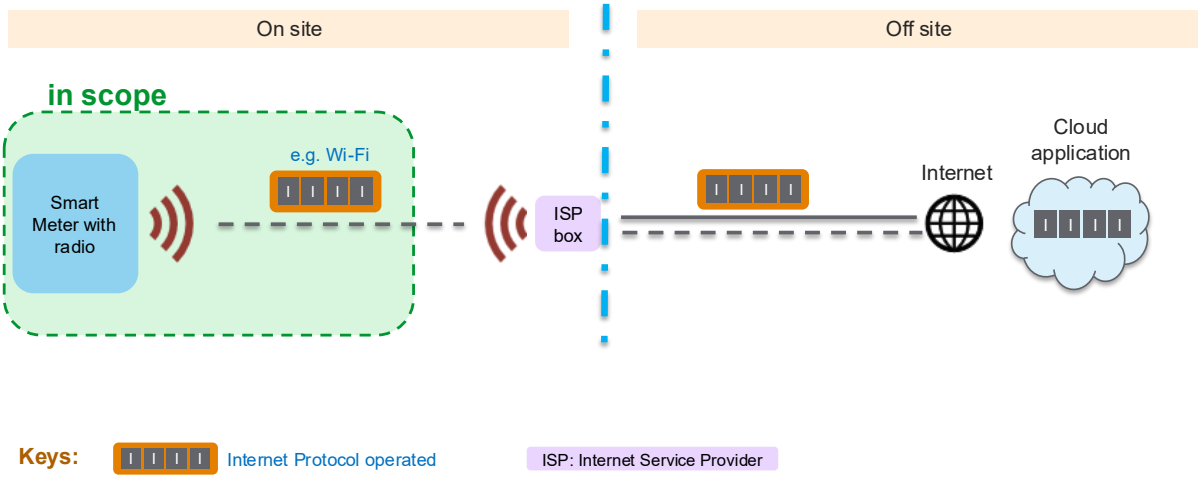

Figure 6: Example of equipment within scope of EU 2022/30.

The equipment shown in Figure 6 is capable of establishing an IP based communication over the Internet, via another equipment (ISP box) and it has a radio capability. Therefore, such equipment is **in scope** of EU 2022/30 [2] and for this guidance document.

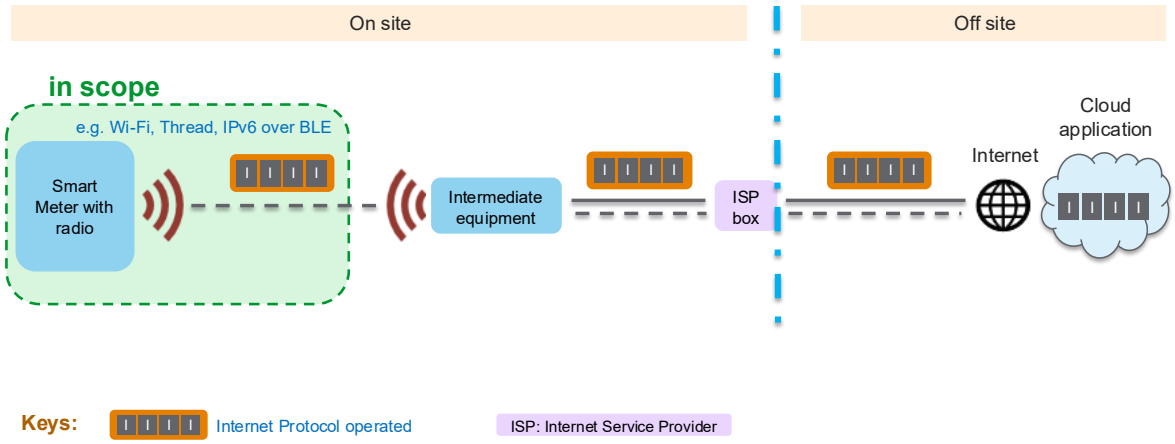

Figure 7: Example of equipment within scope of EU 2022/30.

The equipment shown in Figure 7 is capable of establishing an IP based communication over the Internet, via 2 other equipment, and it has a radio capability. Therefore, such equipment is **in scope** of EU 2022/30 [2] and for this guidance document.

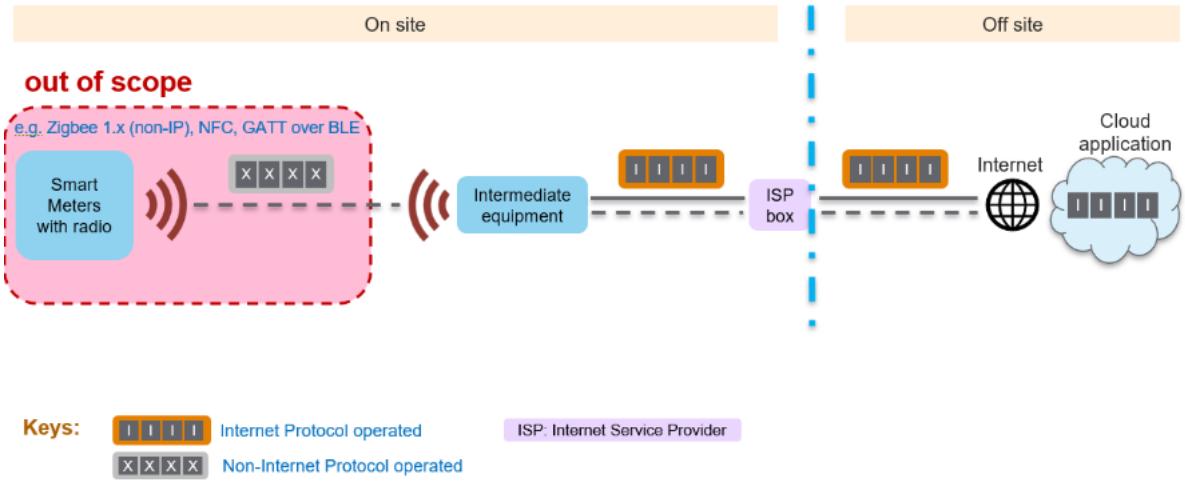

Figure 8: Example of equipment not in scope of EU 2022/30.

The equipment shown in Figure 8 is not capable of establishing an IP based communication over the Internet but has a radio capability. Therefore, such equipment is **not in scope** of EU 2022/30 [2] and for this guidance document.

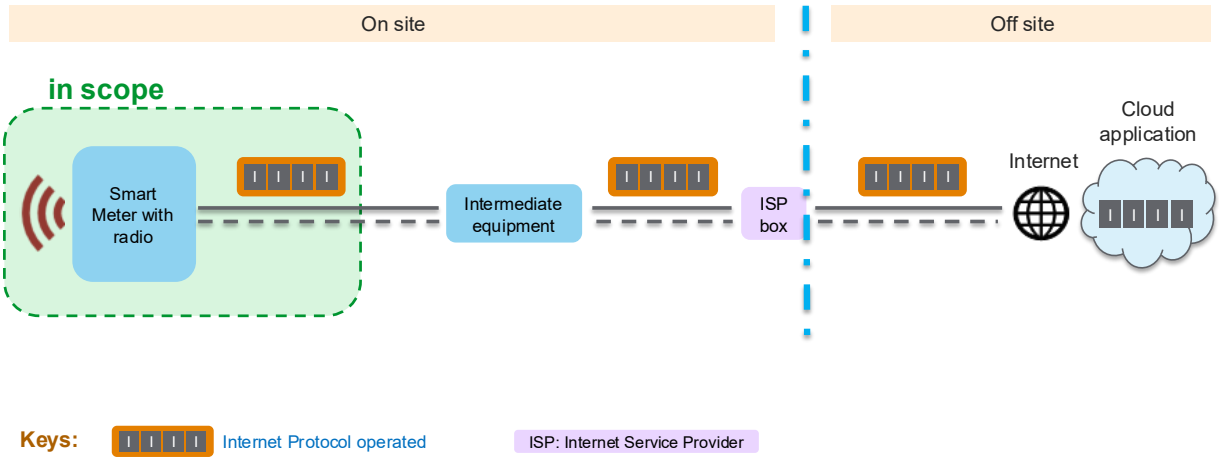

Figure 9: Example of equipment within scope of EU 2022/30.

The equipment shown in Figure 9 is capable of establishing an IP based communication over the Internet, via 2 other equipment, and it has a radio capability. Therefore, such equipment is **in scope** of EU 2022/30 [2] and for this guidance document.

If a smart meter is considered to be out of scope for the Delegated Regulation (EU) 2022/30 [2] according to the previous criteria, it may still be in scope of the Cyber Resilience Act and the remainder of this guidance document may still be valid for smart meters under CRA.

6.APPLICABILITY OF STANDARDS

The manufacturer should implement a process that analyses the smart meters in scope of the EU 2022/30 [2] to identify if requirements in Articles 3.3 (d), or 3.3 (e), or 3.3 (f) apply.

If a smart meter has been assessed to fall under the scope of one of the above articles of the RED Delegated Regulation (EU) 2022/30 [2], presumption of conformity with the essential requirements can be demonstrated by applying the appropriate parts of the EN18031 series: EN18031-1 for products falling withing Article 3.3 (d) [4], EN18031-2 for products falling withing Article 3.3 (e) [5], and EN18031-3 for products falling withing Article 3.3 (f) [6].

If a harmonised standard is used for demonstrating conformity to the essential requirements in the Delegated Regulation (EU) 2022/30 [2], the entire standard shall be used. Furthermore, the restrictions listed in COMMISSION IMPLEMENTING DECISION (EU) 2025/138 [14] shall be considered.

The requirements associated with the RED Cyber provisions and set out in the EN 18031 [4,5,6] standards are applicable to all internet-connected radio equipment to be placed on the European market. Nevertheless, the standard allows some products to be excepted from some of the requirements under certain circumstances, as set out in the standard.

For smart meters, there are examples of some national and pan-national energy architectures where some of the cyber requirements are not necessary – and may even be unwelcome – and which need to be accommodated. For example, in some countries it is necessary to make the unidirectional H1 interface (see CEN/CLC/ETSI/TR 50572) [7] available with no form of encryption - the assumption for this architecture being that the meters will be deployed in protected location (i.e. people's homes). In case such exceptions apply to the requirements of the standard(s), the public documentation of the product should clearly indicate this and explain for what type of architectures the product is designed.

There are four ways in which such products might be placed on the market:

Market placement with restrictions: the meters should only be made available in those countries in which the architecture exists and the marketing material, meter documentation (handbook etc), packaging and Declaration of Conformity should clearly highlight those countries in which the product might be legally put into service. See the Blue Guide for more details.

Secure by default: the meters should be manufactured and configured to be placed on the market in a fully secure state, with a final configuration (decommissioning some security features) carried out before delivery to a customer that has requested this configuration. In reality the two processes (manufacturing and configuration) might be combined, as long as a version can be delivered to other customers with a full complement of security features.

Risk transfer: If a customer requests, as part of their formal request for tender, meters be delivered with certain security features disabled, then this risk transfer (to the customer) should be documented in the product's risk assessment and the product documentation.

7. CYBERSECURITY RISK MANAGEMENT

The manufacturer is required to have a process in place to analyse the cybersecurity risk of the smart meter under assessment. This is needed to substantiate the justifications and reasoning for the complete omission of a requirement or the necessary proportional implementation of the mechanisms documented in the specific assessment sections of the harmonized standards.

More information regarding Cyber Security Risk Assessment and threat modelling could be found in EN 18031, Annex A.2.3 (STRIDE). Furthermore, for a comprehensive risk analysis and risk management of information systems see ISO/IEC 27005 "Guidance on managing information security risks"[12].

An appropriate process for managing cybersecurity risks for a smart meter could include the typical activities listed in Annex A. By applying these steps, a manufacturer can take the appropriate decisions when self-assessing the smart meter according to the guidelines laid out in section 11.

8. PLACING OF PRODUCTS ON AND MAKING AVAILABLE ON THE MARKET

Each meter that is placed in the market after August 1st 2025, must comply with the regulation. Even if other meters of the same series have been placed prior to August 1st 2025 (and did not need to be compliant before).

The Blue Guide [17] sets out the difference between making products available on the market (Quote 1) and placing of products on the market (Quote 2) in the EU.

- *A product is made available on the market when supplied for distribution, consumption or use on the Union market in the course of commercial activity, whether in return for payment or free of charge.*
- *The concept of making available refers to* ***each individual product****.*

Quote 1: Making available on the market (Blue Guide, section 2.2 [17]).

- *A product is placed on the market when it is made available for the first time on the Union market. According to Union harmonisation legislation, each individual product can only be placed once on the Union market.*
- *Product made available on the market must comply with the applicable Union harmonisation legislation at the moment of placing on the market.*

Quote *2*: Placing on the market (Blue Guide, section 2.3 [17]).

Furthermore, the text clarifies that the RED Delegated Regulation (EU) 2022/30 [2] requires all products that are offered or sold, and manufactured after August 1st 2025 has to comply with the essential requirements of (EU) 2022/30 [2].

> ***As for 'making available', the concept of placing on the market refers to each individual product, not a type of product, and whether it was manufactured as an individual unit or in series****. Consequently, placing on the Union market can only happen once for each individual product across the EU and does not take place in each Member State.* ***Even though a product model or type has been supplied before new Union harmonisation legislation laying down new mandatory requirements entering into force, individual units of the same model or type, which are placed in the market after the new requirements have become applicable, must comply with these new requirements.***

Quote 3: Excerpt of the Blue Guide, section 2.3.

At the point of placing the product on the market it is assumed to be compliant with the essential requirements (e.g. all security patches have been applied). At a later stage in time, after the specific deliverable products are made available to the European market, the RED[2] cannot demand smart meters to be updated (i.e. there is neither an expectation that meters in warehouses will need to be opened up and patched nor customers delivered secure updates). However, of course, it is in manufacturers' commercial and reputational interest to offer end customers certainty as to meters' ongoing cyber-security status. The RED does require meter manufacturers to offer software (and firmware) updating mechanisms.

9.SMART METER ASSETS ACCORDING TO EN 18031 -1/2/3 STANDARDS

There are different types of assets that are defined by the EN 18031 -1/2/3 standards "as the main targets against which to apply the requirements" of the standards:

Essential requirement	3.3.d	3.3.e	3.3.f
Security asset	✓	✓	✓
Network asset	✓		
Privacy asset		✓	
Financial asset			✓

Table 1: Assets and essential requirements (Source: EN 18031-1:2024, Section A.2.6)

It should be noted (as it is documented in section 11) that there is a significant overlap of the two applicable standards (EN 18031 -1 & -2) [4,5], and that the documentation required to demonstrate compliance with each standard can be common, referenced by a summary document as shown in Annex B.

For those smart meters where multiple asset types are applicable, and therefore multiple standards (among EN 18031 -1 & -2 & -3) may apply, it is important to note that the required level of protection may be different for the various assets although the title of the requirements are the same in different parts of the standards.

[2] The Cyber Resilience Act is able to place requirements on through-life activities, including a requirement for security patching, but this is not yet in place.

9.1 SECURITY ASSETS

"Security assets" are defined in the EN 18031 series as "sensitive security parameter or confidential security parameter or security function".

The identification of smart meter's security assets should include, but is not limited to:

- configuration data processed by the smart meter that is to be protected including the data's processing types (at least in terms of storage and transmission) and protection needs (at least in terms of confidentiality and integrity)
- security functions of the smart meter that need protection including a description (at least in terms of potential effects of these functions) and their protection needs (at least in terms of availability, integrity and access control)
- passwords, PIN-codes, as well as symmetric or asymmetric cryptographic keys whose manipulation can compromise the security of any other smart meter asset

9.2 NETWORK ASSETS

"Network assets" are defined in the EN 18031 series as "sensitive network function configuration or confidential network function configuration or network functions".

By definition, smart meters need to be connected via a network to central systems in order for consumption data to be delivered and messages and configuration data to be received. In case the communication technology used is capable of communicating over the internet, EN 18031 -1 (Internet connected radio equipment) [4] undoubtedly applies.

9.3 PRIVACY ASSETS

"Privacy assets" are defined in the EN 18031 series as "sensitive personal information or confidential personal information or sensitive privacy function configuration or confidential privacy function configuration or privacy functions".

Similarly, although few smart meters hold data that would be considered as personal data, nevertheless, total energy values, tariffs related settings , time-of-use setting and history loggings of consumption usage are generally deemed to be sensitive in that a snooper may be able to deduce from these patterns a household's daily habits and routine, and so EN 18031-2 (radio equipment processing data) [5] will apply.

9.4 FINANCIAL ASSETS

"Financial assets" are defined in the EN 18031 series as "sensitive financial data or confidential financial data or sensitive financial function configuration or confidential financial function configuration or financial functions".

Smart meters do not, typically, process virtual money or monetary value. Meters typically contain measurements in kWh, cubic meters or GJ and not in Euro's.

Data from head end systems do present information pertaining to finance (tariffs) to end users, and the data collected by the smart meter is conveyed to the headend, where monetary calculations are carried out, but it is assumed that checks and balances will be in place on headend servers to detect fraudulent activity (by households or 3rd-party attackers), and that this functionality lies outside the capabilities of the meter. Therefore, EN 18031-3 (Internet connected radio equipment processing virtual money or monetary value) [6] does not typically apply, unless such functionality is envisaged to be carried on the smart meter, or tokens representing monetary value are stored on prepayment meters[3].

[3] Prepayment calculations are typically carried out on head-end systems.

10. FUNCTIONAL REFERENCE ARCHITECTURE OF A SMART METERING SYSTEM

Figure 10 presents the Reference architecture of a smart metering system as defined by the CEN/CENELEC/ETSI Coordination Group on Smart Metering.

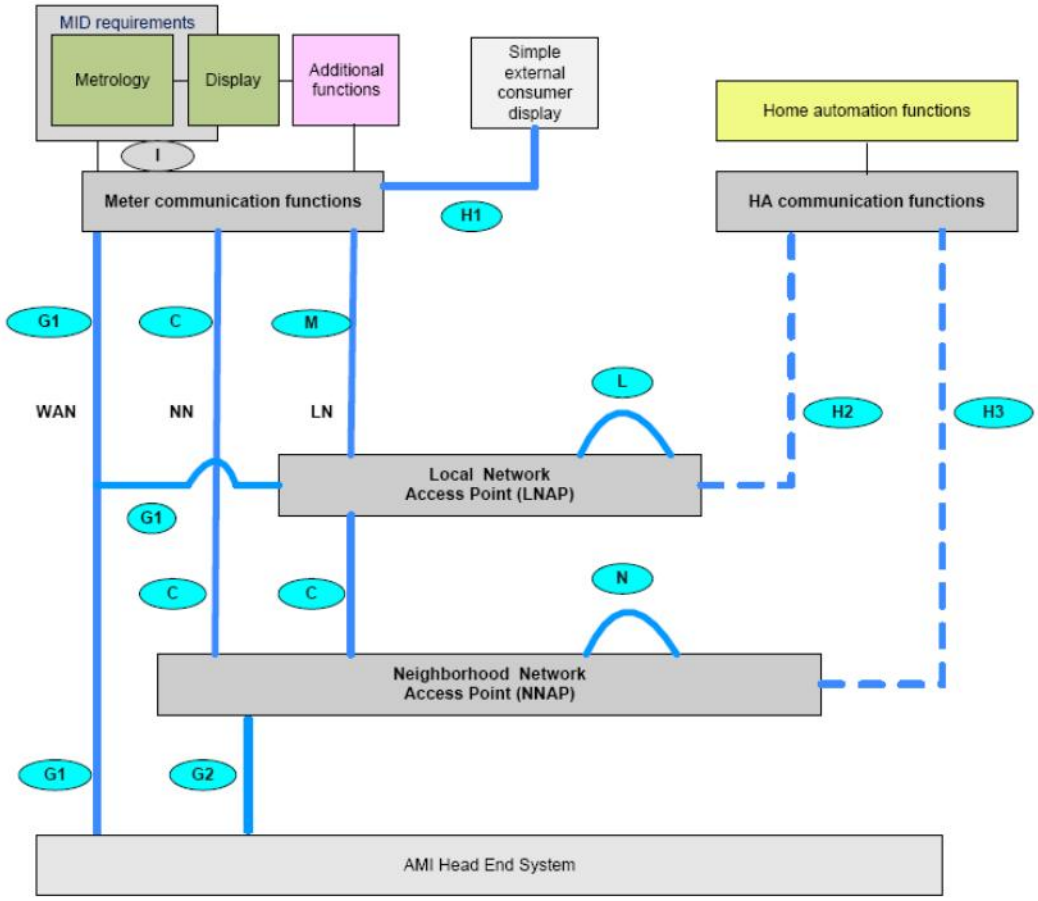

Figure 10: Reference architecture of a smart metering system as defined in TR 50572 [7]

In this architecture the LNAP is an optional element such as Smart Meter Gateway in Germany and the Comms Hub in the UK. The NNAP is an optional element typically known as Data Concentrator.

10.1 DETAILED ASSETS

Term	Meaning
Financial asset	**sensitive financial data** or **confidential financial data** or **sensitive financial function configuration** or **confidential financial function configuration** or **financial functions**
Network asset	**sensitive network function configuration** or **confidential network function configuration** or **network functions**
- Port M communication hardware and software	Interface for connecting other meters or a gateway (LNAP)

- Port M network function configuration software	
- Port H1 communication hardware and software	Interface for connecting in-home consumer tools for display of consumption or energy management
- Port H1 function configuration software	
- Port C communication hardware and software	Interface for connecting to a NNAP (such as Data Concentrator) via a neighbourhood network
- Port C function configuration software	
- Port G1 communication hardware and software	Interface to connect to a Head End System via a Wide Area Network
- Port G1 function configuration software	
Privacy asset	**sensitive personal information** or **confidential personal information** or **sensitive privacy function configuration** or **confidential privacy function configuration** or **privacy functions**
- Measured and calculated energy data	Imported and exported energy on the grid connection point. Calculated values per time period. Profiles.
- Measurement configuration software	
Security asset	**sensitive security parameter** or **confidential security parameter** or **security function**
- Cryptographic module to encrypt and decrypt data to be exchanged	
- Cryptographic keys	

Table 2: Assets relevant to smart meters

10.2 DETAILED ENTITIES

The definition of an "entity" in EN 18031 series is "user, device, equipment or service", i.e. that uses and can have access to the equipment/smart meter.

Entity	Description
Consumer (*)	The party that uses the meter for measuring its energy consumption and generation
Meter Operator (*)	The party that operates the metering infrastructure and has access to meter data and configuration
Service Operator	The party that has access to meter configuration
Other smart meters (*)	Other connected smart commodity meters installed at the same location (In some countries the gas, water or thermal energy meters can be connected to the electricity meter)
In Home Display	A device that displays meter data for the consumer
Energy Management System	A device that uses meter data for home/building energy management
Head End System (HES) (*)	A system that collects meter data and sends commands/information to the meter
LNAP (*)	A local (within the same premises as the meter) device that connects to one or more meters, collects meter data, sends commands/information to the meter. Is located between a HES and the meters(s).
NNAP (*)	A network device covering a number of premises that transfers data from the meter to the HES and vice versa. It can also aggregate data from the connected meters (Data Concentration).

Table 3: Entities relevant to smart meters (: for definition of terms see also ref. [7])*

ASSESSMENT AGAINST 18031-1 & 18031-2

The guidance on the applicability and implemented sufficiency of a specific mechanism stated in this section, for each requirement, will neither cover all product types nor all use cases that might exist. It shall list the most common assumptions of architectures and smart meter implementation in the fields of electricity, thermal energy, water and gas.

The requirements sections of the standards contain normative text (SHALL) and so, in order to gain presumption of conformity these requirements must be respected) The assessment sections of the standards (6.x.x.4 - to understand the format, see Table 1 in the standard) do not contain normative text but can be used in parallel with the cybersecurity risk assessment to prove compliance.

The standards assume that the assessment will be carried out by a third-party test house and are written as such, but this is not mandated by the standard and manufacturers carrying out self-assessments should use the tests therein as a guide for their work (see section 11). However, this approach should be documented in the accompanying risk assessment.

Each requirement has associated with it mandatory data to be recorded about the device under test. This is set out in the **Required information** section (section x.x.x.4.3). All of this information can be understood by reading the three assessments, below. **The completion of this information should suffice to prove that the device under test is conformant with the specification.** The assessor may choose to add additional information (such as screen shots from real systems) associated with the three assessments to support the documentation above and this would provide additional confidence that the technical file will be accepted in the event of an MSA assessment.

Many of the requirements (e.g. [ACM] Access control mechanism) have an initial sub-requirement (e.g. [ACM-1]) that contain the word, 'Applicability'. This initial sub-requirement simply asks whether a mechanism is in

place for each asset that is to be protected. Later sub-requirements explore the details of the way in which the mechanism is implemented.

The three types of assessment suggested to be carried out are:

- **Conceptual assessment** (section x.x.x.4.4): where aspects of the design of the device are to be recorded (see 'Required information' above), leading to 'Pass' or ''Not applicable using the Figure in the 'Assessment unit' (section x.x.x.4.4.3). th[4]. If the conclusion is 'Not applicable' then a well-reasoned justification must be documented (under [E.Just.DT.xxx-x]).

  An example decision-tree assessment is provided in section 10.4.

- **Functional completeness assessment** (section x.x.x.4.5): where a declaration that various aspects of the design documented in the Conceptual assessment (e.g. for ACM-1, Applicability of Access Control Mechanism, that all assets that can be accessed are documented) are in place. As part of a self-assessment, it would be nonsensical to conclude anything other than affirmative, but self-certifiers are encouraged to read the associated assessment steps (section x.x.x.4.5) to confirm that all aspects have been considered in the design of equipment.

- **Functional sufficiency assessment** (section x.x.x.4.6): where, in principle, demonstrations of the functionality described in the Conceptual Assessment (e.g. for ACM-1, that access control mechanisms are in place) are to be carried out and evidence recorded. Again, it would be nonsensical to conclude anything other than affirmative, and no specific documentation is demanded by the specification but in the associated Assessment unit (x.x.x.4.6.3) details of the requested tests should be reviewed and the self-assessor might consider providing evidence of some or all the checks described, either with a sample equipment or by reference to user documentation.

Implementation categories (section x.x.x.4.2): implementation mechanism options to be declared for some of the requirements. They should be documented under Required Information[5] and are referred to by assessments in the Functional completeness and Functional Assessment sections.

The manufacturer does his own cybersecurity risk assessment applying best practices as far as possible, considering the present use case. A hint on the acceptance level for residual risks can be assisted by the meter classification in section *Types of smart meters*.

10.3 IDENTIFYING ASSETS AND ENTITIES

Each of the requirements references the assets (security, privacy & network) that are to be protected and so in order to avoid repetition, it is suggested that tables of assets and entities identified are set out at the start of the assessment, to be referred to in short form in the commentary on each requirements. This should be in the form of four tables using the reference material given in section 11.

10.4 SAMPLE DECISION-TREE ASSESSMENT

Section 0 of this guide sets out the recommended decisions that should be assumed for most smart meter assessments. Under each requirement, a table is provided such as the one for [ACM-1] Applicability of access control mechanisms.

[4] In principle an assessment might conclude a 'Fail', but this would need to be discussed with a Notified Body and an alternative exception to those documented in the standards justified. As such, that lies outside the scope of this guide.

[5] The exact Required information element under which it should be recorded is inconsistent from requirement to requirement and the self assessor should use their judgement as to where it is recorded.

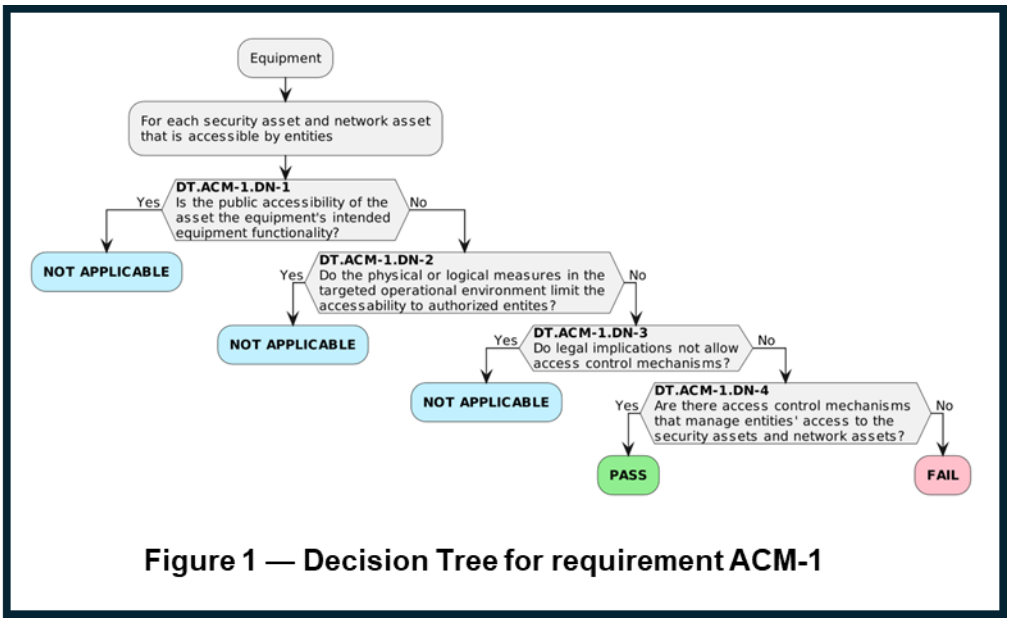

Figure 1 — Decision Tree for requirement ACM-1

Figure 11: Sample decision tree

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
ACM-1-DN-1	Not recommended	Recommended (go to ACM-1-DN-2)	Public accessibility might be assumed, but sensitive data still needs to be protected
ACM-1-DN-2	Not recommended	Recommended (go to ACM-1-DN-3)	Cannot be assumed
ACM-1-DN-3	Not recommended	Recommended (go to ACM-1-DN-4)	No such legal implications
ACM-1-DN-4	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Table 4: Sample decision tree

The recommended decision-tree documentation therefore would look like the table below.

Decision nr	**Decision**
ACM-1-DN-1	No
ACM-1-DN-2	No
ACM-1-DN-3	No
ACM-1-DN-4	Yes/PASS – see section on Access control & authentication

Table 5: Sample decision tree documentation. Decisions DN-1 to DN-3 are uncontroversial and do not need to be justified (although if a manufacturer did decide that one of the exceptions applied – effectively bringing traversal of the Decision tree to an end – a justification would need to be recorded). The final decision, DN-4, needs to be justified and can either be written in detail into the table or reference made to text earlier in the technical file under the heading Required information.

Another example is SUM-3, Automated Updates, where the assessment is brought to an end earlier in the Decision tree.

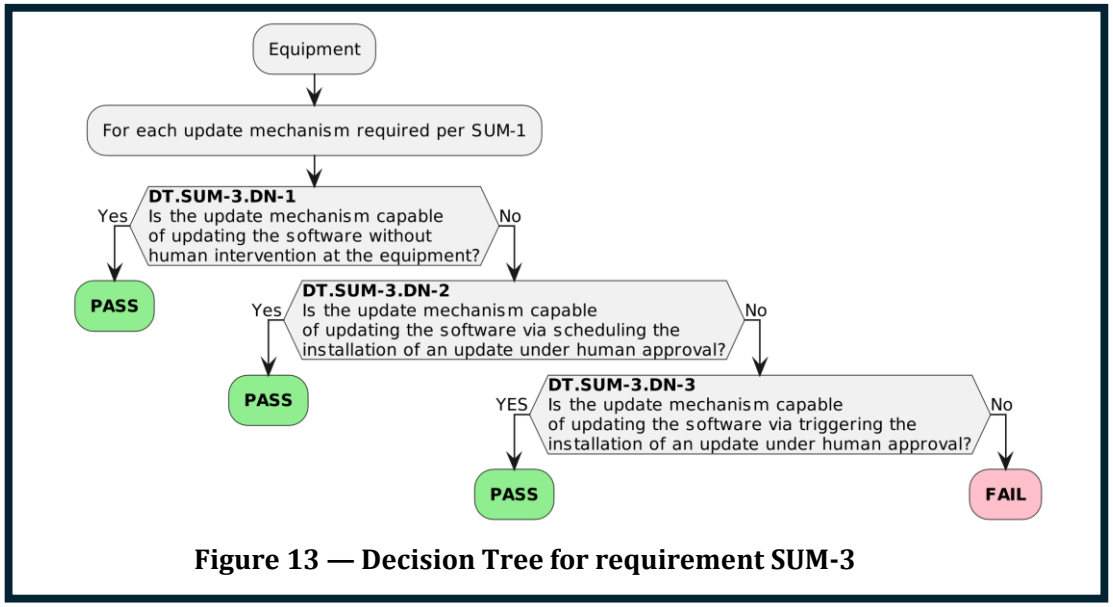

Figure 13 — Decision Tree for requirement SUM-3

Figure 12: Sample decision tree

Assessment decision tree (decision nodes are with reference is EN 18031-1)			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
SUM-3.DN-1	Recommended (END)	Not recommended	Normal operation for smart meters
SUM-3.DN-2	Recommended	Not recommended	This would describe a locally scheduled update which would be unusual for utility meters
SUM-3.DN-3	Recommended	Not recommended	This would describe a locally triggered update which would be unusual for utility meters

Table 6: Sample decision treeThe recommended decision-tree documentation therefore would look like the table below.

Decision nr	Decision
SUM-3-DN-1	Yes/PASS - see section on Software Updates
SUM -3-DN-2	N/A
SUM -3-DN-3	N/A
SUM -3-DN-4	N/A

Table 7: Sample decision tree documentation

11. 18031 REQUIREMENTS

11.1 INTRODUCTION

This section is the main guidance section on how to self-declare presumption of conformity with the essential requirements of (EU) 2022/30 using the EN 18031 harmonized standards.

To use harmonized standards as a tool for declaring presumption of conformity, all security requirements in the standard shall be assessed. The EN18031 standards provide two different types of requirements. The task for documentation and assessment activities in those two types of requirements will be different:

- **Applicability** of a security mechanism (usually denoted [AAA-1]. Note: A security mechanism can be documented as NOT being APPLICABLE for the product being assessed. The following should be documented:
- choices and justifications in decision trees.
- fundamental asset identification and required protection needs.
- **Appropriateness** of a security mechanism (usually denoted [AAA-2,3,…]. A security mechanism can be documented as being sufficiently implemented for the intended use and environment of use of the product being assessed, according to the risk assessment being performed for the product. The following should be documented:
- choices and justifications in decision trees.
- implementation categories (i.e. any options selected).
- sufficiency analysis

This guidance describes the recommended path through the decision trees of EN18031. Following this recommendation should lead to the highest possibility of a PASS for smart meters. Selecting non-recommended paths in the decision tree will be possible but may result in the need for a third-party assessment .

11.2 [ACM] ACCESS CONTROL MECHANISM

11.2.1 [ACM-1] APPLICABILITY OF ACCESS CONTROL MECHANISMS

Requirement [18031-1] [18031-2]:

The equipment shall use access control mechanisms to manage entities' access to security assets and {network}* assets, except for access to security assets or {network}* assets where:

- public accessibility is the equipment's intended functionality; or
- physical or logical measures in the equipment's targeted operational environment limit their accessibility to authorized entities; or
- legal implications do not allow for access control mechanisms

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Access control mechanisms will be required for any access that exists, but it will be unusual for a mechanism to allow access to data locally on the meter (PIN numbers or German strobe lights) through some form of physical interface. Most access will either be via the WAN or other local radio interfaces

such as NFC or wireless M-Bus. The mechanisms for gaining access via these interfaces need to be secured and the solution for securing them described. This may, as part of the description of intended use, require a description of auxiliary tools (even though they are not placed on the market as part of a single product) as well as via headend systems connected via the WAN.

Whilst interval data is considered personal data, register reads (the latest of which is typically on display) are not.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
ACM-1-DN-1	Not recommended (END)	Recommended (go to ACM-1-DN-2)	Public accessibility might be assumed, but sensitive still needs to be protected
ACM-1-DN-2	Not recommended (END)	Recommended (go to ACM-1-DN-3)	Cannot be assumed
ACM-1-DN-3	Not recommended (END)	Recommended (go to ACM-1-DN-4)	No such legal implications
ACM-1-DN-4	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each security asset* that is accessible by entities**, including possible entities' accesses to the security asset on the equipment.

* refer to the list of assets and entities that should be compiled before the assessment of each individual requirement

11.2.2 [ACM-2] APPROPRIATE ACCESS CONTROL MECHANISMS

Requirement [18031-1] [18031-2]:

Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and {network}* assets.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

The manufacturer implements a configuration function for access rights for entities (see Table 3) for every network and security asset (see Table 2).
The manufacturer implements a possibility to expire the established session after a pre-defined time.
After a specified (configurable) number of unsuccessful access attempts the access will be temporarily denied.
General note: access control via WANs and even maintenance units are typically managed on smart metering headend systems and so are out of the scope of a smart meter assessment – electronic access being achieved using PKI infrastructure or pre-shared symmetric keys. Local access by the customer is typically, likewise, achieved by contacting a utility and requesting access.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**

ACM-2.DN-1	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Implementation categories:

For most smart meter systems, these access controls will be external to the product itself, however for some smart meters systems access control mechanism may be present. The mechanism underlying the access control might be RBAC or DAC, dependent on the way in which the system is designed, but the difference is not controversial given the way in which access control is typically managed.

[IC.ACM-2.RBAC]: Typically, head-end system functionality and so out of the scope of the assessment

[IC.ACM-2.DAC]: Typically, head-end system functionality and so out of the scope of the assessment

[IC.ACM-2.MAC Typically, head-end system functionality and so out of the scope of the assessment.

[IC.ACM-2.Generic]: Typically, the most appropriate category.

Required information:

The description of each access control mechanism should address how the capabilities described below are associated with each implementation category.

If AU.ACM-2.RBAC

- Document HOW…roles are assigned to each user with associated authorization; and
- Document HOW…least privileges are associated with the roles; and
- Document HOW…the security asset or network asset is only accessible by authorized users given by their role; and
- Document HOW…changes in roles can only be performed by authorized users.

If AU.ACM-2.DAC

Document HOW…identities are assigned to each user with associated authorization; and

- Document HOW…least privileges are associated with the identities; and
- Document HOW…the security asset or network asset is only accessible by authorized users given by their identity; and
- Document HOW…changes in identities can only be performed by authorized users.

If AU.ACM-2.MAC

- Document HOW…the security asset or network asset is only accessible by authorized users after clearance was issued by the operating system and/or system administrator; and
- Document HOW…the issuance of clearance is associated with the principle of least privileges; and
- Document HOW…changing the operating system and/or system administrator that is responsible for the issuance of clearance to the user can only be performed by the authorized system administrator.

If AU.ACM-2.Generic

- Document HOW…the security asset or network asset is only accessible by authorized users; and
- Document HOW…the principle of least privileges for users is followed; and
- Document HOW…changing settings related to the access control mechanism or changes of privileges of users are only allowed to be performed by authorized users

11.2.3 [ACM-3] DEFAULT ACCESS CONTROL FOR CHILDREN IN TOYS

This requirement is not applicable to smart meters

11.2.4 [ACM-4] DEFAULT ACCESS CONTROL TO CHILDREN'S PRIVACY ASSETS FOR TOYS AND CHILDCARE EQUIPMENT

This requirement is not applicable to smart meters

11.2.5 [ACM-5] PARENTAL/GUARDIAN ACCESS CONTROLS FOR CHILDREN IN TOYS

This requirement is not applicable to smart meters

11.2.6 [ACM-6] PARENTAL/GUARDIAN ACCESS CONTROLS FOR OTHER ENTITIES' ACCESS TO MANAGED CHILDREN'S PRIVACY ASSETS IN TOYS

This requirement is not applicable to smart meters

11.3 [AUM] AUTHENTICATION MECHANISM

11.3.1 [AUM-1-1] APPLICABILITY OF AUTHENTICATION MECHANISMS FOR EXTERNAL INTERFACES - REQUIREMENT NETWORK INTERFACE

Requirement [18031-1] [18031-2]:

Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via network interfaces that allow to:

- read confidential {network}* function configuration {}** or confidential security parameters; or
- modify sensitive {network}* function configuration {}** or sensitive security parameters; or
- use {network}* functions or security functions,

except for access:

- {to network functions or network function configuration}*** where the absence of authentication is required for the equipment's intended functionality; or
- via networks where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorised entities.

* 18031-2: privacy

** 18031-2: ,confidential personal information

*** 18031-2: to personal information, privacy functions or privacy function configuration

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

This requirement is linked to ACM requirements, typically applying to every access mode highlighted in ACM. Given that most access mechanisms are not achieved through a physical interface on the meter,

AUM-1-1 generally applies (including for optical ports). The technical file should include a description of the authentication mechanisms associated with each of the ACM options described above.

If the network connection is a unidirectional protocol it may not be possible to grant access through this interface. In this case encryption might be needed on the interface and the password shall be implemented on the remote display following a pairing process with the smart meter. (e.g. using a QR code).

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
AUM-1-1-DN-1	Not recommended (END)	Recommended (Go to AUM-1-1-DN-2)	N/A
AUM-1-1-DN-2	Not recommended (END)	Recommended (Go to AUM-1-1-DN-3)	Networks should be assumed to be insecure (strength in depth)
AUM-1-1-DN-3	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each access control mechanism required per ACM-1 for managing entities' access over network interfaces that allow to read confidential network function configuration/privacy or confidential security parameters; or modify sensitive network function configuration/privacy or sensitive security parameters; or use network functions or security functions

For each access mechanism, classify as:

- [E.Info.AUM-1-1.ACM.NetworkInterface]: Description of the network interfaces for the managed access; and
- [E.Info.AUM-1-1.ACM.ManagedAccessPrivacyAsset]: Description of the managed access to privacy assets via network interfaces; and
- [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset]: Description of the managed access to security assets via network interfaces;

11.3.2 [AUM-1-2] APPLICABILITY OF AUTHENTICATION MECHANISMS FOR EXTERNAL INTERFACES - REQUIREMENT USER INTERFACE

Requirement [18031-1] [18031-2]:

Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to:

- read confidential {network}* function configuration{}** or confidential security parameters; or
- modify sensitive {network}* function configuration{}** or sensitive security parameters; or
- use network functions or security functions,

except for access:

- where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorized entities;

and except for read only access {to network functions or network functions configuration}*** where access without authentication is needed:

- to enable the intended equipment functionality; or
- because legal implications do not allow for authentication mechanisms.

* 18031-2: privacy

** 18031-2: ,confidential personal information

*** 18031-2: to personal information, privacy functions or privacy function configuration

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

This requirement is linked to ACM requirements for mechanisms that allow local access to the meter which is typically, at most, the ability to enter a PIN number to gain limited access to further information.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
AUM-1-2-DN-1	Not recommended (END)	Recommended (Go to AUM-1-2-DN-2)	N/A
AUM-1-2-DN-2	Not recommended (END)	Recommended (go to AUM-1-2-DN-3)	The operational environment should always be assumed to be insecure
AUM-1-2-DN-3	Not recommended (END)	Recommended (go to AUM-1-2-DN-4)	
AUM-1-2-DN-4	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each access control mechanism required per ACM-1 for managing entities' access over user interfaces that allow to read confidential personal information, confidential privacy function configuration or confidential security parameters; or modify sensitive personal information, sensitive privacy function configuration or sensitive security parameters; or use privacy functions or security functions, including:

- A description of the user interfaces for the managed access; and
- [E.Info.AUM-1-2.ACM.ManagedAccessPrivacyAsset]: Description of the managed access to privacy assets via user interfaces; and
- [E.Info.AUM-1-2.ACM.ManagedAccessSecurityAsset]: Description of the managed access to security assets via user interfaces; and
- (if physical or logical measures in the targeted environment provide confidence in the correctness of an entity's claim) [E.Info.AUM-1-2.ACM.IntendedEnvironment]: Description of the physical or logical measures in the targeted environment.

11.3.3 [AUM-2] APPROPRIATE AUTHENTICATION MECHANISMS (EN_18031-1 ONLY)

Requirement [18031-1]:

Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity's claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication).

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**N/A**

Commentary:

Any access to the meters irrespective of the interface should be protected by a suitable form of Authentication mechanism" because [AUM-2] Is authentication mechanism and not encryption. Any simple MMI interfaces, such as numerical interfaces allow PINs to be entered, that are implemented should have a suitable authentication mechanism on them if they allow direct access to sensitive data.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
AUM-2.DN-1	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Options:
Description of the authenticators including their categories (knowledge, possession and inherence).
NOTE: 'authenticators' (or authenticator factors) refers to the type of information used to authenticate access and how it is entered e.g. a PIN, password or smart card (if appropriate).

11.3.4 [AUM-2-1] REQUIREMENT ONE FACTOR AUTHENTICATION (EN_18031-2 ONLY)

Requirement [18031-2]:

Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) * shall verify an entity's claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication).

Applicable Smart metering	**Yes**	**18031-1**	**N/A**
		18031-2	**Yes**

Commentary:

The main access to most meters will be via network and other electronic interfaces and should be protected by a suitable form of encryption (see SCM). Any simple MMI interfaces, such as numerical interfaces allow PINs to be entered, that are implemented should have a suitable authentication mechanism on them if they allow direct access to privacy data.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
AUM-2.1.DN-1	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Required information:
Description of each authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface) including:

[E.Info.AUM-2-1.AuthenticationMechanism.AuthFactor]: Description of the authenticators including their categories (knowledge, possession and inherence).

* 'authenticators' (or authenticator factors) refers to the type of information used to authenticate access and how it is entered e.g. a PIN, password or smart card (if appropriate).

11.3.5 [AUM-2-2] REQUIREMENT TWO FACTOR AUTHENTICATION

As personal information of special categories according to the definition in EN 18031-2, 3.31 is typically not handled on smart meters this requirement does not apply to smart meters.

11.3.6 [AUM-3] AUTHENTICATOR VALIDATION

Requirement [18031-1] [18031-2]:

Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) {}* shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

This requirement applies to any smart meter device in scope (no exceptions), regardless of the commodity the meter is intended for. All attributes offered by the authenticator shall be used, for example, all letters of a password or all ciphers in a key, shall be validated.

The exception could be exemplified in the context that in case of PKI, the certificate chain and root of trust should be evaluated in the meter even if the meter is offline, but the set of relevant properties to check can differ depending on whether the equipment is actually internet-connected or not.

Assessment decision tree			
Decision nr	**Conditions for Yes**	**Conditions for No**	**Comments**
AUM-3.DN-1 (user interface)	Not recommended (END)	Not recommended unless needed to be referred to a Notified Body	

Implementation categories:
Three implementation categories are considered relevant for smart meters.

[IC.AUM-3.Password]: The authenticator is a password.
Can be appropriate for a local keypad or number access

[IC.AUM-3.CertificatePrivateKey]: The authenticator is a private key associated to a certificate trusted by the equipment.
Appropriate for many smart meters.

[IC.AUM-3.Generic]: The authenticator is different from [IC.AUM-3.Password] or [IC.AUM-3.CertificatePrivateKey].

Smart meters using symmetric keys would use this category.

Any network configuration or metering data values that need protection by symmetric keys (e.g. autonomous **remote** access to privacy meter data or network configuration) as determined under AUM-2.

If IC.AUM-3.Password

- Document HOW TO PREVENT…incorrect passwords can be used for successful authentication; and
- Document HOW TO PREVENT … (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of a recorded successful authentication attempt can be used for successful authentication; and
- Document HOW TO PREVENT …parts of the correct password can be used for authentication; and
- Document HOW TO PREVENT … (if different user accounts exist or can be created) passwords of other entities can be used for authentication.

If IC.AUM-3.CertificatePrivateKey

- Document HOW TO PREVENT …incorrect private keys to a trusted certificate can be used for successful authentication; and
- Document HOW TO PREVENT … (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of a recorded successful authentication attempt can be used for successful authentication; and
- Document HOW TO PREVENT …valid private keys to untrusted or invalid certificates can be used for successful authentication; and

NOTE: untrusted or invalid certificates can be certificates revoked by the certificate authority, expired certificates, certificates with an invalid chain of trust e.g., generated by an untrusted entity containing an expected “Common Name” (CN) entry.

- Document HOW TO PREVENT … (if different user accounts exist or can be created) private keys to a trusted certificate of other entities can be used for authentication.

If IC.AUM-3.Generic

- Document HOW TO PREVENT …incorrect authenticators can be used for successful authentication; and
- Document HOW TO PREVENT … (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of a recorded successful authentication attempt can be used for successful authentication; and
- Document HOW TO PREVENT … (if different user accounts exist or can be created) authenticators of other entities can be used for authentication.

Reference to standards:
EN13757-7; Communication systems for meters - Part 7: Transport and security services

11.3.7 [AUM-4] CHANGING AUTHENTICATORS

Requirement [18031-1] [18031-2]:

Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 {}* shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

AUM-1-1 – network authenticators. A smart meter includes data which need to be communicated while confidentiality, integrity and authenticity is ensured. For that purpose, a cryptographic key is needed. The security strength may in some cases relate to the key length, but also the algorithm used is important. E.g. symmetric cryptography using AES-128 algorithms are expected to be secure for decades to come. The breaking of such symmetric key is therefore unlikely to happen.
Conflicting security objectives could be:

- For battery operated smart meters a scheme of a very high transmission interval is typically applied to maintain many years of lifetime on the same battery. Opportunities to access these types of smart meters are limited to a short period after the transmission intervals.
- Replacement of compromised smart meters

It is strongly recommended that smart meters implement key exchange mechanisms.

- The lifetime of a smart meter can be decades.
- The authenticator material may be compromised in the Meter operator or service operator entities

AUM-1-2 – user interface. The smart meter totalisers are legally obliged (MID) to be shown on the meters display. Log data or consumption interval data with a certain resolution that can reveal habits of the consumer should be considered a privacy asset. Access to any privacy assets needs to be protected by a suitable authentication mechanism and therefore are in scope for this requirement as well. Conflicting security objectives could be:

- The meters intended environment of use is entirely on consumers premises.
- The meter is a district meter accumulating values from a larger group of consumers

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
AUM-4-DN-1	Not recommended (END)	Recommended (Go to AUM-4.DN-2)	
AUM-4-DN-2	Necessary for compliance	Not recommended unless needed to be	If the change of an authenticator accepts the setting of no authenticator 3rd

		referred to a Notified Body	party assessment is deemed necessary according to COMMISSION IMPLEMENTING DECISION (EU) 2025/138.

Required information
Description of each authentication mechanism required per AUM-1-1 (network interface) and AUM-1-2 (user interface), including:

- Description for each authentication mechanism documented, how the change of the authenticator is performed under consideration of the security concept of the smart meter.

- (if conflicting security goals do not allow for a change) A description of the conflicting security goals from the security concept of the smart meter concerning the change of the authenticator;
    - Document HOW… newly assigned authenticator grants access on each path to security assets and/or privacy assets; and
    - Document HOW… previous authenticator does no longer grant access on any path to security assets and/or privacy assets.

11.3.8 [AUM-5-1] PASSWORD STRENGTH - REQUIREMENT FOR FACTORY DEFAULT PASSWORDS

Requirement [18031-1] [18031-2]:

If factory default passwords are used by an authentication mechanism that is required per AUM-1-1 or AUM-1-2 {}*, they shall:

- be unique per equipment; and
- follow best practice concerning strength;

or

- be enforced to be changed by the user before or on first use.

NOTE: The user may choose to not use any password.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Default factory passwords used for network connections have to be unique for a smart meters and it is recommended to follow established standards for the generation of random numbers used to generate factory default passwords, e.g. NIST Special Publication 800-63B [9], ISO/IEC EN 27002:2022 [3], ISO/IEC EN 24760 [4], IEC EN 62443-4-2 [2] and ETSI EN 303 645 [5].

In case the meter supports the function that the user can change the default password, the user is required to us a password, however the strength of the user defined password does not need to be checked by the meter.

If a password is used to protect the privacy assets of the consumer on either a built-in display or a remote display (e.g. port H1), this password may initially not be available or common. The consumer shall be enforced to set a password of his choice before access to privacy data is granted.

If the smart meter accepts the setting of no password, 3rd party assessment is deemed necessary according to COMMISSION IMPLEMENTING DECISION (EU) 2025/138.

General note: smart meters typically do not have passwords that allow access to sensitive data, and certainly not by default. Therefore, typically this requirement will not be applicable. Access to the meters is

typically by electronic means. However, some meters can have a password set remotely by a utility and so 5-2 would apply.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
AUM-5-1.DN-1	Not recommended (END)	Recommended (Go to AUM-5-1.DN-2)	A password enforced to be set (e.g. by the consumer or service provider) before access to privacy assets are granted on the internal display or network port may lead to a PASS. This should only be implemented for specific ports (e.g. H1 or P1) and not in general for accessing smart meter assets.
AUM-5-1.DN-2	Recommended (Go to AUM-5-1.DN3)	Not recommended unless needed to be referred to a Notified Body	
AUM-5-1.DN-3	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	Passwords are at least unique in the scope of a utilities meter range (e.g. linked to consumer's installation/billing number)

Implementation categories:

IC.AUM-5-1.UniqueBestPractice]: The user is not enforced to change a factory default password on or before first use and a password is unique per equipment and follows best practice concerning strength.
Typically, not applicable. If limited data access can be set up for local customer access, a 4-digit PIN is normally needed sufficient.

[IC.AUM-5-1.EnforceSettingFirstUse]: The user is enforced to change a factory default password on or before first use.
Typically, not applicable

Required information:

Description of each authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface) that uses factory default passwords, including:

- [E.Info.AUM-5-1.AUM.PwdProperty]: Description for each authentication mechanism's factory default password:
- (if the implementation is based on [IC.AUM-5-1.UniqueBestPractice]) of how uniqueness and best practice concerning password strengths is implemented for the password with regard to the underlying use case of the authentication; and
- (if the implementation is based on [IC.AUM-5-1.EnforceSettingFirstUse]) of how the change of the password is enforced on or before first use.

11.3.9 [AUM-5-2] PASSWORD STRENGTH - REQUIREMENT FOR NON-FACTORY DEFAULT PASSWORDS

Requirement [18031-1] [18031-2]
If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2 {}*, they shall:

- be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or
- be defined by an authorized entity within a network where access is limited to authorised entities; or
- be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.

NOTE The user may choose to not use any password.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary
Passwords used for network connections should eventually become unique for a smart meter in a certain context (e.g. inside premises or factories).

If a password is used to protect the privacy assets of the consumer on either a built-in display or a remote display (e.g. port H1), this password may initially not be available or common. The consumer shall be enforced to set a password that is strong enough before access to privacy data is granted.

Alternatively, the password can be defined by an authorised entity (meter operator or service operator). This password can be based on consumer specific information (e.g. linked to consumer's installation/billing number). The consumer may receive the information to enter a password as instructed by using parts of information that is already in the consumers possession.

The NOTE in the requirement has caused a restriction published in COMMISSION IMPLEMENTING DECISION (EU) 2025/138. A password shall always be set if applicable in the product. If the smart meter allows for the setting of no password 3rd party assessment is deemed necessary (not recommended).
See General note under 5-1

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
AUM-5-2.DN-1	Not recommended (END)	Recommended (Go to AUM-5-2.DN-2)	A password enforced to be set by the consumer before access to privacy assets are granted on the internal display or network port may lead to a PASS. This should only be implemented for specific ports (e.g. H1 or P1) and not in general for accessing smart meter assets.
AUM-5-2.DN-2	Recommended (END)	Not Recommended (Go to AUM-5-2.DN-3)	Passwords are set during installation procedure by the authorized entity (meter operator, service provider), or the passwords are configured after installation by the authorised entity, or passwords are instructed to

			be set by the consumer before access to the privacy consumption data is granted
AUM-5-2.DN-3	Not recommended (END)	Not recommended unless needed to be referred to a Notified Body	

Implementation categories:

[IC.AUM-5-2.SettingFirstUse]: The user is enforced to set a non-factory default password on or before first use before the equipment is logically connected to a network.
Typically, not applicable

[IC.AUM-5-2.DefinedAuthEntity]: An authorized entity defines a non-factory default password within a network where access is limited to authorised entities.
Some meters allow remote setting of a password giving users limited access to data locally. If limited data access can be set up for local customer access, a 4-digit PIN is normally needed sufficient.

[IC.AUM-5-2.EquipmentGenerated]: A non-factory default password is generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities
Typically, not applicable

Required information:

Description for each authentication mechanism's non-factory default password:

- (if the implementation is based on [IC.AUM-5-2.SettingFirstUse]) of how the setting of the password is enforced and the means to prevent logical network connection before setting the password; and
- (if the implementation is based on [IC.AUM-5-2.DefinedAuthEntity]) of how the definition of the password is restricted to authorized entities and the means to prevent their definition within a network where access is not limited to authorised entities; and
- (if the implementation is based on [IC.AUM-5-2.EquipmentGenerated]) of how best practice concerning password strengths is implemented with regard to the underlying use case of the authentication and the means to prevent their communication to unauthorized entities or within a network where access is not limited to authorised entities.

Documentation includes all implemented features such as:

- Cryptographic algorithms
- Key and signature length
- Specification of entropy
- Cryptographic RNG
- Storage of keys

11.3.10 [AUM-6] BRUTE FORCE PROTECTION

Requirement [18031-1] [18031-2]:

Authentication mechanisms required per AUM-1-1 or AUM-1-2 {}* shall be resilient against brute force attacks.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Keys:

Smart Meters that implement authentication mechanisms will use resources for validating authenticators. A brute force attack on a communication key will machine initiate a number of trials, systematically challenging the authenticators.

A smart meter shall only accept commands that are properly authorised. The rejection of excessive unauthorised messages can be very resource demanding and may lead to decreased functionality, e.g. decrease in responsiveness of an electrical smart meter. Therefore, it may be advantageous in some use cases to shield the smart meter from brute force attacks by adding firewalls or otherwise creating sub-division on the network where a smart meter is installed (list of allowed IP addresses).

To prevent a successful brute force attack it is recommended to reduce the number of "unauthorised" trials that can be executed against a smart meter. For many battery-operated smart meters downlink commands follow one or more uplink commands (access opportunities). The smart meter will sleep most of the time, wake up periodically, transmit data and open access opportunities for receiving commands.

Furthermore, it can be implemented that if several authentication failures are detected (accept limited number of failed authentication attempts) during a communication sequence, the smart meter may close the communication session and initiate a new uplink command with a new access opportunity at a later stage (time delays) (see e.g. EN13757-7) [15].

For smart meters that need a high responsiveness (e.g. an energy smart meter always able to receive breaker commands) it has to be ensured that authenticators are sufficiently strong for the use case or that exhaustible authenticators can be exchanged.

Passwords:
Brute force attacks on passwords, normally will require access to the meter . If a smart meter is offering password access it should demand a sufficiently strong password.

General note: brute force attacks are typically only feasible via electronic interfaces.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
AUM-6.DN-1	Recommended	Not recommended unless needed to be referred to a Notified Body	

Implementation categories:

[IC.AUM-6.TimeDelay]: The methods for resilience against brute force attacks rely on time delays between authentication attempts.
Typically, this is the method preferred by manufacturers preventing brute force attacks, especially for battery powered meters, in order to conserve battery energy. This is also supported by many communication standards used for metering.

[IC.AUM-6.LimitedAttemps]: The methods for resilience against brute force attacks rely on a limited number of authentication attempts.
Typically, this is supported by many communication standards used in metering systems.

[IC.AUM-6.AuthenticatorComplexity]: The methods for resilience against brute force attacks rely on authenticator complexity.
EXAMPLE: mandatory multi factor authentication, enforce CCKs with a minimum-security strength of 112-bits
Typically, not appropriate

[IC.AUM-6.Generic]: The methods for resilience against brute force attacks rely on methods other than [IC.AUM-6.TimeDelay], [IC.AUM-6.LimitedAttemps] or [IC.AUM-6.AuthenticatorComplexity].

Typically, not appropriate

Required information:

[E.Info.AUM-6.AUM.BFProtection] Description how the resilience against brute force attacks is ensured, considering the implementation categories

If [IC.AUM-6.TimeDelay]
Document HOW…time delays enforced by the equipment between consecutive failed attempts

If [IC.AUM-6. LimitedAttempts]
Document HOW…counting the number consecutive failed attempts before the equipment prevents further attempts

If [IC.AUM-6.AuthenticatorComplexity]
Document HOW…complexity criteria

11.4 [SUM] SECURE UPDATE MECHANISM

11.4.1 [SUM-1] APPLICABILITY OF UPDATE MECHANISMS

Requirement [18031-1] [18031-2]:

The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or {network}* assets, except for software:

- where functional safety implications do not allow updatability; or
- which is immutable; or
- where alternative measures protect the affected security assets and/or {network}* assets during the entire lifecycle of the equipment.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Smart meters are handling network assets and privacy assets. The legal part of the meter is part of the Metering Instrument Directive. The software affecting security assets and/or {network}* assets may be separated from or be part of the software handling the legal part. If the latter is the case, and the smart meter is equipped with facilities for a software update without breaking a seal, the guidance can be found in the WELMEC Guide 7.2: 2023 Software Guide, chapter 10 [16].

If the software affecting security assets and/or {network}* assets have no relation to the legal metrology software, this has no restrictions in the MID. *Note that metering data is considered as privacy data and therefore affected by the legal software*.

Assessment decision tree: The decision tree shall be assessed for each part of the software that can be handled/stored separately.

Decision nr	Condition for Yes	Condition for No	Comments
SUM-1.DN-1	The evaluated SW part affects security assets and/or {network}* assets (Go to SUM-1.DN-2)	security assets and/or {network}* assets are not affected by the evaluated SW part (END)	
SUM-1.DN-2	Not recommended (END)	Recommended (Go to SUM-1.DN-3)	For electricity meters that has an integrated breaker function there could be

	Only smart meters that operates in an environment where safety can be compromised may use this exception.	Most smart meters can be updated with no interruption to their functionality and in any case would not affect safety if exposed to a short outage period.	hazards involved when updating the software if this involves a non-functioning product during the update. Before using the exception, a manufacturer should document that no countermeasures can be implemented mitigating the safety risk during a software update.
SUM-1.DN-3	Not recommended (END) It is documented that the part of software is by design not updateable	Recommended (Go to SUM-1.DN-4) The software part is stored in a modifiable memory.	In case not applicable, other mitigation techniques shall be mandated and documented, e.g. replacement of hardware. This should be part of the user documentation
SUM-1.DN-4	Not recommended Evident documentation is provided, that data is protected otherwise after the compromised algorithm, e.g. enabling another security mode or otherwise provide a tunnelling mechanism to protect the data.	Recommended No additional protection is possible (Go to SUM-1.DN-5)	[See below]
DT.SUM-1.DN-5	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each part of the software affecting the security assets and/or privacy assets including:

- (if the part of the software is not updatable for functional safety implications) [E.Info.SUM-1.PartOfSoftw.FuncSaftyImp]: Description of:
  - the functional safety requirements and their source; and
  - the software's function relation to the functional safety requirements
- (if the part of the software is not updatable because it is immutable) [E.Info.SUM-1.PartOfSoftw.Immutable]: Description of the methods that ensure that the part of the software is immutable;

Document (if software cannot be updated) which alternatives are provided if a publicly known exploitable vulnerability affecting security assets and/or {network}* assets, is compromised. This should typically also be stated in the manual

- Example: Replacement
- The lifetime of the equipment

Reference to standards:
N.A.

11.4.2 [SUM-2] SECURE UPDATES

Requirement [18031-1] [18031-2]:

Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.			
Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

For each update mechanism applicable in SUM-1, the update mechanism of the smart meter shall verify the integrity and authenticity of firmware images before they are applied or activated.
The success of a secure update requires that all entities involved (meter operator, service operator, HES) can distribute their responsibilities, e.g. securing authentication keys and certificates.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
SUM-2.DN-1	Recommended	Not recommended unless needed to be referred to a Notified Body	Notified Body might want documentation for that software update is only intended to be done in a controlled environment.

Implementation categories:

IC.SUM-2.AuthIntVal.Sign]: The methods to validate the software's integrity and authenticity solely rely on digital signatures for software updates by authorized entities.
Typically, this is the preferred method for validating software

[IC.SUM-2.AuthIntVal.SecChan]: The methods to validate the software's integrity and authenticity solely rely on a secure communication mechanism to the authorized software update's source as required per SCM-1 and SCM-2.
Typically, not appropriate

[IC.SUM-2.AuthIntVal.AccContMech]: The methods to validate the software's integrity and authenticity solely rely on access control mechanisms that only allow updates by authorized entities as required per ACM-1 combined with hash-protected software update.
Typically, not appropriate

[IC.SUM-2.AuthIntVal.Generic]: The methods to validate the software's integrity and authenticity are different from [IC.SUM-2.AuthIntVal.Sign], [IC.SUM-2.AuthIntVal.SecChan] or [IC.SUM-2.AuthIntVal.AccContMech].
Typically, not appropriate

Required information:

Description of each update mechanism that can update a part of the software documented in [E.Info.SUM-1.PartOfSoftw] including:

- (if the implementation is based on [IC.SUM-2.AuthIntVal.Sign]) [E.Info.SUM-2.SUM.Sign]: Description of the digital signature scheme used with a description of the underlying best practice cryptography as per [E.Info.CRY-1.Assets.Cryptography]; and
- (if the implementation is based on [IC.SUM-2.AuthIntVal.SecChan]) [E.Info.SUM-2.SUM.SecChan]: Description of the secure communication mechanism referring to [E.Info.SCM-1.SCM] with a description of the underlying best practice cryptography as per [E.Info.CRY-1.Assets.Cryptography]; and
- (if the implementation is based on [IC.SUM-2.AuthIntVal.AccContMech]) [E.Info.SUM-2.SUM.AccContMech]: Description of the access control mechanism referring to [E.Info.ACM-2.SecurityAsset.ACM] and of the hash function referring to [E.Info.CRY-1.Assets.Cryptography]; and
- (if the implementation is based on [IC.SUM-2.AuthIntVal.Generic]) [E.Info.SUM-2.SUM.Generic]: Description of the methods used to validate the software's integrity and authenticity.

If [IC.SUM-2.AuthIntVal.Sign]

- Document HOW…an unsigned software update cannot be installed; and
- Document HOW…a software update with a modified signature cannot be installed; and
- Document HOW…a modified software update with a valid signature for the unmodified software update cannot be installed

If [IC.SUM-2. AuthIntVal.SecChan]

- Document HOW…a software update from an unauthorized source cannot be installed; and
- Document HOW…the secure communication channel cannot be used to impersonate the authorized software updates source via a man-in-the-middle attack; and
- Document HOW…a software update that is modified during communication cannot be installed.

If [IC.SUM-2.AuthIntVal. AccContMech]

- Document HOW…it is implemented using the access control mechanism according to ACM; and
- Document HOW…a modified software update with a valid hash for the unmodified software update cannot be installed; and
- Document HOW…a software update with a hash generated by an unsupported hash function cannot be installed; and
- Document HOW…a software update provided by an unauthorized entity cannot be installed.

If [IC.SUM-2.AuthIntVal. Generic]

- Document HOW…a software update whose integrity is not valid cannot be installed and
- Document HOW…a software update whose authenticity is not valid cannot be installed.

11.4.3 [SUM-3] AUTOMATED UPDATES

Requirement [18031-1] /[18031-2]:

{}*, Each update mechanism that is required per SUM-1 shall be capable of updating the software:

- without human intervention at the equipment; or
- via scheduling the installation of an update under human approval; or
- via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment.

* 18031-2: When the equipment is internet-connected,

Applicable smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Software updates on smart meters are typically (never) handled by the consumer. Therefore, the attention of when and how to update the software of a smart meter is typically delegated to the meter operator or service operator.

Automated software update is meant to be part of a secure update mechanism. It is put in place to eliminate failures during software update. It means that a software update should be running fully automatic from when it is initiated until it is done.

The initiation would typically be a human action, regardless of performed locally or remote. No manual actions in-between should be allowed. Preferably, only a single manual action should be needed to initiate and finalize the update (including validation). For smart meters it is NOT recommended to implement systems that autonomously initiates/performs automatic updates without the intervention of the meter operator or service operator.

Remark: This is only an example section. Explanation should be given in the guidance part

Assessment decision tree (decision nodes are with reference is EN 18031-1)

Decision nr	Condition for Yes	Condition for No	Comments
SUM-3.DN-1	Recommended (END)	Not recommended	Normal operation for smart meters
SUM-3.DN-2	Not recommended	Not recommended	This would describe a locally scheduled update which would be unusual for utility meters
SUM-3.DN-3	Not recommended	Not recommended	This would describe a locally triggered update which would be unusual for utility meters

Required information:

Description of each update mechanism required per SUM-1, including:

- [E.Info.SUM-3.SUM.Automation]: Description of the means to automate the update mechanism.

Document HOW…equipment performs the software update:

- without human intervention at the equipment; or
- via scheduling the installation of an update under human approval; or
- via triggering the installation of an update under human approval.

11.5 [SSM] SECURE STORAGE MECHANISM

11.5.1 [SSM-1] APPLICABILITY OF SECURE STORAGE MECHANISMS

Requirement [18031-1] /[18031-2]:

The equipment shall always use secure storage mechanisms for protecting the security assets and

{network}*/ {privacy}** assets persistently stored on the equipment, except for persistently stored security assets or {network}*/ {privacy}**/assets where:

- the physical or logical measures in the target environment ensures the security asset or {network}* asset stored on the equipment accessibility is limited to authorized entities.

* 18031-1: network assets

** 18031-2: privacy assets

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

The smart meter ensures the secure storage of security assets and {network}*/{privacy}** assets against unauthorized access or tampering.

The manufacturer implements mechanisms such as:

- cryptographic measures like encryption to ensure confidentiality;
- cryptographic measures like digital signatures to ensure integrity and authenticity;
- access control using authentication or authorization;
- hardware protection measures;
- physical protection measures.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
SSM-1.DN-1	Not recommended	Recommended (Go to SSM-1.DN-2)	The firmware and associated security assets in the smart meter are partially protected by the smart meter's target operational environment: 1) secure access, integrity and protection against alteration of the firmware are ensured by cryptographic mechanisms implemented/controlled by the Head End System (digital signatures); 2) integrity/confidentiality of data running (file system) on the firmware are protected by cryptographic mechanisms in the smart meter;
SSM-1.DN-2	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Required information:

[E.Info.SSM-1.SecurityAsset]: Description of each security asset persistently stored on the equipment, including for each of its persistent storage:

- (if a secure storage mechanism is claimed to be not required because physical or logical measures in the environment's target operational environment ensure that the stored security asset's

accessibility is limited to authorized entities) [E.Info.SSM-1.SecurityAsset.Environment]: Description of:
  - physical or logical measures in the equipment's targeted operational environment; and
  - how entities are authenticated/authorized in the equipment's targeted operational environment; and
- (if the persistent storage is provided by a secure storage mechanism) [E.Info.SSM-1.SecurityAsset.SSM]: Description of the secure storage mechanism.

[E.Info.SSM-1.NetworkAsset]: Description of each network asset persistently stored on the equipment, including for each of its persistent storage:

- (if a secure storage mechanism is claimed to be not required because physical or logical measures in the environment's target operational environment ensure that the stored network asset's accessibility is limited to authorized entities) [E.Info.SSM-1.NetworkAsset.Environment]: Description of:
  - physical or logical measures in the equipment's targeted operational environment; and
  - how entities are authenticated/authorized in the equipment's targeted operational environment; and
- (if the persistent storage is claimed to be required by a secure storage mechanism) [E.Info.SSM-1.NetworkAsset.SSM]: Description of the secure storage mechanism.
- For each security asset, how it is persistently stored solely via secure storage mechanisms;

For each network asset, how it is persistently stored solely via secure storage mechanisms.

Reference to standards:

ISO/IEC 27040:2024 "Information technology — Security techniques — Storage security"

11.5.2 [SSM-2] APPROPRIATE INTEGRITY PROTECTION FOR SECURE STORAGE MECHANISMS

Requirement [18031-1] /[18031-2]:

Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and {network}* assets it stores persistently.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Metrology data integrity is partly covered by the MID and so the applications of standards such as 50470-1 should also be considered. Evaluation though, should be done for all storage mechanism in which Security or Network functions or parameters are stored and are not part of the legally relevant part.

General note: the solutions to SSM-2 & SSM-3 are typically identical

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
SSM-2.DN-1	Recommended	Not recommended unless needed to be referred to a Notified Body	

Implementation categories:

[IC.SSM-2.DigitalSignature]: The method to ensure the integrity of stored security assets or privacy assets is based on digital signatures derived using a cryptographic secret provisioned during manufacturing, commissioning, or normal operation of an equipment.
Typically, this is a preferred method for protecting secure storage of data

[IC.SSM-2.AccessControl]: The method to ensure the integrity of stored security assets or privacy assets is using access control mechanisms that deny unauthorized modification.
Typically, this is a preferred method for protecting secure storage of data

[IC.SSM-2.OTProgrammable]: The method to ensure the integrity of stored security assets or privacy assets is based on one-time programmable memory.
Typically, this is a preferred method for protecting secure storage of data

[IC.SSM-2.HardwareProtection]: The method to ensure the integrity of stored security assets or privacy assets is based on hardware protecting the memory.
Typically, not appropriate

[IC.SSM-2.Generic]: The methods to ensure the integrity and of stored security assets and privacy assets do not solely rely on [IC.SSM-2.DigitalSignature], [IC.SSM-2.AccessControl], [IC.SSM-2.OTProgrammable] or [IC.SSM-2.HardwareProtection].
Typically, not appropriate

Required information:

Description of each secure storage mechanism, including

- a list of all security assets and privacy assets it stores persistently; and
- (if the SSM implementation is based on [IC.SSM-2.DigitalSignature]) [E.Info.SSM-2.SSM.DigitalSignature]: Description of how integrity protection is realized using digital signature including:
    - description of the digital signature mechanism and the cryptography for the security assets and privacy assets it stores persistently; and
    - a description of how the cryptographic secret used to derive the signature is provisioned onto or generated by the equipment; and
- (if the SSM implementation is based on [IC.SSM-2.AccessControl]) [E.Info.SSM-2.SSM.AccessControl]: Description of how integrity protection is realized using access control mechanisms, including:
- a description of the access control mechanisms and the corresponding access rights for the security assets and privacy assets it stores persistently; and
    - (if the SSM implementation is based on IC.SSM-2.OTProgrammable) [E.Info.SSM-2.SSM.OTProgrammable]: Description of how integrity protection is realized using one-time programmable memory, including:
        - a description of what type of one-time programmable memory is used for the security assets and privacy assets it stores persistently; and
    - (if the SSM implementation is based on [IC.SSM-2.HardwareProtection]) [E.Info.SSM-2.SSM.HardwareProtection]: Description of how integrity protection is realized using hardware protection including:
        - a description of what hardware protection is used for the security assets and privacy assets it stores persistently; and
    - (if the SSM implementation is based on [IC.SSM-2.Generic]) [E.Info.SSM-2.SSM.Generic]: Description of the integrity protection mechanism used to protect the security assets or privacy assets; and

- if it is claimed that the secure storage mechanism is compliant with recognised security standards or certification schemes, provide evidence to the recognised security standard or certification schemes the secure storage mechanism complies to.

If [IC.SSM-2.DigitalSignature]

- Document HOW…the secret used to digitally sign the security assets or privacy assets cannot be intercepted, deduced, or extracted; and
- Document HOW…a modification of the security assets and privacy assets without valid signature is detected by the secure storage mechanism.

If [IC.SSM-2. AccessControl]

- Document HOW…unauthorized modification of the stored security assets and privacy assets is denied.

If [IC.SSM-2. OTProgrammable]

- Document HOW…modification of the security assets and privacy assets is not possible

If [IC.SSM-2. HardwareProtection]

- Document HOW…an unauthorized modification of the security assets and privacy assets is not possible or can be detected by the secure storage mechanism.

If [IC.SSM-2. Generic]

- Document HOW…unauthorized modification of the security assets or privacy assets is not possible or can be detected by the secure storage mechanism.

Reference to standards:

ISO/IEC 27040:2024 “Information technology — Security techniques — Storage security”

ISO/IEC 27002:2022: “Information security, cybersecurity and privacy protection — Information security controls”

11.5.3 [SSM-3] APPROPRIATE CONFIDENTIALITY PROTECTION FOR SECURE STORAGE MECHANISMS

Requirement [18031-1] /[18031-2]:

[18031-1] Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently.

[18031-2] Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential personal information, confidential privacy function configuration, and confidential security parameter persistently stored on the equipment.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Confidentiality is typically ensured through encryption.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments

SSM-3.DN-1	Recommended	Not recommended unless needed to be referred to a Notified Body	

Implementation categories:

Several of the following implementation categories could be used in combination as feasible.

[IC.SSM-3.Encryption]: The method to ensure the secrecy of stored confidential personal information, confidential privacy function configuration, and confidential security parameter is based on encryption using a secret provisioned during manufacturing, derived during commissioning or normal operation of an equipment.

Typically, this is a preferred method for protecting secure storage of data

[IC.SSM-3.AccessControl]: The method to ensure the secrecy of the stored confidential personal information, confidential privacy function configuration, and confidential security parameter is using access control mechanisms that deny unauthorized reading.

Typically, this is a preferred method for protecting secure storage of data

[IC.SSM-3.HardwareProtection]: The method to ensure the secrecy of stored confidential personal information, confidential privacy function configuration, and confidential security parameter based on hardware protection (e.g. scrambling, obfuscation, etc.).

Typically, this is a preferred method for protecting secure storage of data

[IC.SSM-3.Generic]: The methods to ensure the secrecy of stored confidential personal information, confidential privacy function configuration, and confidential security parameter do not solely rely on [IC.SSM-3.Encryption], [IC.SSM-3.AccessControl] or [IC.SSM-3.HardwareProtection].

Typically, not appropriate

Required information:

Description of each secure storage mechanism that persistently stores confidential personal information, confidential privacy function configuration or confidential security parameter, including:

- [E.Info.SSM-3.SSM.Asset]: List of all confidential personal information, confidential privacy function configuration and confidential security parameter it stores persistently; and
    - (if the SSM implementation is based on [IC.SSM-3.Encryption]) [E.Info.SSM-3.SSM.Encryption]: Description of how secrecy is realized using encryption including:
        - the encryption mechanism and the cryptography that are used to protect the confidentiality of the confidential personal information, confidential privacy function configuration and confidential security parameter it stores persistently; and
        - how the secret used to encrypt the asset was provisioned or derived; and
    - (if the SSM implementation is based on [IC.SSM-3.AccessControl]) [E.Info.SSM-3.SSM.AccessControl]: Description of how secrecy is realized using access control mechanisms including:
        - a description of the access control mechanisms including the corresponding access rights for the confidential personal information, confidential privacy function configuration and confidential security parameter it stores persistently; and
    - (if the SSM implementation is based on [IC.SSM-3.HardwareProtection]) [E.Info.SSM-3.SSM.HardwareProtection]: Description of how secrecy is realized using hardware protection including:
        - a description of what hardware protection is used for the confidential personal information, confidential privacy function configuration and confidential security parameter it stores persistently; and

- (if the SSM implementation is based on [IC.SSM-3.Generic]) [E.Info.SSM-3.SSM.Generic]: Description of the confidentiality protection mechanism used to protect the secrecy of confidential personal information, confidential privacy function configuration or confidential security parameter it stores persistently; and
- if it is claimed that the secure storage mechanism is compliant with recognised security standards or certification schemes, provide evidence to the recognised security standard or certification schemes the secure storage mechanism complies to.

If [IC.SSM-3.Encryption]

- Document HOW…the secret used to encrypt the confidential security parameters, confidential personal information or confidential privacy function configuration cannot be intercepted, deducted, or extracted; and
- Document HOW…reading confidential security parameters, confidential personal information and confidential privacy function configuration without access to the secret used for decryption is not possible

If [IC.SSM-3. AccessControl]

- an unauthorized reading of the stored confidential security parameters, confidential personal information and confidential privacy function configuration is denied.

If [IC.SSM-3. HardwareProtection]

- Document HOW…mechanism used to protect the confidentiality of the stored confidential security parameters, confidential personal information and confidential privacy function configuration cannot be broken or bypassed; and
- Document HOW…an unauthorized reading of the stored confidential security parameters, confidential personal information and confidential privacy function configuration is not possible.

If [IC.SSM-3. Generic]

- Document HOW…unauthorized reading of the stored confidential security parameters, confidential personal information and confidential privacy function configuration is not possible.

Reference to standards:

ISO/IEC 27040:2024 “Information technology — Security techniques — Storage security”

ISO/IEC 27002:2022: “Information security, cybersecurity and privacy protection — Information security controls”

11.6 [SCM] SECURE COMMUNICATION MECHANISM

11.6.1 [SCM-1] APPLICABILITY OF SECURE COMMUNICATION MECHANISMS

Requirement [18031-1] /[18031-2]

The equipment shall always use secure communication mechanisms for communicating security assets and {network}* assets with other entities via network interfaces, except for:

- communicating security assets or {network}* assets whose transfer is protected by physical or logical measures in the targeted environment that ensure that network assets or security assets are not exposed to unauthorised entities; or
- communicating security assets {or network assets}** whose exposure is part of establishing or managing a connection combined with additional measures to authenticate the connection or trust relation

* 18031-2: privacy

** 18031-2: {}

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

- Secure communication mechanisms should use protocols embedding encryption and authentication;
- Specify in the documentation which secure communication protocols have been used/implemented.

In smart metering systems, data might be transmitted to the HES using several intermediate communication protocols. In a layered protocol context, it is therefore always recommended to end-to-end protect the metering data on the application layer. The protection solely by a communication protocol is only advisable if the security layer is terminated in a trusted hosting zone.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
SCM-1.DN-1	Recommended (END)	Not recommended (Go to SCM1-1.DN-2)	Communication of assets should be secure at all times.
SCM-1.DN-2	Not recommended	Go to SCM1-1.DN-3	We cannot assume this
SCM-1.DN-3	Not recommended	Not recommended unless needed to be referred to a Notified Body	We cannot assume this

Required information

Description of each network interface including:

- the description of the physical characteristics including:
  - (in case of a radio interface) [E.Info.SCM-1.NetworkInterface.Radio]: Technology used, the occupied radio spectrum, the transmission power used on the radio interface and the modes of operation that are implemented; or
  - (in case of a wired interface) [E.Info.SCM-1.NetworkInterface.Wired]: Electrical characteristics used on the wired interface and the modes of operation that are implemented; or
  - (in case of an optical interface) [E.Info.SCM-1.NetworkInterface.Optical]: Optical technology used on the interface and the modes of operation that are implemented; or
  - (in case of an acoustic interface) [E.Info.SCM-1.NetworkInterface.Acoustic]: Acoustic technology used on the interface and the modes of operation that are implemented; and
- the description of the logical characteristics including:
  - [E.Info.SCM-1.NetworkInterface.Protocol]:
- Description of all communication protocols implemented on the interface documented in [E.Info.SCM-1.NetworkInterface.Radio], [E.Info.SCM-1.NetworkInterface.Wired], [E.Info.SCM-1.NetworkInterface.Optical] or [E.Info.SCM-1.NetworkInterface.Acoustic] and the modes of operation that are implemented, the version of the protocol and, if applicable, the SW library that is used for the implementation; and
  - the description of the configuration including:
    - applied configuration for the equipment and the available options to change the interface's physical or logical behaviour.
- [E.Info.SCM-1.SecurityAsset]: Description of each stored security asset that is communicated over network interfaces documented in [E.Info.SCM-1.NetworkInterface] and for which confidentiality, integrity or authenticity is needed in order to protect the equipment's privacy assets

For each security asset and for each network asset:

- What up-to-date evaluation methods are used;

What secure communication mechanisms are implemented;

Reference to standards:

ISO/IEC 27033-1:2015 series "Information technology — Security techniques — Network security"

ISO/IEC 27011:2024 "Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations"

ISO/IEC TS 23167:2020 "Information technology — Cloud computing — Common technologies and techniques"

EN13757-7 "Communication systems for meters - Part 7: Transport and security services"

11.6.2 [SCM-2] APPROPRIATE INTEGRITY AND AUTHENTICITY PROTECTION FOR SECURE COMMUNICATION MECHANISMS

Requirement [18031-1] [18031-2]:

Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the integrity and authenticity of the security assets and {network}* assets communicated, except for communicating security assets or {network}* assets where:

- a deviation from best practice for integrity or authenticity protection is required for interoperability reasons.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

- All data exchanges SHALL be cryptographically protected and optionally also physically protected.
- Since Risk Analysis may indicate different levels of protection are appropriate, exceptions to this encryption requirement MAY be possible for certain data e.g. the meter serial number which can be printed in front of the meter; however, the requirement should apply to logical IDs related to meters, e.g. the meter ID (logical) and the delivery point ID (logical);
- Different levels of protection MAY be provided, depending on the type of the data.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
SCM-2.DN-1	Recommended (END)	Not recommended (Go to SCM-2.DM-2)	Interoperability issues cannot be used as an exception for smart meters
SCM-2.DN-2	Not recommended	Not recommended unless needed to be referred to a Notified Body	

Implementation categories:

[IC.SCM-2.ManufSecret]: The method is to introduce the (initial) secret used to ensure integrity and authenticity of communicated privacy assets and security assets the production of the equipment. The secret is individual for an equipment and is only used inside it. The protection of integrity and authenticity itself is realized as channel or message based with a message authentication code based on the secret.

Typically, this is a preferred method for securing communications. This is supported by many communication standards used in metering systems.

[IC.SCM-2.SecChanExchange]: The method to exchange initial secrets relies on an independent channel: The (initial) secret used to ensure integrity and authenticity of communicated privacy assets and security assets is solely exchanged via a second channel which is independent from the communication mechanism. The protection of integrity and authenticity itself is realized as channel or message based with a message authentication code based on the secret.

EXAMPLE: Input of a shared key through a QR Code or manual entry of a secret

Some smart meters can be commissioned using local ports to read QR or barcodes to introduce initial secrets

[IC.SCM-2.PKI-based]: The method to authenticate the certificate used to ensure integrity and authenticity of communicated privacy assets and security assets is solely based on the signature of the certificate issued by a trusted PKI. The protection of integrity and authenticity itself is realized channel or message based with a message authentication code based on the secret.

EXAMPLE: Usage of X.509 PKI-Certificates for TLS

Typically, this is a preferred method for securing communications. This is supported by many communication standards used in metering systems

[IC.SCM-2.ThirdPartyTrust]: The method to authenticate the (initial) secret used to ensure integrity and authenticity of communicated privacy assets and security is solely based on an existing trust relation to a third party which confirms the authenticity of the secret. The protection of integrity and authenticity itself is realized channel or message based with a message authentication code based on the secret.

EXAMPLE: Kerberos protocol

Typically, not appropriate

[IC.SCM-2.Generic]: The methods to ensure integrity and authenticity of communicated privacy assets (documented in [E.Info.SCM-2.PrivacyAsset]) and security assets do not solely rely on any of the methods described before in this section.

Typically, not appropriate

Required information:

- Description of each stored security asset that is communicated over network interfaces documented in and for which integrity or authenticity protection is needed in order to protect the equipment's network assets, including:
    - Description of the use case where the asset is communicated (e.g. pairing with base station)
- Description of each network asset that is communicated over network interfaces documented in and for which integrity or authenticity protection is needed, including:
    - Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface.
- Description of all network interfaces of the equipment, including

- All communication protocols implemented and the modes of operation that are implemented, the version of the protocol and, if applicable, the SW library that is used for the implementation.

- Description of each secure communication mechanism that is required per SCM-1 for the integrity and authenticity protection of communicated network assets documented in or security assets documented in, including
  - [Description of the security mechanisms and cryptographic modes that are used to protect the integrity and authenticity of security assets documented in or network assets documented in while communicated over network interfaces security; and
  - (if the SCM implementation is based on [IC.SCM-2.ManufSecret]): Description of how the initial trust is achieved for integrity and authenticity protection and how it is implemented in the protocol ; and
  - (if the SCM implementation is based on [IC.SCM-2.SecChanExchange]) [E.Info.SCM-2.SCM.SecChanExchange]: Description of how the second channel is realized and how the secret is used for integrity and authenticity protection and how it is implemented in the protocol ; and
  - (if the SCM implementation is based on [IC.SCM-2.PKI-based]): Description of how the PKI-certificates are validated and how this is implemented for integrity and authenticity protection in the protocol doc; and
  - (if the SCM implementation is based on [IC.SCM-2.ThirdPartyTrust]): Description of how the existing trust relation to a third party which confirms the authenticity of the secret is realized and how this is implemented for integrity and authenticity protection in the protocol, and
  - (if the SCM implementation is based on [IC.SCM-2.Generic]) [E.Info.SCM-2.SCM.Generic]: Description of how integrity and authenticity protection is realized in the protocol; and
  - (if available) [E.Info.SCM-2.SCM.ImplDetail]: Refer to versioned standards or specifications where the selected implementation category is defined and, if applicable, the SW library that is used for the implementation; and
  - The description of the properties of the confidential cryptographic keys used for integrity and authenticity protection (see CRY-1); and
  - The description on how the mechanism protects against the following security threats:
    o Spoofing; and
    o Tampering.

- Description of the selected path through the decision tree in Figure 18 for each secure communication mechanism documented in [E.Info.SCM-2.SCM].

  NOTE: 3 Multiple valid paths might need documentation due to the classification of security assets or network assets and the equipment states doc.

For each security asset and network asset:

- What up-to-date evaluation methods are used;
- What integrity and authenticity protection is ensured by the communication mechanisms;

If [AU.SCM-2.ManufSecret]:

- how the secret introduced during production cannot be intercepted while the equipment is communicating via network; and
- how a manipulated message is not accepted as being of integrity; and
- how an unauthorized message is not accepted as authentic; and

- how a successful MitM attack is not possible in case that channel-based communication is used.

If [AU.SCM-2.SecChanExchange]:

- how the secret cannot be intercepted using the assessed communication mechanism; and
- how a manipulated message is not accepted as being of integrity; and
- how an unauthorized message is not accepted as authentic; and
- how a successful MitM attack is not possible in case that channel-based communication is used.

If [AU.SCM-2.PKI-based]:

- how a forged certificate is not accepted; and
- how a manipulated message is not accepted as being of integrity; and
- how an unauthorized message is not accepted as authentic; and
- how a successful MitM attack is not possible in case that channel-based communication is used.

If [AU.SCM-2.ThirdPartyTrust]:

- how the response of the third party cannot be manipulated; and
- how a manipulated message is not accepted as being of integrity; and
- how an unauthorized message is not accepted as authentic; and
- how a successful MitM attack is not possible in case that channel-based communication is used.
- how is the root of trust verified

If [AU.SCM-2.Generic]:

- how secrets used for the protection of authenticity and integrity cannot be intercepted and misused; and
- how a manipulated message is not accepted as being of integrity; and
- how an unauthorized message is not accepted as authentic; and
- how a successful MitM attack is not possible in case that channel-based communication is used.

Reference to standards:

ISO/IEC 27033-1:2015 series “Information technology — Security techniques — Network security”

ISO/IEC 27011:2024 “Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations”

ISO/IEC TS 23167:2020 “Information technology — Cloud computing — Common technologies and techniques”

EN13757-7 “Communication systems for meters - Part 7: Transport and security services”

11.6.3 [SCM-3] APPROPRIATE CONFIDENTIALITY PROTECTION FOR SECURE COMMUNICATION MECHANISMS

Requirement [18031-1] [18031-2]:

Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated {network}* assets and security assets where confidentiality protection of those is needed, except for communicating security assets or {network}* assets where:

- a deviation from best practice for protecting confidentiality is required for interoperability reasons.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

For each network interface, the communication of security assets and network assets [18031-1] or privacy assets [18031-2] must be performed using communication protocols ensuring the confidentiality by means of appropriate encryption algorithms.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
SCM-3.DN-1	Recommended (END)	Not recommended (Go to SCM-3.DN-2)	Interoperability issues should not be a reason to compromise smart meters
SCM-3.DN-2	Not recommended	Not recommended unless needed to be referred to a Notified Body	

Implementation category:

[IC.SCM-3.MessageEnc]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the encryption. The method is that each message encapsulates the content-encryption key to decrypt the payload of the message. This key is encrypted symmetrically or asymmetrically with the existing secret. An authorized receiving entity can only decrypt the payload, if it holds the key to decrypt the content-encryption key before.

[IC.SCM-3.ChannelEnc]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the encryption. The method is that the equipment and the receiving entity possess the same symmetric key which is used to decrypt and encrypt the payload of communicated messages.

[IC.SCM-3.Generic]: The methods to ensure the confidentiality of communicated privacy assets and security assets do not solely rely on any of the methods described before in this section.

Required information:

- Description of each stored security asset that is communicated over network interfaces and for which confidentiality is needed in order to protect the equipment's network assets, including:
    - Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface doc
- Description of all network assets that are communicated over network interfaces and for which confidentiality is needed, including
- Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface.
- Description of all network interfaces of the equipment, including
    - All communication protocols implemented and the modes of operation that are implemented, the version of the protocol and, if applicable, the SW library that is used for the implementation.

- Description of each secure communication mechanism that is required per SCM-1 for confidentiality protection of network assets or security assets, including:

- Description of the security mechanisms and cryptographic modes that are used to protect the confidentiality of security assets or network assets while communicated over network interfaces; and
- (if the SCM implementation is based on [IC.SCM-3.MessageEnc]) Description of how the content-encryption key is generated and encrypted for confidentiality protection and how it is implemented in the protocol; and
- (if the SCM implementation is based on [IC.SCM-3.ChannelEnc]) Description of how the session key is generated and used for confidentiality protection and how it is implemented in the protocol; and
- (if the SCM implementation is based on [IC.SCM-3.Generic]) Description of how confidentiality protection is realized in the protocol; and
- (if available) [E.Info.SCM-3.SCM.ImplDetail]: Refer to versioned standards or specifications where the selected implementation category is defined and, if applicable, the SW library that is used for the implementation; and
- The properties of the confidential cryptographic keys used for confidentiality protection (see CRY-1); and
- How the mechanism at least protects against the following security threats:
  - Information disclosure; and
  - Elevation of privilege

- For each security asset and network asset:
  - What up-to-date evaluation methods are used;
  - Document HOW confidentiality protection is ensured by the communication mechanisms;

If [AU.SCM-3.MessageEnc]:

- Document HOW the key inside the message which is used to encrypt the payload cannot be disclosed; and
- Document HOW the communicated security assets and network assets cannot be eavesdropped.

If [AU.SCM-3.ChannelEnc]:

- Document HOW the key which is used to encrypt the messages inside the communication channel cannot be intercepted; and
- Document HOW the communicated security assets and network assets cannot be eavesdropped.

If [AU.SCM-3.Generic]:

- Document HOW the secret used to encrypt the message cannot be intercepted or eavesdropped; and
- Document HOW the encrypted content of the message cannot be eavesdropped or disclosed.

Reference to standards:

ISO/IEC 27033-1:2015 series “Information technology — Security techniques — Network security”
ISO/IEC 27011:2024 “Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations”
ISO/IEC TS 23167:2020 “Information technology — Cloud computing — Common technologies and techniques”
EN13757-7 “Communication systems for meters - Part 7: Transport and security services”

11.6.4 [SCM-4] APPROPRIATE REPLAY PROTECTION FOR SECURE COMMUNICATION MECHANISMS

Requirement [18031-1] [18031-2]:

Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the {network}* assets communicated against replay attacks, except for communicating security assets or {network}* assets where:

- a duplicate transfer does not impose a threat of a replay attack; or
- {a deviation from best practice for replay protection is required for interoperability reasons.}

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

For each network interface, the communication of security assets and network assets [18031-1] or privacy assets [18031-2] must be performed using communication protocols ensuring the protection against replay attacks by means of appropriate cryptographic algorithms.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
SCM-4.DN-1	Recommended (END)	Not recommended (Go to SCM-4.DN-2)	Smart meters should be protected against replay attack under all circumstances
SCM-4.DN-2	Not recommended (END)	Not recommended (Go to SCM-4.DN-3)	
SCM-4.DN-3	Not recommended	Not recommended unless needed to be referred to a Notified Body	

Implementation categories:

- [IC.SCM-4.SeqNumb]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the message authentication code to ensure the integrity of the communication. The method is that a unique sequence number is assigned to each message transmitted. When the recipient receives a message, it checks the sequence number to ensure that it has not been received before. If the sequence number has already been seen, the message is discarded as a replay attack.
  NOTE 1: To protect against MitM Attacks the authenticity of the sequence number can be ensured by using it as input to the function generating the message authentication code (MAC).
  This is a typical method for protecting against replay attacks

- [IC.SCM-4.TimeStamp]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the message authentication code to ensure the integrity of the communication. The method is that the equipment integrates timestamps in messages to ensure that they are not being replayed at a later point in time. The recipient checks the timestamp to make sure that the message was not generated too far in the past or future.
  NOTE 2: To protect against MitM Attacks the authenticity of the timestamp can be ensured by using it as input to the function generating the message authentication code (MAC).
  This is a typical method for protecting against replay attacks

- [IC.SCM-4.OneTimeEncKey]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the message authentication code to ensure the integrity of the communication. The method is that the equipment and the receiver establish a

completely random session key, which is a type of code that is only valid for one transaction and cannot be reused.
This is a typical method for protecting against replay attacks

-
- [IC.SCM-4.Generic]: The methods to avoid replay attacks concerning communicated privacy assets security assets do not solely rely on any of the methods described before in this section.

  Under this category the use of nonces to assure freshness and prevent replay attacks is very common in the metering world (e.g. EN13757-7)

Required information:

- Description of each stored security asset that is communicated over network interfaces for which replay protection is needed in order to protect the equipment's network assets, including:
  - Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface
- Description of each network asset that is communicated over network interfaces do and for which replay protection is needed, including:
  - Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface
- Description of each network interface of the equipment, including:
  - All communication protocols implemented and the modes of operation that are implemented, the version of the protocol and, if applicable, the SW library that is used for the implementation.

- Description of each secure communication mechanism that is required per SCM-1 for replay protection of network assets or security assets including:
  - Description of the security mechanisms and cryptographic modes that are used to avoid replay attacks on communication containing security assets or network assets and
  - (if the SCM implementation is based on [IC.SCM-4.SeqNumb]) Description of how the sequence numbers are used and integrated in the message authentication code for replay protection and how it is implemented in the protocol; and
  - (if the SCM implementation is based on [IC.SCM-4.TimeStamp]) : Description of how the time stamps are used and integrated in the message authentication code for replay protection and how it is implemented in the protocol ; and
  - (if the SCM implementation is based on [IC.SCM-4.OneTimeEncKey]) Description of how the one-time encryption key is generated and used for replay protection and how it is implemented in the protocol; and
  - (if the SCM implementation is based on [IC.SCM-4.Generic]): Description of how replay protection is realized in the protocol doc; and
  - (if standards or specifications where the selected implementation category is defined are available) : Reference to versioned standards or specifications where the selected implementation category is defined and, if applicable, the SW library that is used for the implementation; and
  - Description of how the mechanism at least protects against the security threat "Repudiation".

  - For each security asset and network asset:
    - What up-to-date evaluation methods are used;
    - Document HOW replay protection is ensured by the communication mechanisms;

If [AU.SCM-4.SeqNumb]:

- Document HOW the incoming message (part of the communication of security assets and network assets) with a repeating sequence number is not accepted.

If [AU.SCM-4.TimeStamp]:

- Document HOW the incoming message (part of the communication of security assets and network assets) with an irregular timestamp is not accepted.

If [AU.SCM-4.OneTimeEncKey]:
- Document HOW the encryption key cannot be intercepted; and
- Document HOW the duplicate (binary copy) of an already accepted message (part of the communication of security assets and network assets) is not accepted again.

If [AU.SCM-4.Generic]:
- Document HOW the duplicate (binary copy) of an already accepted message (part of the communication of security assets and network assets) is not accepted again.

Reference to standards:

ISO/IEC 27033-1:2015 series "Information technology — Security techniques — Network security"
ISO/IEC 27011:2024 "Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations"
ISO/IEC TS 23167:2020 "Information technology — Cloud computing — Common technologies and techniques"
EN13757-7 "Communication systems for meters - Part 7: Transport and security services"

11.7 [RLM] RESILIENCE MECHANISM

11.7.1 [RLM-1] APPLICABILITY OF RESILIENCE MECHANISMS

Requirement [18031-1]:

The equipment shall use resilience mechanisms to mitigate the effects of Denial of Service (DoS) Attacks on the network interfaces and return to a defined state after the attack except for:
- network interfaces that are only used in a local network that do not interoperate with other networks; or
- network interfaces where other devices in the network provide sufficient protection against DoS attacks and loss of essential functions for network operations.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

The manufacturer implements supervision of the availability of network assets. There are recovery capabilities implemented to return to a defined state after an attack.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
RLM-1.DN-1	Recommended (END)	Not recommended (Go to RLM-1.DN-2)	The H1 port might not need to be protected
RLM-1.DN-2	Not recommended	Not (Go to RLM-1.DN-3)	
RLM-1.DN-3	Not recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

For each network interface:
- Description of each network interface
- Description of the implemented resilience mechanism

Options
MAY Not be APPLICABLE for Port H1 MAY Not be APPLICABLE for Port M

11.8 [NMM] NETWORK MONITORING MECHANISM

11.8.1 [NMM-1] APPLICABILITY OF AND APPROPRIATE NETWORK MONITORING MECHANISMS

Smart meters are not Network equipment, so this requirement does not apply.

11.9 [TCM] TRAFFIC CONTROL MECHANISM

11.9.1 [TCM-1] APPLICABILITY OF AND APPROPRIATE TRAFFIC CONTROL MECHANISMS

Smart meters are not Network equipment, so the requirement does not apply.

11.10 [LGM] LOGGING MECHANISM

11.10.1 [LGM-1] APPLICABILITY OF LOGGING MECHANISMS

Requirement [18031-2]:

The equipment shall provide a mechanism to log internal activities that are relevant to privacy assets and their protection (referred to as Events).

Applicable Smart metering	**Yes**	**18031-1**	**No**
		18031-2	**Yes**

Commentary:

The smart meter maintains a log of security events and protects the log against unauthorized modification. See Protection Profile (reference [2]) P-Logging.

The manufacturer will implement the following (Protection Profile reference):

- physical tampering attempts to be logged (FPT_TNN.1);
- list of other events to be logged and the basic content of the log records (FAU_GEN.1);
- provision of accurate time for use in the log records (FPT_STM.1);
- ensure that audit records can only be deleted by authorised roles and that they cannot be modified (by any entity) (FMT_MTD.1and FAU_STG.1);
- only authorized entities can read the audit log (FAU_SAR.1);
- the action to be taken if the log is in danger of filling up (FAU_STG.3);
- definition of the entities on which audit activity and constraints are based (FMT_SMR.1).

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
LGM-1.DN-1	Not recommended	Recommended (Go to LGM-1.DN-2)	There is no legal obligation that prohibits logging of E.Info.LoggingEvents

LGM-1.DN-2	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each internal activity that is relevant for privacy assets and their protection, including:

- (if a legal obligation prohibits logging of the internal activity) [E.Info.LGM-1.PrivacyAssetEvent.Legal]: References to all corresponding paragraph(s) or passages in all relevant legal documents, including a description on how this is applicable for the equipment's internal activity; and
- (if no legal obligation prohibits logging of the internal activity) [E.Info.LGM-1.PrivacyAssetEvent.LGM]: Description of the logging mechanism used to log the event

Description of each Privacy Asset Event (activities, exceptions or faults) to be logged

From "Minimum Security requirements for AMI components" (ref [1]):

- User Authentication for a particular role (Successful and failed authentication)
- Firmware updates (successful and failed)
- Setting the time of the device
- Tamper detection
- Reconfiguration of cryptographic parameters
  - Key changes
  - Change of access rights
  - Reset of random number generator
- Security attack attempt

Reference to standards:

CENCLCETSI_SMCG/Sec/00156/DC Protection Profile for Smart Meter Minimum Security Requirements [9]

11.10.2 [LGM-2] PERSISTENT STORAGE OF LOG DATA

Requirement [18031-2]:

Logging mechanisms that are required per LGM-1 shall store log data for related events in the equipment's persistent storage, except for events where:

- related log data is stored outside the equipment.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Where possible, meter events should be stored in flash memory allowing their retention even when onboard batteries fails.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
LGM-2.DN-1	Sometimes (END)	Sometimes (Go to LGM-2.DN-2)	Sometimes the data is held on a head end system and so would be

			out of scope of the analysis
LGM-2.DN-2	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each logging mechanism that is required per LGM-1, including:

- a description of the logged events, including:
  - (if log data storage in equipment's persistent storage is claimed to be required) [E.Info.LGM-2.LGM.InternalStorage]: The storage location of log data for related events on the equipment and a description of how persistence of the stored log data is ensured; and
  - (if log data storage in equipment's persistent storage is claimed to be not required because storage happens outside the equipment) [E.Info.LGM-2.LGM.ExternalStorage]: Description of the equipment's functionality to support storage of log data outside the equipment

11.10.3 [LGM-3] MINIMUM NUMBER OF PERSISTENTLY STORED EVENTS

Requirement [18031-2]:

All log data stored in equipment's persistent storage by logging mechanisms that are required per LGM-1 shall always include:

- a minimum number of the latest events; and
- the latest event.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Typically smart meters should be able to store prefered 100 events if resources permit that are related to the security of the meter.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
LGM-3.DN-1	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

- Description of the logged events [E.Info.LGM-3.Events], where related log data is persistently stored on the equipment and [E.Info.LGM-3.Quantity] where
  - [E.Info.LGM-3.Quantity]: Minimum number of the latest events for which log data can be persistently stored on the equipment simultaneously and a description of the log data's storage locations

11.10.4 [LGM-4] TIME-RELATED INFORMATION OF PERSISTENTLY STORED LOG DATA

Requirement [18031-2]:

All log data stored in equipment's persistent storage by logging mechanisms that are required per LGM-1 shall include:

- a timestamp if real time is available on the equipment; and
- time-related information if real time is not available on the equipment

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

There is a known error in the original version of the specifications which will be documented in a corrigendum.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
LGM-4.DN-1	Recommended (Go to LGM-4.DN-2)	Not recommended unless needed to be referred to a Notified Body	
LGM-4.DN-2	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

- Description of the logged events, where related log data is persistently stored on the equipment.

- [E.Info.LGM-4.LGM]: Description of each logging mechanism that is required per LGM-1 that generates log data stored in equipment's persistent storage, including:
  - (if real time information can be available on the equipment) [E.Info.LGM-4.LGM.Timestamp]: Description of each real time source and the corresponding timestamp included in the persistently stored log data; and
  - (if real time information is not reliably available on the equipment) [E.Info.LGM-4.LGM.Timerelated]: Description of the time-related information included in the persistently stored log data.

NOTE : Inconsistency in the EN 18031-2, figure 29: Decision Tree for requirement LGM-4
A YES in DT.LGM-4.DN-1 shall lead to PASS
A NO in DT.LGM-4.DN-1 shall lead to DT.LGM-4.DN-2
A YES DT.LGM-4.DN-2 shall lead to PASS
A NO in DT.LGM-4.DN-2 shall lead to FAIL

11.11 [DLM] DELETION MECHANISM

11.11.1 [DLM-1] APPLICABILITY OF DELETION MECHANISMS

Requirement [18031-2]:

The equipment shall provide a deletion mechanism that allows a user to delete their personal data and sensitive security parameters stored on the equipment.

Applicable Smart metering	**Yes**	**18031-1**	**No**
		18031-2	**Yes**

Commentary:

For smart meters the consumer's historical meter data may reveal use habits and can therefore eventually be used to predict a person's location. It is a right for users to be able to decide on their personal (location or user pattern) data. The standardisation request (M585) explains the reason for this requirement with "enabling the disposal or replacement of equipment without the risk of exposing personal data".

The totalizer of a smart meter will never be deleted. Historic values or values that can be used to reveal consumer habits, or keys and passwords that are defined by the consumer, shall have the ability to be deleted.

In practice authorized deletion of data is performed by the meter operator or service operator on behalf of the consumer when the consumer moves out of the premises (re-using the smart meter) or the meter is replaced (for disposal).

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
DLM-1.DN-1	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each deletion mechanism including a description on whether the deletion mechanism ensures that personal data and/or sensitive security parameters stored on the equipment can be deleted, for the purpose of disposal or replacement of the equipment:

- by users; or
- when an authorised entity has supervisory responsibility to delete the personal data and/or sensitive security parameter on behalf of the user, by this entity.

11.12 [UNM] USER NOTIFICATION MECHANISM

11.12.1 [UNM-1] APPLICABILITY OF USER NOTIFICATION MECHANISMS

Requirement [18031-2]:

The equipment shall provide user notification mechanism(s) for informing the user of the equipment about changes affecting the protection or privacy of personal information, except for changes where:

- other methods of informing the user exist, which do not involve the equipment.

Applicable Smart metering	**Yes**	**18031-1**	**No**
		18031-2	**Yes**

Commentary:

Information to the user may be provided as text on a display, using a sound/voice or a light. A smart meter is typically installed in a location that is rarely visited by the costumer (e.g. a water meter in a pit). Therefore, it makes often no sense to use the smart meter itself as a notification equipment. Furthermore, there are few use cases where the consumer is able to take a corrective mitigation action to the notified event. Therefore, if possible, it is an advantage to notify the consumer via the owner of the equipment (utility) using other channels (E-mail, letter, telephone, etc.).

Compromising the smart meter in any way (e.g. tampering, circumventions of security mechanisms) should lead to an alerting event being created in the smart meter. The smart meter should report about events to the HES to inform the meter operator to take corrective measures.

Other use cases are events that are directed towards the meter operator or service operator:

- Security updates – The manufacturer has identified that a smart meter needs security update (firmware, and/or patching). The service operator may be able to patch the affected products/series
- Compromise of data – A key or a range of keys have been exposed. The meter operator should as soon as possible mitigate the problem by changing authenticators (keys) and inform the end consumer about the security event

- Change of data collection – Example: The utility decides to collect data from the consumer with a higher resolution than agreed in the contract. The customer shall be informed in advance of the change.

The user manual of the smart meter shall describe which events and under which conditions they will lead to a notification on the smart meter and/or in the HES.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
UNM-1.DN-1	Typically (END) The information on security events or security updates is provided by the manufacturer to the meter operator or service operator without delay. The information on a security event or if configuration changes collection of consumption data is provided to the consumer with minimum delay in a way agreed in a contract between the utility and the consumer.	The user is notified via information on the equipment (Go to UNM-1-DN2)	
UNM-1-DN2	Recommended The consumer has the possibility to be informed about security events affecting privacy data.	No possibility of notifying the consumer about security events affecting privacy data Not recommended unless needed to be referred to a Notified Body	

Required information:

- Description of each use case where changes can affect the protection or privacy of the personal information, including:
  - [E.Info.UNM-1.PersonalInformation.UseCase.Notification]: Description of the user notification mechanism that notifies the user about this change; or
  - (if there is another method to inform the user, which do not involve the equipment) [E.Info.UNM-1.PersonalInformation.UseCase.OtherInfo]: Description of other method(s) to inform the user not involving the equipment

11.12.2 [UNM-2] APPROPRIATE USER NOTIFICATION CONTENT

Requirement [18031-2]:

The content of a notification provided by a user notification mechanism that is required per UNM-1 shall include at least:

- a description of a change; and
- a description of how a change will affect the protection and privacy of personal information.

Applicable Smart metering	**Yes**	**18031-1**	**No**
		18031-2	**Yes**

Commentary:

This requirement is only applicable to smart meters that notify consumers using the smart meter itself.

The user manual or the manufacturers home page of the smart meter shall clearly describe which events are notified on the smart meter and how the status message is formatted and understood (e.g. meaning of error codes if not in clear text).

NOTE: The consumer is not expected to identify the exact model number. Therefore, error codes should not be reused for different purposes in a manufacturer's product suite.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
UNM-2.DN-1	Recommended Description in the notification message is sufficiently descriptive of the represented event or with a clear lookup to the user manual or link to the manufacturers home page.	Notification does not lead to determination of the security event. Not recommended unless needed to be referred to a Notified Body	

Required information:

- Description of each user notification mechanism that is required per UNM-1, including:
  - [E.Info.UNM-2.Notifications.UseCase]: Description of each use case where notifications are provided by the user notification mechanisms, including:
    - [E.Info.UNM-2.Notifications.UseCase.Content]: Description of the content of the notifications for the use case.

11.13 [CCK] CONFIDENTIAL CRYPTOGRAPHIC KEYS

11.13.1 [CCK-1] APPROPRIATE CCKS

Requirement [18031-1] [18031-2]:

Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits, except for:

- CCKs that are solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.

NOTE 1: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used {to harm the network or its functioning or for the misuse of network resources}*, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key.

NOTE 2 The requirement refers to all confidential cryptographic keys chosen by the equipment manufacturer either directly or imposed by a protocol. For instance, the manufacturer directly chooses/configures the cipher suite of TLS protocol to be used by the device, other protocols may impose one single option for cryptographic algorithms and their respective keys.

* 18031-2: to compromise the user's or subscriber's privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

The manufacturer implements crypto mechanism and key management that is compliant with recognized/proven and approved open standards. The mechanisms providing encryption and authentication considers NIST recommended (or NSA suite B) cryptography.
Note: Requirements ACM, AUM, SCM, SUM and SSM exempt some data transfer from cryptographic protection and so this requirement does not apply in each of these circumstances.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
CCK-1.DN-1	Not typical (END)	Typical (move to CCK-1.DN-2)	
CCK-1.DN-2	Necessary for compliance	Not recommended unless needed to be referred to a Notified Body	

Required information:

For each confidential cryptographic key (whether preinstalled or generated by the equipment during its use), describe:

- The cryptographic algorithms for the confidential cryptographic key and the key length of confidential cryptographic key's implementation; and
- (if the confidential cryptographic key is solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM)[E.Info.CCK-1.CCK.Deviation]: Reference to the corresponding justification and to the required information the justification is based on; and
- The security strength and the reference of the lookup tables used in the assessment.

11.13.2 [CCK-2] CCK GENERATION MECHANISMS

Requirement [18031-1] [18031-2]
The generation of confidential cryptographic keys shall adhere to best practice cryptography, except for:

- the generation of CCKs for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.

NOTE: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to {harm the network or its functioning or for the misuse of network resources}*, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key.

* 18031-2: compromise the user's or subscriber's privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

For cryptographic keys that are generated in the device, it is strongly recommended to use hardware strong random number generation functions.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
CCK-2.DN-1	Not recommended (END)	Recommended (Go to CCK-2.DN.2)	ACM, AUM, SCM, SUM and SSM state exemption in case the CCK is exclusively used for the exempt

			use case. The reason for these exemptions can be the required function, the intended operational environment or legal requirements. (for details, please check ACM, AUM, SCM, SUM and SSM
CCK-2.DN-2	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each generation mechanism for confidential cryptographic keys, including the following details:

- [E.Info.CCK-2.Generation.CCK]: Specification of the confidential cryptographic keys the mechanism generates and whether their generation adheres to best practice cryptography; and
- (if the generation mechanism for CCK relies on a random number source and is used for the generation of confidential cryptographic key that adhere to best practice cryptography)
  - specify the best practices followed by the random number source; and
  - explain why the random number source provides sufficient security strength; and
  - explain how the random number source is configured and initialised; and
  - if it is claimed that the CCK is compliant with recognised security standards or certification schemes, provide evidence to the recognised security standard or certification schemes the CCK complies to; and
- (if the generation mechanism for CCK relies on a random number generator and is used for the generation of confidential cryptographic key that adhere to best practice cryptography):
  - specify whether it is a deterministic or a non-deterministic random number generator; and
  - specify the best practices followed by the random number generator; and
  - specify why the random number generator provides sufficient security strength; and
  - explain how the random number generator is configured and initialised; and
  - if it is claimed that the CCK is compliant with recognised security standards or certification schemes, provide evidence to the recognised security standard or certification schemes the CCK complies to; and
- (if the generation mechanism for CCK relies on a derivation mechanism/ establishment mechanism and is used for the generation of confidential cryptographic key that adhere to best practice cryptography):
  - specify the best practices followed by the derivation mechanism/ establishment mechanism; and
  - specify the key derivation/generation algorithm used for that; and
- (if the generation mechanism generates confidential cryptographic keys used solely by a specific security mechanism, where a deviation from best practice cryptography is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM) [E.Info.CCK-2.Generation.Deviation]:
  - reference the corresponding justification and to the required information the justification is based on.

11.13.3 [CCK-3] PREVENTING STATIC DEFAULT VALUES FOR PREINSTALLED CCKS

Requirement [18031-1] [18031-2]:

Preinstalled confidential cryptographic keys shall be practically unique per equipment, except for:
- CCKs that are only used for establishing initial trust relationships under conditions controlled by an authorized entity; or
- CCKS key are shared parameters required for the equipment's intended functionality.

NOTE: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used {to harm the network or its functioning or for the misuse of network resources}*, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key.

* 18031-2: to compromise the user's or subscriber's privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
CCK-3.DN-1	Recommended (END)	Not recommended (Go to CCK-3.DN-2)	
CCK-3.DN-2	Not recommended (END)	Not recommended (Go to CCK-3.DN-3)	
CCK-3.DN-3	Not recommended (END)	Not recommended unless needed to be referred to a Notified Body	

Required information:

Description of each preinstalled confidential cryptographic key on the equipment, including:
- [E.Info.CCK-3.CCK.Unique]: Description of the methods that result in the CCK being practically unique per equipment.

11.14 [GEC] GENERAL EQUIPMENT CAPABILITIES

11.14.1 [GEC-1] UP-TO-DATE SOFTWARE AND HARDWARE WITH NO PUBLICLY KNOWN EXPLOITABLE VULNERABILITIES

Requirement [18031-1] [18031-2]:

The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and {network}* assets, except for vulnerabilities:
- that cannot be exploited in the specific conditions of the equipment; or
- that have been mitigated to an acceptable residual risk; or
- that have been accepted on a risk basis.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

A smart meter may be deployed for a lifetime of up to 20 years. In this case the updateability requirement in SUM plays an important role.

Metering systems though are often deployed in stages. When deploying new smart meters to existing smart meter systems based on older security architectures, there is a risk that the newly deployed smart meters may be compatible with the older systems for interoperability reasons. These older security designs may contain security solutions that differ from state of the art and may even be deprecated in newest protocol standards or specifications.

It is always recommended that smart meter is deployed without known exploitable vulnerabilities. If a smart meter needs to be used in a legacy installation this should preferably be done by configuration after installation, while applying countermeasures to the exploitation of the vulnerability based on the concrete installation.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
GEC-1.DN-1	Not recommended (Go to GEC-1.DN.2)	PASS / Recommended	
GEC-1.DN-2	Not recommended (Go to GEC-1.DN-4	Not recommended	The effects on overall functionality of the smart meter should be considered when justifying NOT APPLICABLE
GEC-1.DN-3	Not recommended (Go to GEC-1.DN-4	Not recommended	If justifying NOT APPLICABLE, it shall be documented why it cannot be exploited (architecture, configuration, etc.)
GEC-1.DN-4	Mitigation has been implemented against the exploitation of the vulnerability (e.g. a software patch is available that can be applied before use) (END)	Not recommended No mitigation has been found (Go to GEC-1.DN-4)	
GEC-1.DN-5	The vulnerability is accepted due to a minimal risk, e.g. it cannot be exploited in a normal use case scenario. (END)	Not recommended unless needed to be referred to a Notified Body	

Required information:

- Description of the software of the equipment, including their versions, that affect the security assets and the privacy assets
- Description of the hardware of the equipment that affect the security assets and the privacy assets
- Description of all publicly known exploitable vulnerabilities in the hardware and software that affect the security assets and the privacy assets. The document includes also the source of the vulnerabilities' information. Further a justification is given for each vulnerability that affects privacy assets and security assets about the remediation, mitigation and non-exploitation of the listed hardware or software publicly known exploitable vulnerabilities, including:
  - (if the vulnerability is remediated) [E.Info.GEC-1.ListOfVulnerabilities.Remediated]: The measures implemented to remediate the vulnerability; and
  - (if the vulnerability cannot be exploited in the specific conditions of the equipment) [E.Info.GEC-1.ListOfVulnerabilities.SpecificCondition]: The description of specific conditions in which the vulnerability cannot be exploited; and
  - (if the vulnerability is mitigated) [E.Info.GEC-1.ListOfVulnerabilities.Mitgated]: The description of the measures for the mitigation; and

- (if the vulnerability is accepted) [E.Info.GEC-1.ListOfVulnerabilities.Accepted]: The description of the acceptance of the vulnerability on a risk basis.

11.14.2 [GEC-2] LIMIT EXPOSURE OF SERVICES VIA RELATED NETWORK INTERFACES

Requirement [18031-1] [18031-2]:

In factory default state the equipment shall only expose

- network interfaces; and
- services via network interfaces

affecting security assets or {network}* assets which are necessary for equipment setup or for basic operation of the equipment.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

A smart meter providing meter data (service) via network interfaces is categorized as an equipment with a controlled fixed functionality. Data can either be transmitted unsolicited or on request.

In factory default state (or transport state) the smart meter should not start transmitting its privacy assets before a proper installation has been made and key material has been established between the smart meter and its communication partner. The exchange of security assets (key material), if not pre-installed, shall only be possible via a secured protocols and/or supervised by an authorized person.

Network assets (services) shall only temporarily be exposed in factory default state to establish the trusted security context.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
GEC-2.DN-1	The network interface or service assessed is available in factory default (Go to GEC-2.DN-2)	The network interface or service assessed is not available in factory default (END)	No recommendation
GEC-2.DN-2	The assessed interface or service affects security assets or network assets (Go to GEC2.DN-3)	No privacy data or network data or key material are affected via the assessed network interface (END)	No recommendation
GEC-2.DN-3	Recommended The smart meter has a pre-installed key that demands the corresponding key to be available to decode metering data or to authenticate metering data requests. The network interface provides only network assets that are required for establishing the smart meter's secure communication (END)	Not recommended unless needed to be referred to a Notified Body	

Required information:

- Description of each network interface and exposed service (via network interfaces) in factory default state of the equipment, including information if they are required for the basic operation or for the setup of the equipment or if they are optional.
- (if the equipment implements a setup process) Documentation how to setup the equipment.
- Description of each security asset that is accessible via network interfaces.
- Description of each privacy asset that is accessible via network interfaces.

11.14.3 [GEC-3] CONFIGURATION OF OPTIONAL SERVICES AND THE RELATED EXPOSED NETWORK INTERFACES

Requirement [18031-1] [18031-2]:

Optional network interfaces or optional services exposed via network interfaces affecting security assets or {network}* assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Optional interfaces or exposed services are disabled in factory-default state. They may also include services or interfaces that are not required to fulfil typical functional use cases of a smart meter but still may affect the meter's assets.

The configuration (enabling/disabling) to expose optional services and/or optional interfaces that can affect meter data, shall not be possible by unauthorized personnel. The consumer can in some cases be authorized.

An example of an optional interface/service could be the H1/P1 port that a smart meter can have in certain countries for attaching an extra in-home display. It is recommended this interface is controlled in agreement between the consumer and the utility.

If not used optional services should remain disabled.

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
GEC-3.DN-1	The optional interface or optional exposed service may provide access to the meter's assets. (Go to GEC-3.D.-2)	Security assets or network assets are not affected by the network interface or service (END)	
GEC-3.DN-2	PASS / Recommended	Not recommended unless needed to be referred to a Notified Body	Only authorized personnel shall have the capability to enable/disable the optional interface or optional exposed service, i.e. by the utility or a consumer that is

			uniquely (and perhaps temporarily) empowered by the utility.

Required information:

- Description of each network interface and exposed service (via network interfaces) in factory default state of the equipment, including information if there is an option for an authorized user to enable and disable the network interface or service.
- Description of each security asset that is accessible via network interfaces.
- Description of each privacy asset that is accessible via network interfaces.

- Document HOW… it is possible to at least change the status of the optional network interfaces and exposed optional services (via network interfaces) to enabled and disabled; and
- Document HOW…the configuration of the settings of the optional network interfaces and exposed optional services (via network interfaces) which are part of the factory default state is only possible by authorized users.

11.14.4 [GEC-4] DOCUMENTATION OF EXPOSED NETWORK INTERFACES AND EXPOSED SERVICES VIA NETWORK INTERFACES

Requirement [18031-1] [18031-2]:

The equipment's user documentation shall contain a description of

- all exposed network interfaces; and
- all services exposed via network interfaces,

which are delivered as part of the factory default state

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary: documentation should normally made available to utility customers listing all open interfaces

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
GEC-4.DN-1	Recommended (Go to GEC-4.DN-2	Not recommended) (END)	Most meters will be shipped with some form of exposed network interface which simply needs to be documented in publicly available form
GEC-4.DN-2	Recommended	Not recommended unless needed to be referred to a Notified Body	Open network interfaces need to be publicly known

Required information:

- User documentation of each exposed network interface and exposed service (via network interfaces) in factory default state of the equipment.
- Description of each exposed network interface and exposed service (via network interfaces) in factory default state of the equipment.
- Description of the selected path through the decision tree in Figure 39 for each exposed network interface and exposed service (via network interfaces).

11.14.5 [GEC-5] NO UNNECESSARY EXTERNAL INTERFACES

Requirement [18031-1] [18031-2]:

The equipment shall only expose physical external interfaces if they are necessary for its intended functionality.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

A smart meter will have at least one interface to communicate with a Head End System or a smart meter gateway. Other interfaces, such as a local near-real-time data port and a connection to other meters, are optional. They are implemented or not based on national requirements.

Implementation:

Every meter must have a function to enable and disable the optional interfaces implemented (see also the Minimum-security requirements for AMI components [8]). This function is accessible by the meter operator and/or installer.

Decision tree

Decision nr.	Condition for Yes	Condition for No	Comment
GEC-5.DN-1	Recommended	Not recommended unless needed to be referred to a Notified Body	If a physical interface is implemented but not used, it should be disabled.

Required information:

Description of each physical external interface including:

- [E.Info.GEC-5.PhysicalExternalInterface.Purpose]: The purpose of the interface; and
- [E.Info.SCM-1.PhysicalExternalInterface.Type]: Description of the interface type (e.g. USB-C)
- [E.Info.GEC-5.IntFunc]: Description of the intended functionality of the equipment.

11.14.6 [GEC-6] INPUT VALIDATION

Requirement [18031-1] [18031-2]:

The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or {network}* assets.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Most smart meters do not provide facilities locally to enter data other than PINs and following of menu options which means that input validation is minimal.

For remote access, checks should be in place to:
- sanitize input;
· accept only input that is conform to the used protocols (e.g., as per data model) and limit non-encrypted/authenticated input;
· manufacturer should test its equipment with tools such as fuzzers.

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**
GEC-6.DN-1	Many meters do not allow the user to enter data (END)	If one or more interfaces can receive input has potential impact on security assets and/or privacy assets (Go to GEC-6.DN-2)	
GEC-6.DN-2	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

- Description of each external interface including:
  - Description of any used APIs, protocols, input data types, file formats; and
  - Description how the input for instance via checking syntactic and semantic correctness is validated.
- Description of each security asset that is potentially impacted via external interfaces.
- Description of each privacy asset that is potentially impacted via external interfaces.
- [E.Info.DT.GEC-6]: Description of the selected path through the decision tree in Figure 41 for each of the external interfaces documented in [E.Info.GEC-6.ExternalInterface].

11.14.7 [GEC-7] DOCUMENTATION OF EXTERNAL SENSING CAPABILITIES

Requirement [18031-2]:

All external sensing capabilities of the equipment that are related to the user's or subscriber's privacy shall be documented for the user.

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Assessment decision tree			
Decision nr	**Condition for Yes**	**Condition for No**	**Comments**

GEC-7.DN-1	Recommended (Go to GEC-7.DN-2)	Some meters will have to tamper detection or any other form of sensing (END)	But most modern meters implement some form of tamper detection capabilities which need to be documented for the procuring utility
GEC-7.DN-2	Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

- Description of each non-network external interface of the equipment, that can affect the user's or subscriber's privacy.
- (if non-network external interfaces can affect the user's or subscriber's privacy)
  - [E.Info.GEC-7.UserDoc.NonNetworkInterface]: User documentation describing each non-network external interface of the equipment that can affect the user's or subscriber's privacy.

11.15 [CRY] CRYPTOGRAPHY

11.15.1 [CRY-1] BEST PRACTICE CRYPTOGRAPHY

Requirement [18031-1] [18031-2]:

The equipment shall use best practice for cryptography that is used for the protection of the security assets or {network}* assets, except for:

- cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.

* 18031-2: privacy

Applicable Smart metering	**Yes**	**18031-1**	**Yes**
		18031-2	**Yes**

Commentary:

Assessment decision tree

Decision nr	Condition for Yes	Condition for No	Comments
CRY-1.DN-1	Cryptography is used for a specific security mechanism, where a deviation is identified and justified.	Typically: Cryptography is **not** used for a specific security mechanism, where a deviation is identified and justified. (Go to CRY-1.DN-2)	ACM, AUM, SCM, SUM and SSM state exemption in case the CCK is exclusively used for the exempt use case. The reason for these exemptions can be the required function, the intended operational

			environment or legal requirements. (for details, please check ACM, AUM, SCM, SUM and SSM
CRY-1.DN-2	PASS / Recommended	Not recommended unless needed to be referred to a Notified Body	

Required information:

List of all security assets and privacy assets on the equipment protected by cryptography, including for each cryptography used for cryptographic protection:

- Description of the cryptography used for cryptographic protection, including:
  - description of each cryptographic protection goal; and
  - evidence to justify that the cryptography is best practice for the cryptographic protection goals

ANNEX A: TYPICAL ACTIVITIES IN A CYBERSECURITY RISK MANAGEMENT

1. ESTABLISHING THE SMART METER CONTEXT

The starting point for a cybersecurity risk analysis is to determine the context in which the smart meter shall be used. From this behaviour the threats can be analysed.

The smart meter context for the appropriate management of cybersecurity risks could include:

- the smart meter's intended purpose
- the smart meter's reasonably foreseeable use
- the smart meter's reasonably foreseeable misuse
- the smart meter's essential functionality (see figure 13)
- the smart meter's intended operational environment of use

A generic model of a smart meter that might be used in the analysis is shown in **Fout! Verwijzingsbron niet gevonden.**.

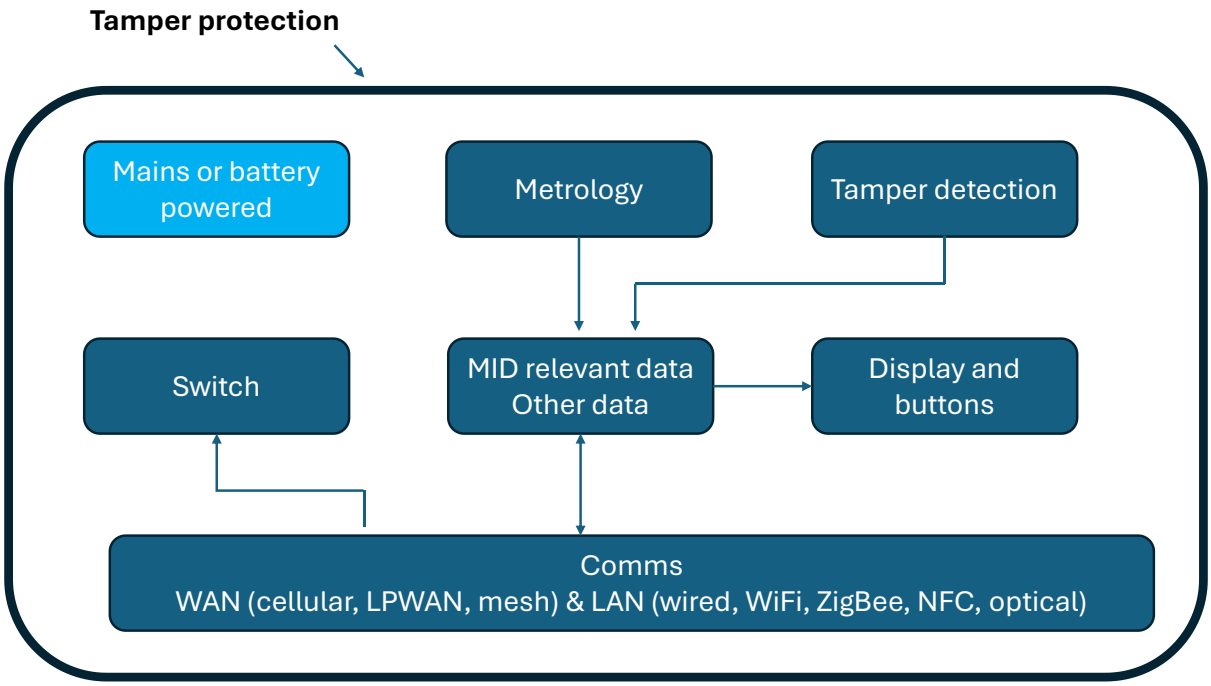

Figure 13: Generic model smart meter

2. PERFORMING AN ASSESSMENT OF THE SMART METER'S CYBERSECURITY RISKS

When the operational context of the smart meter is known the following could be considered:

- an identification of the smart meter's cybersecurity risks including:
  - an identification of the smart meter's cybersecurity assets (see section 9)
  - an identification of smart meter's direct threats within the smart meter's context (see also section Annex A - 50)
- an analysis of the smart meter's cybersecurity risks;
- an evaluation of the smart meter's cybersecurity risks within the intended and reasonably foreseeable use.

The analysis of the smart meter's cybersecurity risks could include a quantitative or qualitative estimation of the cybersecurity risks based on their likelihood of occurrence and magnitude of loss or disruption (see also Annex A - 5.2).

The evaluation of a smart meter's cybersecurity risks within the intended and reasonably foreseeable use identifies:

- demands on the treatment of non-tolerable cybersecurity risks
- justifications for tolerable residual cybersecurity risks.

An evaluation of a smart meter's cybersecurity within the intended and reasonably foreseeable use (context) risks could include:

- comparisons of the cybersecurity risks with criteria for tolerable risks and
- statements for the cybersecurity risks whether they are tolerable or not and
- (for cybersecurity risks that are tolerable) justifications for the tolerability of cybersecurity risks.

3. APPROPRIATE TREATMENT OF THE SMART METER'S CYBERSECURITY RISKS

An appropriate treatment of the product's cybersecurity risks, using the EN18031 standards, should:

- perform an applicability analysis of any security mechanisms described (XXX-1 sections), including justifications in case of non-applicability (exceptions); and
- include the implementation of the security mechanisms to satisfy the sufficiency sections (XXX-2..N) of the applicable security mechanisms; and
- prefer the implementation of security mechanisms over cybersecurity risk sharing for reducing risks within the intended and reasonably foreseeable use, unless an appropriateness criterion for risk sharing applies; and
- only accept residual risks within the intended and reasonably foreseeable use, that are tolerable according to an evaluation of the smart meter's cybersecurity risks.
- Any residual risk should be communicated clearly to the smart meter business user (i.e. utility) enabling the party sharing the risk, if appropriate, to implement necessary countermeasures.

4. OTHER ACTIVITIES

These activities are not in the scope of EU 2022/30 [2] nor this technical report but will be emphasised in detail under EU 2024/2847 [3].
During the lifetime of a smart meter several activities will enhance the overall cybersecurity in the smart meter community. These activities may include:

- Consulting on and communicating the smart meter's cybersecurity risks
- Reviewing and monitoring the management of the smart meter's cybersecurity risks
- Recording the management of the smart meter's cybersecurity risks

5. EXAMPLES OF POSSIBLE THREATS

5.1 INSUFFICIENT AUTHENTICATOR VALIDATION [AUM-3]

When not using all authenticator information as determined under AUM-2:

Local attack (simple hostile attack) from an entity different of a Service Operator, a Consumer or an In-Home Display

- If the smart meter is located in a public area, passwords can be easily guessed, and relevant privacy assets can be exposed (typically not manipulated);
- If the smart meter is in a public area, passwords can be easily guessed and relevant network assets can be manipulated, this may compromise efficient use of network resources.

Remote attack (advanced hostile attack) from an entity different to Meter Operator, HES, NNAP, or Energy Management System

- Symmetric: Security strength decreases below requirement of CCK-1 if authenticator is not fully exploited;
- PKI/Certificate: Security strength decreases below requirement of CCK-1 if authenticator cannot timely renewed or relevant information is not fully exploited (forged authenticators).

5.2 ABSCENCE OF AN UPDATE MECHANISM [SUM-1]

Commonly used security algorithms may be broken. An attacker can attempt to exploit this known vulnerability, potentially affect many smart meters at the same time. It must be foreseen, the lifetime of smart meters exceeds the horizon for predicting the lifetime of security algorithms, due to quantum computation technologies.

The secure update mechanism is a recovery mitigation technique that can be used against all types of threats (S,T,R,I,D,E)

5.3 INSECURE UPDATE MECHANISM [SUM-2]

If a software update mechanism can be tampered (e.g. interception or manipulation of the image file) or the update mechanism allows for updating the smart meter with unverified images, this might directly compromise the protection of the assets. Furthermore, as smart meter's software can be designed in a way that the MID (legal) metrology part is bundled with the software parts containing e.g. security mechanisms that need to be updated, compliance to the MID may be compromised.

6. CONSIDERATIONS WHEN ASSESSING DIFFERENT METER TYPES

Smart meter manufacturers should always analyse risks associated with smart meters being assessed in its actual context. To assist this process, **Fout! Verwijzingsbron niet gevonden.** provides guidance for a comparative assessment, in a relative approach, of the risk level with regards of different assets

- **The Bidirectional capability:** A bidirectional meter, being compromised would allow access to the data and control of the smart meter which could lead to an negative effect on the Network asset and privacy asset.
- **The presence of an actuator:** When the smart meter is equipped with an actuator, the consequences of cybersecurity risks compromising the actuator could be higher comparing to consequences of risks identified for smart meters without actuators.
- **Battery operation:** Smart meters which are main powered could allow continuous access and control of the smart meter which widen the scope and increase the probability of a hostile attack.

Figure 13 : Examples of risks levels according to Smart meter capabilities provides an example of levels of risks according to smart meters capabilities; these levels are provided as examples and might be different according to the context.

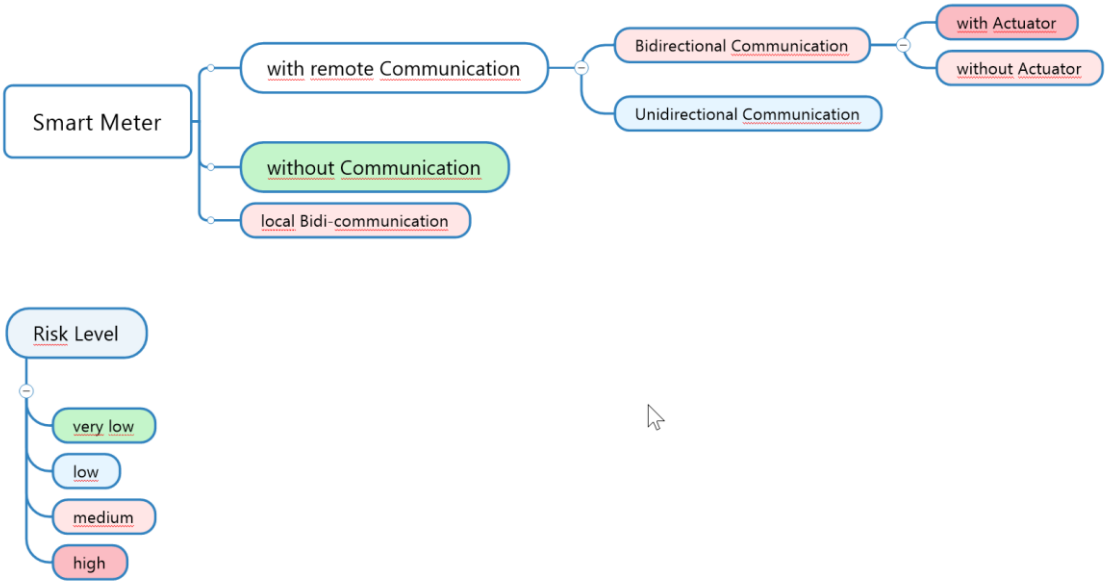

Figure 13 : Examples of risks levels according to Smart meter capabilities

ANNEX B: SAMPLE RESPONSE

Introduction

This section provides a possible template for completing the self-assessment technical file required by EN 18031. Given the similarities between EN18031-1 and –2, a single file should suffice for demonstrating protection of all assets to be protected. The template comprises suggested headings and then descriptions (in italics) of all information to be recorded. Text in other sections, not in italics, represents suggested actual text.

Section 5 contains responses to the specific assessment sections of EN 18031 and, it is suggested, comprises mainly references to information documented in earlier sections. It is complete for the first requirement, [ACM-1]. It should be noted that each section 5 response should, in principle, be completed for every asset to be protected, but in reality, the same protection mechanism, will be used to protect more than one (or even all) assets; therefore, each section 5 assessment is likely to be needed to be completed between one and three times, for each requirement.

1. Intended use

Description of the product's intended use, probably taken from data sheets and user documentation.

2. Architecture

Description of the product's technical architecture to help to put the security controls in later sections in context.

3. Assets to be protected & entities to access

3.1 Security Assets

Descriptions of list of security assets to be protected. These should be grouped into convenient collections that can be treated in an equivalent way in the assessments below.

3.2 Network assets

Descriptions of list of network assets to be protected. These should be grouped into convenient collections that can be treated in an equivalent way in the assessments below.

3.3 Privacy assets

Descriptions of list of privacy assets to be protected. These should be grouped into convenient collections that can be treated in an equivalent way in the assessments below.

3.4 Entities to access assets

Description of every entity (person or system) that is expected to have legitimate access to any of the assets.

4. Security controls deployed

4.1 Access control and authentication [ACM, AUM]

Description of the access control and authentication capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.2 Software updates [SUM]

Description of the software update capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.3 Secure storage mechanisms [SSN]

Description of the secure storage capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.4 Secure communications [SCM]

Description of the secure communications capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.5 Logging [LGM]

Description of the logging capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.6 Deletion [DLM]

Description of the data deletion capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.7 Resilience Mechanism

Description of the resilience capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.8 User notification

Description of the user notification capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.9 Network Monitoring & traffic control Mechanisms [RLM, NMM, TCM]

Description of the monitoring & traffic control capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.10 Key management

Description of the key management capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

4.11 General Equipment Capabilities

Description of the general equipment capabilities of the product and how they would satisfy the underlying requirements for each and every type of asset.

5. 18031-1 & -2 assessments

5.1 [ACM-1] Applicability of access control mechanisms

5.1.1 Implementation categories

There are no implementation categories under this requirement.

5.1.2 Required information

See Security controls deployed: Access control and authentication.

5.1.3 Conceptual assessment

Decision nr	Decision

ACM-1-DN-1	No
ACM-1-DN-2	No
ACM-1-DN-3	No
ACM-1-DN-4	Yes/PASS – see section on Access control & authentication

The verdict of this assessment for all relevant assets is PASS.

5.1.4 Functional completeness assessment

All relevant assets, that are accessible by entities are documented above. Furthermore, thorough penetration testing has tested for other open ports.

The verdict of this assessment for all relevant assets is PASS.

5.1.5 Functional sufficiency assessment

The access control mechanisms are protected as set out under Required information.

The verdict of this assessment for all relevant assets is PASS.

5.2 [ACM-2] Appropriate access control mechanisms

5.1.1 Implementation categories

Continued to [CRY-1]

About ESMIG

ESMIG is the European voice of the providers of smart energy solutions. Our members provide products, information technology and services for multi-commodity metering, display and management of energy consumption and production at consumer premises.
Our activities are focused on systems for smart metering, consumer energy management and safe and secure data transfer.

We work closely with EU policy makers and other EU associations to make Europe's energy and water systems cleaner, reliable, more efficient and the European consumer informed, empowered and engaged.

About AQUA

AQUA is the European trade association representing manufacturers of water and thermal-energy meters. Since 1960, it has promoted innovation, quality, and compliance in metering technologies, working closely with European and international institutions to shape standards and regulations.

By fostering technical expertise and collaboration, AQUA ensures that smart and reliable metering solutions contribute to efficiency, sustainability, and the fair use of vital resources across Europe.

About OMS

The OMS-Group e. V. is a community of interest of associations, presently Figawa and KNX, and enterprises in the area of metering relevant to billing. With the Open Metering System Specification the OMS-Group has developed an open, vendor independent standard for communication interfaces and basic requirements.