Requirements Catalog

End-to-End Security for Smart Metering

Commissioned by Oesterreichs Energie, Brahmsplatz 3, 1041 Wien

By European Network for Cyber Security, P.O. Box 16068, 2500 BB Den Haag, The Netherlands

Version:	2014-1.0
Editor:	Project Group End2End Security Smart Metering
Date:	December 3rd, 2014
Pages:	76

Österreichs E-Wirtschaft

Brahmsplatz 3 Tel +43 1 501 98-0 info@oesterreichsenergie.at
1040 Wien Fax +43 1 501 98-900 www.oesterreichsenergie.at

DVR 0422100, UID ATU37583307, ZVR 064107101; UniCredit Bank Austria AG, SWIFT/BIC: BKAUATWW, IBAN: AT90 1100 0006 4204 1800

Disclaimer

Despite careful checking it is not possible to guarantee the accuracy of contents. With the exception of intent and gross negligence, no liability shall be accepted by the issuer and media proprietor for the contents of this document.

Media proprietor:
Österreichs E-Wirtschaft
1040 Vienna, Brahmsplatz 3
Phone: +43 1 501 98- 0
Fax: +43 1 501 98- 900
info@oesterreichsenergie.at,
www.oesterreichsenergie.at

AUTHORS: PG END2END SECURITY SMART METERING, Oesterreichs Energie

MICHAEL JOHN, European Network for Cyber Security (Project Lead ENCS)

KLAUS KURSAWE, European Network for Cyber Security

CHRISTIANE PETERS, European Network for Cyber Security

WOLFGANG LÖW, EVN (Project Lead PG)

THOMAS AICHHOLZER, KNG-Kärnten Netz GmbH (Deputy Project Lead PG)

JOHANN BERNHARDT, Energie Burgendland AG

CHRISTOPH EBERL, Wiener Netze GmbH

BERNHARD EGGER, Energie AG OÖ Data GmbH

MANFRED FARTHOFER, Salzburg AG

BERTHOLD HABERLER, Linz Strom GmbH

BRIAN KORITTNIG, Energie Steiermark

PHILIPP MEYER, IKB AG

BERNHARD MORSCHER, VKW

FRIEDRICH NEURAUTER, TINETZ AG

RENE SCHMID, STW Klagenfurt

Table of Contents

A. Setup

A.1 Scope

This catalog describes the minimum requirements for end-to-end secured Smart Metering in Austria. These requirements apply to manufacturers during tender processes for the Smart Meter, Gateway, Central System, and their communication links. The application of end-to-end security is in accordance with the recommended measures of the risk analysis presented by E-Control Austria (ECA) on 27 February 2014 [1] for the information systems of the electricity industry.

The term *Smart Metering* is not to be confused with the term *Smart Grid*; the security of control and telecommunication systems for electrical transmission and distribution, for example, is not part of this list of requirements. The underlying end-to-end security architecture for Smart Metering is described in Chapter B.

The measures in this catalog are based on the current state of the art in ICT security, i.e., security of the information and communication technology. The objectives of ICT security are to ensure the authenticity and integrity of information in digital data traffic[1], as well as to keep confidential data secret. The terms *secure*, *secured*, and *security* should be understood in this catalog within the context of ICT security. Other interpretations, such as *security* and *safety* in terms of operational safety or accident prevention, are explicitly marked.

This document describes the requirements of the grid operators for manufacturers and suppliers in the tender process for equipment and systems that are used in Smart Metering with end-to-end security.

A.2 Wording

In order to distinguish between normative and informative content, this requirement catalog follows the terminology of the Technical Guideline TR-03109 (e.g., [2, Section 1.5]) of the German Federal Office for Information Security. Keywords are printed in capital letters in accordance with RFC2119 [3]:

- MUST / SHALL means that the requirement is mandatory.
- MUST NOT / SHALL NOT / SHALL NEITHER... NOR means the absolute prohibition of the specification(s).
- SHOULD describes a strong recommendation. Deviations from the recommended specifications must be justified.
- SHOULD NOT identifies a strong recommendation to exclude a specification. Deviations from the recommended specifications must be justified.
- CAN / MAY means that the specifications are optional.

[1] Digital data traffic should be understood in terms of the end-to-end Smart Metering architecture (see Chapter B).

A.3 Structure of the Requirements

Each requirement is labelled with an identifier (Req._ID) and consists of the following three items:

1. Requirement
2. Recommendation and Implementation Guidance
3. Recommended Assurance Activity

These are defined as follows:

1. Requirement: A *Requirement* describes a requirement or expectation that is mandatory. This tender document uses the term *Requirement* in the sense of a normative, i.e. compulsory, requirement.

2. Recommendation and Implementation Guideline: A *Recommendation* describes possibilities for how a requirement can be implemented. A requirement may be solved equivalently as long as the equivalent method is justified in detailed writing. *Implementation Guidelines* provide examples and explanations of how the requirement should be interpreted.

3. Recommended Assurance Activity: *Recommended Assurance Activities* provide suggestions for how the request should be checked. The objective is to make recommendations for both the test organization and the manufacturer, and to notify the manufacturer of expected test processes. These recommended testing procedures are explained in detail in Appendix B.

A.4 Applicability

Unless stated otherwise the requirements apply to the Meter, the Gateway, and the Central System.

The requirements for the security of the software used in the Central System are to be understood as a basis and must be complemented by the security policy of the system operator.

Requirements with an ID ending in ".M" specifically apply to the Meter.

Requirements with an ID ending in ".GW" specifically apply to the Gateway.

Requirements with an ID ending in ".CS" specifically apply to the Central System.

References to a group are labeled with an asterisk, e.g., SXR_01.*.

A.5 Outline

The requirements in this document fall into the following categories:

- Chapter C concerns requirements for the Smart Metering system. In particular, the following areas are covered:
  - General Security Requirements
    - Future Proof
    - Interface Minimization
    - Cryptographic Algorithms
  - Data Integrity
  - Resilience
  - Access Control
  - Confidentiality
  - Audits and Logs
  - Product Lifecycle and Governance
- Appendix A provides descriptions of selected processes. These serve as examples of how selected security requirements can be implemented in terms of end-to-end security. The processes should not be interpreted in a normative sense but as support for better understanding.
- Appendix B contains a glossary of terms and abbreviations.
- Appendix C contains references to guidelines and related literature.

B. End-to-End Security Architecture

B.1 Smart Meter Architecture

The generic architecture of the Smart Metering system is shown in Figure 1. The number of interfaces is kept to the necessary minimum. The descriptions are based on the specifications in the Austrian legislation “Intelligente Messgeräte-AnforderungsVO” (IMA-VO).

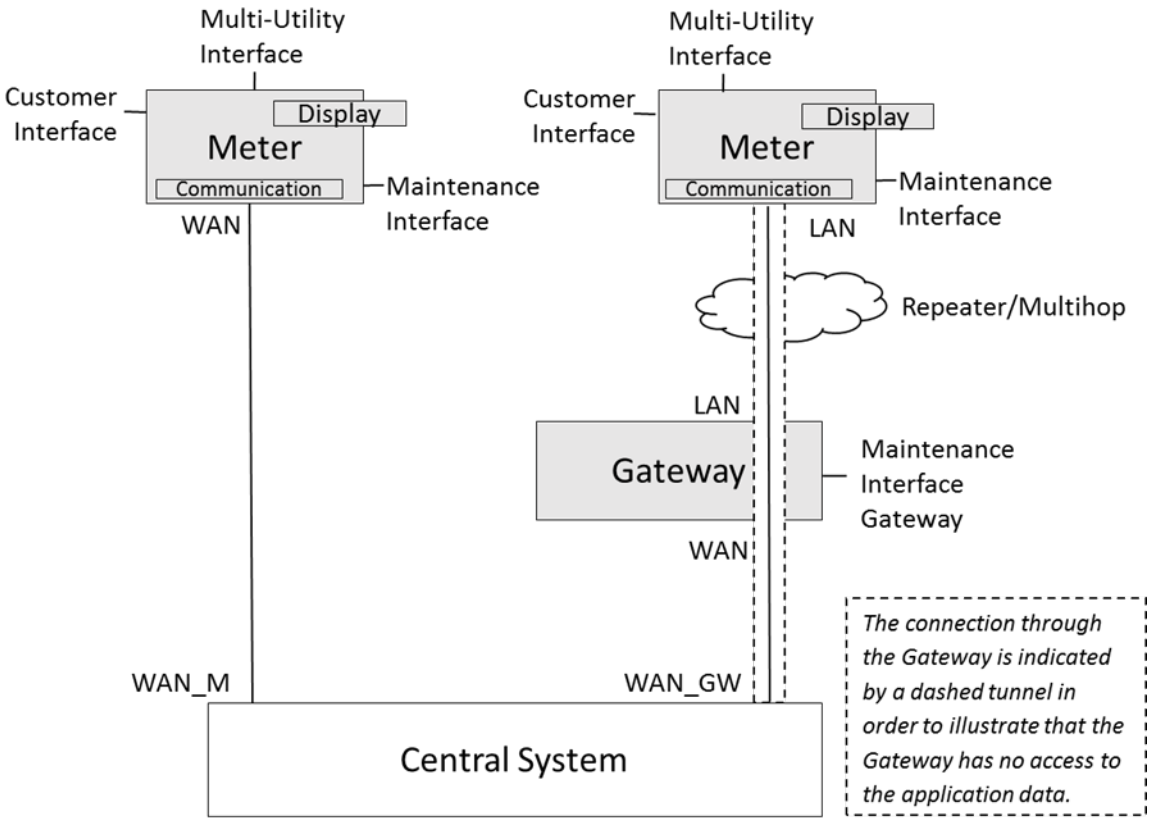

Figure 1: End-to-End Security Architecture for Smart Metering

The end-to-end secure Smart Meter architecture considers two types of meters. The first option considers meters that are connected via a WAN interface to the Central System. The second option considers meters that are connected via a local area network (LAN) to a data concentrator acting as a Gateway to the Central System. All communication from the Central System to individual meters must be end-to-end secured regardless of the chosen solution. Specifically, this means that a data concentrator does not have permission to read information from the Meter, to call functions, or to change settings on the Meter. Communication from the Meter is passed transparently through the Gateway to the Central System.

For this reason, the term *Gateway* is used instead of the term *Data Concentrator*.

In particular it should be noted that the Gateway does not store any cryptographic key material to decrypt, modify, or analyze data that is exchanged between the Meters and the Central System.

In case the Meter and the WAN or LAN communication module are realized by physically separated components, the interfaces between these components must be secured exclusively with cryptographic methods approved in this document.

Meter:

The term *Meter* refers to the electricity meter. Other utility meters such as gas, water, or heat, can be connected to the multi-utility interface of the electricity meter.

Communication:	The Meter supports either a WAN or LAN interface.
Display:	Display refers to the integrated display of the meter. The requirements of the IMA-VO apply.
Customer Interface:	The Customer Interface provides current consumption information to the consumer according to the IMA-VO. The interface must implement exclusively unidirectional communication.
Multi-Utility Interface:	Meters for utilities in the gas, water, and heat domains are connected to the Multi-Utility Interface of the electricity meter. The interface must implement bidirectional communication.
Maintenance Interface:	Access to the electricity meter within the calibration facility, in a test lab, or locally by a technician is realized over the maintenance interface on the electricity meter. The interface must be implemented with bidirectional communication.
LAN Interface:	The LAN Interface of the Meter provides a connection to a Gateway and thus a connection to the Central System. The interface must implement bidirectional communication.
WAN Interface:	The WAN Interface of the Meter provides a direct connection to the Central System. The interface must implement bidirectional communication.

Gateway:

The Gateway is the component within the Smart Metering architecture that provides a transparent communication link between the Central System and the Meter. Transparent is to be interpreted in the context of an end-to-end security architecture.

The term *Gateway* can be seen as the partial functionality of a Data Concentrator reflecting the requirements of end-to-end secured Smart Metering communication.

Maintenance Interface:	The Gateway can be accessed by a technician within a test organization or in the field via the Maintenance Interface. The interface must implement bidirectional communication.
LAN Interface:	The LAN Interface of the Gateway connects the Gateway to the Meters. The interface must implement bidirectional communication.
WAN Interface:	The WAN Interface of the Gateway provides the connection to the Central System. The interface must implement bidirectional communication.

Central System:

The Central System is the central readout and management application that uses and controls the Smart Metering architecture.

WAN_GW Interface:	The WAN_GW Interface of the Central System provides the connections to the Gateways. The interface must implement bidirectional communication.
WAN_M Interface:	The WAN_M Interface of the Central System provides direct connections to the Meters. The interface must implement bidirectional communication.

B.2 Architecture of the Central System

Figure 2 describes the architecture of the Central System. The number of interfaces is kept to the necessary minimum. The arrows indicate whether an interface implements unidirectional or bidirectional communication.

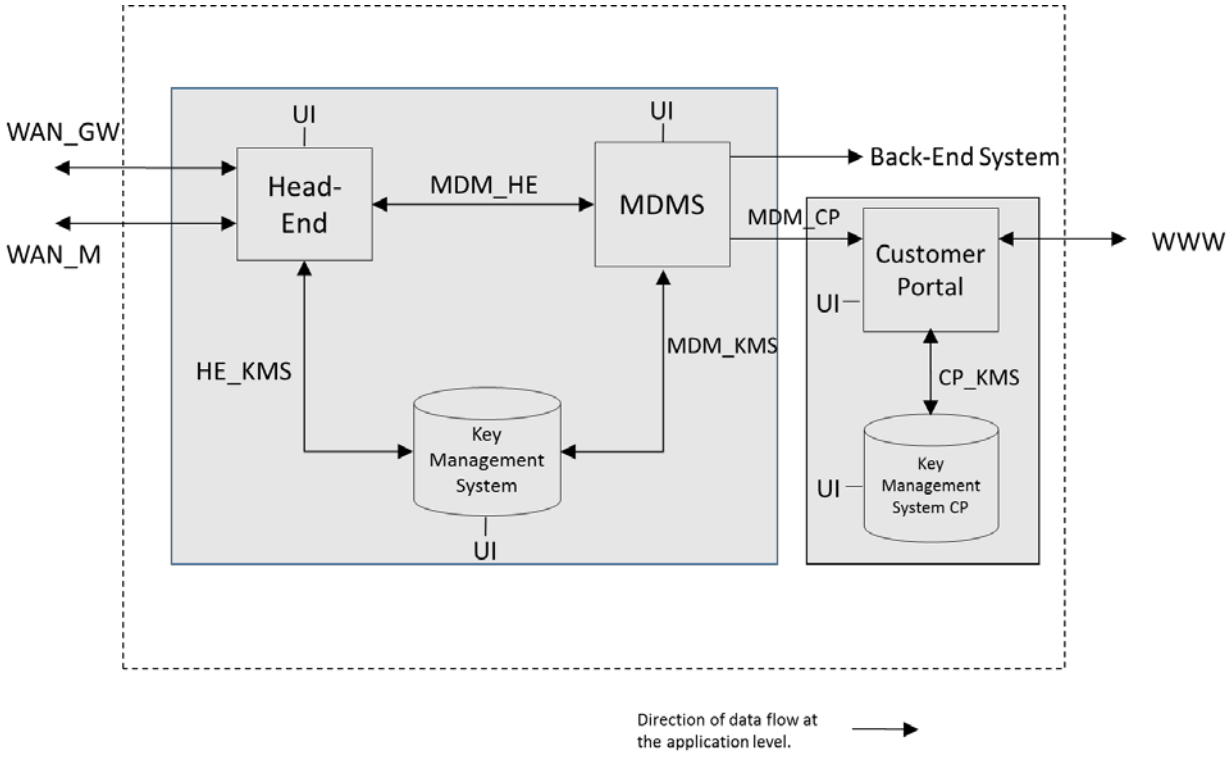

Figure 2: Architecture of the Central System

Head-End System:

The Head-End communicates with the electricity meters and the Gateway, provides data to the Meter Data Management System (MDMS), and forwards messages from the MDMS to the Meters.

User Interface (UI):	Operational and maintenance services of the Head-End System are performed via this interface. The User Interface can also include a remote maintenance interface.
HE_KMS Interface:	This interface allows the Head-End System to communicate with the Key Management System.
MDM_HE Interface:	The Head-End System and the Meter Data Management System communicate using the MDM_HE Interface.

Meter Data Management System:

The Meter Data Management System (MDMS) stores, processes and manages the metering data and makes this data available to the Customer Portal and internal operating processes.

User Interface (UI):	Operational and maintenance services of the Meter Data Management System are performed via this interface. The User Interface can also include a remote maintenance interface.
Back-End System Interface:	This interface connects the Meter Data Management System to the internal corporate network. The communication can be unidirectional; for certain use cases the MDMS only forwards data to enterprise applications, but does not receive information on this interface.
MDM_HE Interface:	The Head-End System and the Meter Data Management System communicate using the MDM_HE Interface.

Key Management System:

The Key Management System (KMS) manages and protects cryptographic keys. The KMS provides secure storage for key material and provides access control for the use of the key material. The Key Management System should consist of independent components, such as a component used by the Head-End and a separate component for the Customer Portal.

User Interface (UI):	Maintenance services of the Key Management System are performed via this interface. It is not recommended that this interface be used for remote maintenance.
HE_KMS Interface:	The Head-End System and the Key Management System communicate using the HE_KMS Interface.
CP_KMS Interface:	Customer Portal and the Key Management System communicate using the CP_KMS Interface.

Customer Portal:

The Customer Portal (CP) in this architecture is to be understood as the customer portal of the grid operator not a third party. The Customer Portal provides access for customers and third parties. The Customer Portal is the only zone with direct access to the public Internet.

User Interface (UI):	Maintenance services of the Customer Portal are performed via this interface. The User Interface can also include a remote maintenance interface.
Web Interface (WWW):	The Web Interface is the connection to the public Internet. Customers and third parties can access the Customer Portal via this interface.
CP_KMS Interface:	The Customer Portal and the Key Management System communicate using the CP_KMS Interface.
MDM_CP Interface:	The Meter Data Management System and the Customer Portal communicate using the MDM_CP Interface. The communication can be unidirectional to protect the MDMS against a corrupted customer portal.

B.3 Roles

This section defines roles and associated privileges for role-based access control roles with respect to the described architecture. The number of roles for the components defined within the architecture is kept to the necessary minimum. The proposed privileges are exemplary. The final privilege settings are to be determined by the grid operator.

B.3.1 Meter Roles

Role	Privileges	Applicability	Meter Interfaces
Calibration and Testing	Tasks of the *Calibration and Testing* role: Provide access for the calibration body, external validation authority, market surveillance, experts or the certification body. Privileges of the *Calibration and Testing* role: Set off-switch, read measurement registers, set tariffs, perform firmware update, access log files, parameterization and configuration.	Internal calibration laboratory of the grid operator, External Validation Authority, Market Surveillance, Certification Body	Maintenance Interface
Maintenance	Tasks of the *Maintenance* role: Configure device locally. Privileges of the *Maintenance* role: Firmware updates, read out registers, configuration (e.g., set time, pair with utility meter (gas, heat, water)), set off-switch.	Handheld Terminal, Service Application	Maintenance Interface
Installation	Tasks of the *Installation* role: Commissioning and installation of the Meter by a technician on site. Privileges of the *Installation* role: Firmware updates, read-out registers, configuration (e.g., set time, pair with	Handheld Terminal, Service Application	Maintenance Interface

	utility meter (gas, heat, water)). This role should be disabled once the Meter has been successfully commissioned. The role may only be reactivated using a secured command.		
Customer	Tasks of the *Customer* role: Unidirectional customer interface to display consumption data. Privileges of the *Customer* role: Read register with the current consumption data. Note: Access to the register values can take place without input by the customer; e.g., it is possible to send consumption data permanently on the customer interface.	Customer Interface	Customer Interface
Display[2]	Tasks of the *Display* role: Allows reading of information that is presented on the display. The authorization of the *Display* role is limited exclusively to the information currently accessible on the Meter display. Examples include current consumption values, firmware version or serial number. The *Display* role may be implemented without user authentication.	Handheld Terminal, External Validation Authority, Market Surveillance	Maintenance Interface

[2] The *Display* role should not be confused with the display of the Meter. The *Display* role has access rights to the same data that is accessible locally via the display of the Meter.

Central System Read-Only	The *Read-Only* role has read access to defined memory areas (register, load profiles, etc.).	Central System	WAN or LAN
Central System Read-Write	The *Read-Write* role has access to all memory areas and functions. This role can change the privileges of all roles.	Central System	WAN or LAN

B.3.2 Gateway Roles

Role	Privileges	Applicability	Gateway Interfaces
Maintenance	Tasks of the *Maintenance* role: Configure device locally. Privileges of the *Maintenance* role: Firmware updates, read out log files, configuration (e.g., set time).	Handheld Terminal, Service Application	Maintenance Interface
Central System Read-Only	The *Read-Only* role has read access to defined memory areas (e.g., configuration files or log files).	Central System	WAN
Central System Read-Write	The *Read-Write* role has access to all memory areas and functions. This role can change the privileges of all roles.	Central System	WAN

B.3.3 Central System Roles

This section defines roles and associated privileges for role-based access control roles with respect to the described architecture. The number of roles for the components defined within the architecture is kept to the necessary minimum. The proposed privileges are exemplary. The final privilege settings are to be determined by the grid operator.

Head-End System

Role	Privileges	Applicability	Central System Interfaces
Head-End Maintenance	The *Head-End Maintenance* role can configure the Head-End.	Head-End	User Interface
MDMS	The MDMS uses the *MDMS* role for user authentication at the Head-End.	Head-End	MDM_HE
Operator Read-Only	The user with the *Operator Read-Only* role can read out data from connected Meters or Gateways.	Head-End	User Interface
Operator Read-Write	The user with the *Operator Read-Write* role can read and write data from connected Meters or Gateways.	Head-End	User Interface

MDM System

Role	Privileges	Applicability	Central System Interfaces
Head-End	The Head-End uses the *Head-End* role for user authentication at the MDMS.	MDMS	MDM_HE
MDMS Maintenance	The *MDMS Maintenance* role can configure the MDMS. In particular, this role can define which information may be forwarded to the Customer Portal and to the Back-End System.	MDMS	User Interface
Operator Read-Only	The user with the *Operator Read-Only* role can read out data from the MDMS.	MDMS	User Interface

Operator Read-Write	The user with the *Operator Read-Write* role can read and write data in the MDMS.	MDMS	User Interface

Customer Portal

Role	Privileges	Applicability	Central System Interfaces
Customer	The *Customer* role can access one or more records in the Customer Portal. Each customer and third party is assigned an individual role.	Customer Portal	Internet
Customer Portal Maintenance	The *Customer Portal Maintenance* role can configure the Customer Portal.	Customer Portal	User Interface
MDMS_CP	The MDMS uses the *MDMS_CP* role for user authentication at the Customer Portal.	Customer Portal	MDM_CP

Key Management System

Role	Privileges	Applicability	Central System Interfaces
KMS Maintenance	The *KMS Maintenance* role can configure the Key Management System.	Key Management System	User Interface
Customer Portal	The Customer Portal uses the *Customer Portal* role for user authentication at the KMS.	Key Management System	CP_KMS
Head-End	The Head-End uses the role of *Customer Portal* for user authentication at the KMS.	Key Management System	HE_KMS

B.4 Security Events

Each security event should, where possible, log the time, user or system identification (ID), interfaces, as well as the result of the event.

The Meter and Gateway should support at least the following event types:

Event	Device
Logging of a successful or failed user authentication for a particular role.	Meter and Gateway
Firmware Updates • Logging of successful firmware updates. • Logging of failed firmware updates due to invalid digital signatures. • Distinction between receiving a firmware image and the activation of a firmware update.	Meter and Gateway
Setting the system time.	Meter and Gateway
Events that are registered by tamper-detection sensors. These include the opening of device covers, for example.	Meter and Gateway
Startup of the device (boot process).	Meter and Gateway
Performing a reset or reboot of the device.	Meter and Gateway
Reset of error or alarm registers or the associated log files.	Meter and Gateway
Logging of device errors. See Requirements SRR_02.*.	Meter and Gateway
Reconfiguration of cryptographic parameters. For example, • Update of cryptographic key material for a selected role. • Change of access rights for a selected role. • Reset of random number generator (seed).	Meter and Gateway
Off-switch: on/off.	Meter
Events related to utility meters: • Device pairing of utility meter and electricity meter • Update of cryptographic key material for the utility meter	Meter
Modification of the parameters of the load limitation	Meter
Load limitation	Meter

C. Secure Meter Communication

C.1 General Security Requirements

C.1.1 Future Proof

Req._ID	
SFR_01.M	**Requirement**
	The Meter SHALL have sufficient memory (volatile and non-volatile) and computational power reserves to allow updates of security functionality. The updatability MUST be ensured throughout the product lifecycle.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that sufficient reserves are available to update security functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. This specifically includes cryptographic algorithms and communication protocols. Please refer to SPR_01. 3. The Meter SHOULD have storage reserved solely for updating security functionality.
	Recommended Assurance Activity
	1. It is recommended to analyze the design documentation provided by the manufacturer.
SFR_01.GW	Requirement
	The Gateway SHALL have sufficient memory (volatile and non-volatile) and computational power reserves to allow updates of security functionality. The updatability MUST be ensured throughout the product lifecycle.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that sufficient reserves are available to update security functionality. Design evidence

	SHOULD be at a level of detail that enables easy verification. 2. This includes in particular cryptographic algorithms and communication protocols. Please refer to SPR_01. 3. The Gateway SHOULD have storage reserved solely for updating security functionality.
	Recommended Assurance Activity
	1. It is recommended to analyze the design documentation provided by the manufacturer.
SFR_01.CS	**Requirement**
	The Central System MUST support updates of security functionality. The updatability MUST be ensured throughout the product lifecycle.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that sufficient reserves are available to update security functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. This specifically includes cryptographic algorithms and communication protocols. Please refer to SPR_01.
	Recommended Assurance Activity
	1. It is recommended to analyze the design documentation provided by the manufacturer.
SFR_02.M	**Requirement**
	Cryptographic algorithms and communication protocols of the Meter SHALL be updated by remote firmware updates.
	Recommendation and Implementation Guidance
	1. See also Requirement SPR_01. 2. Remote updates of the Meter SHOULD be carried out by remote

	firmware updates or remote patching.
	Recommended Assurance Activity
	1. It is recommended to analyze the design documentation provided by the manufacturer. 2. It is recommended to carry out a fuzzing test of the firmware update functions.
SFR_02.GW	**Requirement**
	Cryptographic algorithms and communication protocols of the Gateway SHALL be updated by remote firmware updates.
	Recommendation and Implementation Guidance
	1. See also Requirement SPR_01. 2. Remote updates of the Gateway SHOULD be carried out by remote firmware updates or remote patching.
	Recommended Assurance Activity
	1. It is recommended to analyze the design documentation provided by the manufacturer. 2. It is recommended to carry out a fuzzing test of the firmware update functions.
SFR_03.M	**Requirement**
	The Meter SHALL support the capability to remotely update or revoke privileges of the respective roles as well as the cryptographic keys.
	Recommendation and Implementation Guidance
	1. See Section C.4 for requirements for role-based access control. 2. An authenticated key exchange protocol SHOULD be used for updating cryptographic keys to protect their integrity. 3. When deploying public key cryptography the device SHOULD be capable of generating new key pairs together with a certificate signing

	request. When deploying public key cryptography the Meter SHOULD be capable of importing new certificates.
	Recommended Assurance Activity
	1. This requirement is verified by a functional security test.
SFR_03.GW	**Requirement**
	The Gateway SHALL support the capability to remotely update or revoke privileges of the respective roles as well as the cryptographic keys.
	Recommendation and Implementation Guidance
	1. See Section C.4 for requirements for role-based access control. 2. An authenticated key exchange protocol SHOULD be used for updating cryptographic keys to protect their integrity. 3. When deploying public-key cryptography the device SHOULD be capable of generating new key pairs together with a certificate signing request. When deploying public-key cryptography the Gateway SHOULD be capable of importing new certificates.
	Recommended Assurance Activity
	1. This requirement is verified by a functional security test.
SFR_03.CS	**Requirement**
	The Central System SHALL support the capability to update or revoke privileges of the respective roles as well as the cryptographic keys.
	Recommendation and Implementation Guidance
	1. See Section C.4 for requirements for role-based access control. 2. See SIR_01.CS for the protection of the integrity of cryptographic key material.
	Recommended Assurance Activity

	1. This requirement is verified by a functional security test.

C.1.2 Interface Minimization

Req._ID	
SMR_01	**Requirement**
	Each interface SHALL support only the data types and protocols needed to meet the functional requirements.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that only the described functionality is implemented. Design evidence SHOULD be at a level of detail that enables easy verification. 2. The manufacturer SHOULD provide a complete list of supported data types and supported communication protocols. 3. Examples of redundant functions are: debugging or analysis functions used during the development process, such as the webserver of a Gateway used during the development phase as a debugging tool; or specialized keystroke combinations to enter an engineering menu of a Meter, allowing security-relevant modifications.
	Recommended Assurance Activity
	1. Carrying out a penetration test can provide further assurance that this specification is adequately implemented.
SMR_02	**Requirement**
	Disabled or unused functionality SHALL NOT compromise security.
	Recommendation and Implementation Guidance

	1. The manufacturer SHOULD provide design evidence that any required additional functionality does not compromise security; additional functionality is functionality that goes beyond the operational tasks and regular communication between the Meter and Central System. Design evidence SHOULD be at a level of detail that enables easy verification. 2. Functionality that is disabled and will never be needed on the device SHOULD be completely removed. 3. Disabled functionality should be addressable neither via undocumented functions nor through undefined or faulty operating states. o Examples of unused functionality are routines contained in the firmware that are not used in normal operational mode. o Further examples are testing and debugging functions used for initialization during the production process.
	Recommended Assurance Activity
	1. Carrying out a penetration test can provide further assurance that this specification is adequately implemented. 2. Requesting proof of a code review from the manufacturer is recommended.

C.1.3 Cryptographic Algorithms

Req._ID	
SPR_01	**Requirement**
	1. The manufacturer SHALL follow the most recent version of the following guidelines when employing cryptographic primitives and key lengths: • NIST SP 800-57 Part 1 Rev 3, Recommendation for Key Management: Application-Specific Key Management Guidance. [4] • BSI TR-03116, Part 3, “Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme“ [5]. Only Chapter 2 “Kryptographische Algorithmen” and Chapter 4.1 “Cipher Suites und

	Kurvenparameter" in the referenced 2014 version [5] are applicable.[3] 2. The manufacturer SHALL NEITHER employ proprietary cryptographic functions NOR modify the cryptographic primitives mentioned in item 1.
	Recommendation and Implementation Guidance
	1. TR-03116-3 is updated annually to be in accordance with technical and scientific progress. It is also recommended to pay attention to updates of NIST SP 800-57 Part 1. 2. ENISA's *Algorithms, Key Sizes and Parameters Report* [6] provides details on the state of the art in cryptography. 3. The following algorithms and procedures are recommended. Naming conventions follow [5] and [4]: • Symmetric Encryption with authentication: AES-CBC-CMAC, AES-CCM, AES-GCM. Appendix of NIST SP 800-38D [7] SHOULD be considered regarding implementation of AES-GCM. • Cryptographic Hash Functions: SHA2 Family. • Authenticated Key Exchange using Elliptic Curve Diffie-Hellman (ECKA-DH). • Authenticated Key Transport using Elliptic Curve El-Gamal (ECKA-EG). • Digital Signatures: ECDSA. • Elliptic Curve (EC) based methods SHOULD use elliptic curves over prime fields of a minimum of 256 bits, e.g., the NIST curves (P-256 or higher security levels) in IETF RFC 5114 [8] or the ECC Brainpool curves [9]. 4. Communication on the WAN interface between the Gateway and the Central System SHOULD use the TLS protocol, Version 1.2 [10] (or higher). The following TLS Cipher Suites [11] should be used: • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

[3] Note that in particular, the BSI requirements to secure the HAN using TLS are not part of the metering architecture described in this document.

	• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 5. The manufacturer SHOULD provide design evidence at a level of detail that enables easy verification. 6. See SFR_01.* regarding necessary storage for updating cryptographic functions.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SPR_02	**Requirement**
	All security-relevant random values SHALL be generated by cryptographic random number generators in accordance with AIS 20 [15], AIS 31 [16] or equivalent.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification. 2. Security-relevant random values are used for the generation of digital signatures, cryptographic keys, or authentication protocols, for example. 3. FIPS 186-2 [12] and FIPS 140-2 (Annex C) [14] are considered equivalent to the mentioned guidelines.
	Recommended Assurance Activity
	1. Carrying out a penetration test can provide further assurance that this specification is adequately implemented. 2. Analysis of the design documentation provided by the manufacturer is recommended.

	Requirement
SPR_03	The implementations of cryptographic algorithms SHALL be tested under the NIST Cryptographic Algorithm Validation Program (CAVP) [17] or an equivalent test and certification scheme.
	Recommendation and Implementation Guidance
	1. An Austrian certification body to be named by the regulator can issue an equivalent test and certification scheme. 2. The manufacturer SHOULD provide design evidence that this requirement is addressed. This can be achieved by providing the certificate of the CAVP module validation or the equivalent.
	Recommended Assurance Activity
	1. Verification of the requirement is made by a module validation of the implemented functions or assessment of the conducted module validation.

C.2 Data Integrity

Req._ID	
SIR_01.M	**Requirement**
	The Meter SHALL verify the authenticity and integrity of all data received on the following interfaces: • Multi-Utility Interface between the electricity meter and other utility meters. • Maintenance Interface, • LAN between the electricity meter and Central System, • WAN between the electricity meter and Central System. Both authenticity of the source (sender) and authenticity of the received message SHALL be verified. The message SHALL be dropped if the integrity of the sender or the data

	cannot be verified.
	Recommendation and Implementation Guidance
	1. Messages SHOULD be authenticated by attaching a message authentication code (MAC). 2. The authenticity of the sender can be verified by checking the attached valid digital signature. 3. Requirement SPR_01 lists the allowed cryptographic algorithms. 4. In the context of the end-to-end security architecture this requirement concerns the Application Layer (OSI Layers 5-7).
	Recommended Assurance Activity
	1. The manufacturer SHOULD provide design evidence of the implementation of the required functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. Carrying out a penetration test can provide further assurance that this specification is adequately implemented.
SIR_01.GW	**Requirement**
	The Gateway SHALL verify the authenticity and integrity of data received on the following interfaces: • Maintenance Interface, • WAN Interface to the Central System in case the interface is used for maintenance purposes. Both authenticity of the source (sender) and authenticity of the received message SHALL be verified. The message SHALL be dropped if the integrity of the sender or the data cannot be verified.
	Recommendation and Implementation Guidance
	1. Messages SHOULD be authenticated by attaching a message authentication code (MAC). 2. The authenticity of the sender can be verified by checking an attached

	valid digital signature. 3. Requirement SPR_01 lists the allowed cryptographic algorithms. 4. In the context of the end-to-end security architecture this requirement concerns the Application Layer (OSI Layers 5-7).
	Recommended Assurance Activity
	1. The manufacturer SHOULD provide design evidence of the implementation of the required functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. Carrying out a penetration test can provide further assurance that this specification is adequately implemented.
SIR_01.CS	**Requirement**
	The authenticity and integrity of data received on all interfaces and data traversing between the implemented zones in the Central System SHALL be verified. Both authenticity of the source (sender) and authenticity of the received message SHALL be verified. The message SHALL be dropped if the integrity of the sender or the data cannot be verified.
	Recommendation and Implementation Guidance
	1. Requirement SRR_04.CS provides details on zoning in the Central System. 2. Messages SHOULD be authenticated by attaching a message authentication code (MAC). 3. The authenticity of the sender can be verified by checking an attached valid digital signature. 4. Requirement SPR_01 lists the allowed cryptographic algorithms. 5. In the context of the end-to-end security architecture this requirement concerns the Application Layer (OSI Layers 5-7).
	Recommended Assurance Activity
	1. The manufacturer SHOULD provide design evidence of the implementation of the required functionality. Design evidence SHOULD

	be at a level of detail that enables easy verification. 2. Carrying out a penetration test can provide further assurance that this specification is adequately implemented.
SIR_02.M	**Requirement**
	The Meter SHALL verify the validity of all data packets and the format of data received on the following interfaces: • Multi-Utility Interface between the electricity meter and other utility meters, • Maintenance Interface, • LAN between the electricity meter and Central System, • WAN between the electricity meter and Central System.
	Recommendation and Implementation Guidance
	1. Both the device design and implementation SHOULD ensure that the correct functioning of the Meter is not negatively affected by corrupt or deliberately malformed packets. 2. The requirement is valid for all layers in the OSI model.
	Recommended Assurance Activity
	1. It is recommended to carry out fuzzing tests on the described interfaces. 2. The manufacturer should document performed security tests in a sufficient level of detail to allow for validation. The manufacturer should add the performed security tests to the product documentation.
SIR_02.GW	**Requirement**
	The Gateway SHALL verify the validity of all data packets and the format of data received on the following interfaces: • Maintenance Interface, • WAN Interface to the Central System in case the interface is used for maintenance purposes.
	Recommendation and Implementation Guidance

	1. Both device design and implementation SHOULD ensure that the correct functioning of the Gateway is not negatively affected by corrupt or deliberately malformed packets. 2. The requirement is valid for all layers in the OSI model.
	Recommended Assurance Activity
	1. It is recommended to carry out fuzzing tests on the described interfaces. 2. The manufacturer should document performed security tests with a sufficient level of detail to allow for validation. The manufacturer should add the performed security tests to the product documentation.
SIR_02.CS	**Requirement**
	The Central System SHALL verify the validity of all data packets and the format of data received on all interfaces as well as for the data exchange between implemented zones.
	Recommendation and Implementation Guidance
	1. Requirement SRR_04.CS provides details on zoning in the Central System. 2. The requirement concerns both the external as well as internal interfaces (zone-to-zone). 3. Both the device design and implementation SHOULD ensure that the Central System is not negatively affected by corrupt or deliberately malformed packets. 4. SQL Sanitization is a countermeasure for SQL injection; it is an example of data validation in the Central System. Further examples of data validation on web servers are described in the ÖNORM A 7700 [18] and in the OWASP Chapter "*Data Validation"* [19]. 5. The requirement is valid for all layers in the OSI model.
	Recommended Assurance Activity
	1. It is recommended to carry out fuzzing tests on the described interfaces. 2. The manufacturer should document performed security tests with a sufficient level of detail to allow for validation. The manufacturer should add the performed security tests to the product documentation.

	Requirement
	The Meter SHALL verify the integrity of firmware images before they are applied. • The manufacturer SHALL digitally sign the firmware update. • Firmware updates without a valid digital signature MUST be dropped. • The firmware update MUST be dropped if its version number is lower than the version number of the installed firmware. • The Meter SHALL support the downgrade to an older firmware version if necessary for operations. Any such downgrade SHALL be imported under a new version number. • Data on the Meter (e.g., stored meter data or log entries) SHALL NOT be altered or deleted by a firmware update. • Necessary changes of the configuration of deployed functions SHALL be carried out automatically during the update process.
	Recommendation and Implementation Guidance
SIR_03.M	1. The ECDSA algorithm with an allowed key strength SHOULD be used to generate a digital signature. See SPR_01. 2. The public key for the validation of the digital signature SHOULD be installed on the Meter during the manufacturing process. See Example Processes in Appendix A. 3. Digitally signed firmware updates can be sent out as a broadcast/multicast. See Example Processes in Appendix A. 4. Adequate release management of the firmware build at the manufacturer SHOULD ensure the digital signature of the image is trustworthy.
	Recommended Assurance Activity
	1. The functional requirement should be verified by testing the implemented firmware update functions. 2. With respect to the requirements for processes, security audits can be performed as part of acceptance or functional tests. 3. Security audits of development and firmware release processes can be conducted as part of a general security audit, e.g., ISO 27001. 4. Carrying out a fuzzing test to verify that the firmware update functions are adequately implemented.

	Requirement
	The Gateway SHALL verify the integrity of firmware images before they are applied. • The manufacturer SHALL digitally sign the firmware update. • Firmware updates without a valid digital signature MUST be dropped. • The firmware update MUST be dropped if its version number is lower than the version number of the installed firmware. • The Gateway SHALL support the downgrade to an older firmware version if necessary for operations. Any such downgrade SHALL be imported under a new version number. • Data on the Gateway (e.g., log entries) SHALL NOT be altered or deleted by a firmware update. Necessary changes of the configuration of deployed functions SHALL be carried out automatically during the update process.
	Recommendation and Implementation Guidance
SIR_03.GW	1. The ECDSA algorithm with an allowed key strength SHOULD be used to generate a digital signature. See SPR_01. 2. The public key for the validation of the digital signature SHOULD be installed on the Gateway during the manufacturing process. See Example Processes in Appendix A. 3. Digitally signed firmware updates can be sent out as a broadcast/multicast. See Example Processes in Appendix A. 4. Adequate release management of the firmware build at the manufacturer SHOULD ensure the digital signature of the image is trustworthy.
	Recommended Assurance Activity
	1. The functional requirement should be verified by testing the implemented firmware update functions. 2. With respect to the requirements for processes, security audits can be performed as part of acceptance or functional tests. 3. Security audits of development and firmware release processes can be conducted as part of a general security audit, e.g., ISO27001. 4. It is recommended to carry out a fuzzing test to verify that the firmware update functions are adequately implemented.

SIR_03.CS	Requirement
	The Central System SHALL verify the integrity of software images before they are applied. • The manufacturer SHALL digitally sign the software update. • Software updates without a valid digital signature MUST be dropped. • The Central System SHALL support the downgrade to an older firmware version if necessary for operations. Any such downgrade SHALL be imported under a new version number.
	Recommendation and Implementation Guidance
	1. The ECDSA algorithm with an allowed key strength SHOULD be used to generate a digital signature. See SPR_01. 2. Adequate release management of the software build at the manufacturer SHOULD ensure the digital signature of the update is trustworthy.
	Recommended Assurance Activity
	1. The functional requirement should be verified by testing the implemented software update functions. 2. With respect to the requirements for processes, security audits can be performed as part of acceptance or functional tests. 3. Security audits of development and update release processes can be conducted as part of a general security audit, e.g., ISO27001.
SIR_04.M	**Requirement**
	The Meter SHALL be able to detect replay attacks on the following interfaces: • Multi-Utility Interface between the electricity meter and other utility meters, • Maintenance interface, • LAN between the electricity meter and Central System, • WAN between the electricity meter and Central System. The Meter MUST drop replayed messages.

	Recommendation and Implementation Guidance
	1. To prevent replay attacks all messages SHOULD be secured in one of the following possible ways: • A sequence number (counter). • An authenticated nonce. It is essential that the nonce is authenticated using a MAC algorithm. • Authenticated encryption using a method such as AES-CBC-CMAC, AES-CCM, or AES-GCM.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SIR_04.GW	**Requirement**
	The Gateway SHALL be able to detect replay attacks on the following interfaces: • WAN Interface to the Central System in case the interface is used for maintenance purposes, • Maintenance Interface. The Gateway MUST drop replayed messages.
	Recommendation and Implementation Guidance
	1. To prevent replay attacks all messages SHOULD be secured in one of the following possible ways: • A sequence number (counter). • An authenticated nonce. It is essential that the nonce is authenticated using a MAC algorithm. • Authenticated encryption using a method such as AES-CBC-CMAC, AES-CCM, or AES-GCM.
	Recommended Assurance Activity

	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SIR_04.CS	**Requirement**
	The Central System SHALL be able to detect replay attacks on all external and internal interfaces and between implemented zones (zone-to-zone). The Central System MUST drop replayed messages.
	Recommendation and Implementation Guidance
	1. To prevent replay attacks all messages SHOULD be secured in one of the following possible ways: • A sequence number (counter). • An authenticated nonce. It is essential that the nonce is authenticated using a MAC algorithm. • Authenticated encryption using a method such as AES-CBC-CMAC, AES-CCM, or AES-GCM. 2. Use of TLS or a VPN can provide this functionality. See also SPR_01.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented. 2. Analysis of the design documentation provided by the manufacturer is recommended.

C.3 Resilience

Req._ID	
SRR_01.M	**Requirement**
	Separate functional blocks of the Meter MUST NOT negatively affect each

	other. Non-security functionality SHALL NOT affect the overall system security. The manufacturer SHALL provide design evidence of compartmentalization of security and non-security functions and blocks.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide documentation that the Meter is sufficiently separated into functional blocks. 2. An example for the separation of functional blocks of the Meter is the separation of metrology and communication. Communication problems SHOULD have no negative impact on the metrology.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that the requirement was adequately implemented. 2. Carrying out a fuzzing test is recommended to provide evidence that functional blocks of the Meter do not affect each other.
SRR_01.GW	**Requirement**
	Separate functional blocks of the Gateway MUST NOT negatively affect each other. Non-security functionality SHALL NOT affect the overall system security. The manufacturer SHALL provide design evidence of compartmentalization of security and non-security functions and blocks.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide documentation that the Gateway is sufficiently separated into functional blocks. 2. An example for the separation of functional blocks of the Gateway is memory protection of separate processes (e.g., routing or remote access).
	Recommended Assurance Activity

	1. Carrying out a penetration test is recommended to provide further assurance that the requirement was adequately implemented. 2. Carrying out a fuzzing test is recommended to provide evidence that functional blocks of the Gateway do not affect each other.
SRR_02.M	Requirement
	The Meter SHALL be *fail-secure*. • Confidentiality and integrity of the data and device functions of the Meter MUST still be guaranteed during failures. • The Meter SHALL maintain a secure state even if failures or unforeseen operational states, caused deliberately or unintentionally, occur. The manufacturer SHALL provide design documentation listing relevant failure types and their respective countermeasures.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that the Meter is fail-secure. 2. This can be addressed by implementing a watchdog functionality that allows the Meter to maintain a secured operational state in the event of a failure. 3. Examples for relevant failures of the Meter are: • Voltage drop; • Integrity errors, e.g., of settings, configurations or log files; • Failures during self-tests of the Meter; • Failures during execution of cryptographic functions; • Failures during validation of login credentials; • Failures when entering data (wrong data format, wrong data length, invalid commands, etc.); • Failures when using the local buttons (pressing buttons too fast or at the same time). 4. The manufacturer SHOULD provide design evidence for which relevant failures are covered and how these were tested. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity

	1. Carrying out a penetration test is recommended to provide further assurance of the design robustness. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SRR_02.GW	**Requirement**
	The Gateway SHALL be *fail-secure*. • Confidentiality and integrity of data and device functions of the Gateway MUST still be guaranteed during failures. • The Gateway SHALL maintain a secure state even if failures or unforeseen operational states, caused deliberately or unintentionally, occur. The manufacturer SHALL provide design documentation listing relevant failure types and their respective countermeasures.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that the Gateway is fail-secure. 2. This can be addressed by implementing a watchdog functionality that allows the Gateway to maintain a secured operational state in case of a failure. 3. Examples for relevant failures of the Meter are: • Voltage drop; • Integrity errors, e.g., of settings, configurations or log files; • Failures during self-tests of the Gateway. • Failures during execution of cryptographic functions; • Failures during validation of login credentials; • Failures when entering data (wrong data format, wrong data length, invalid commands, etc.); • Failures when using the local buttons (pressing buttons too fast or at the same time). 4. The manufacturer SHOULD provide design evidence for which relevant failures are covered and how these were tested. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity

	1. Carrying out a penetration test is recommended to provide further assurance of the design robustness. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SRR_02.CS	**Requirement**
	The Central System SHALL be *fail-secure*. • Confidentiality and integrity of the data and device functions from components of the Central System MUST still be guaranteed during failures. • The Central System SHALL maintain a secure state even if failures or unforeseen operational states, caused deliberately or unintentionally, occur. The manufacturer SHALL provide design documentation listing relevant failure types and their respective countermeasures.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that the Central System is fail-secure. 2. Examples for relevant failures are: • Integrity errors, e.g., of settings, configurations or log files; • Failures during execution of cryptographic functions; • Failures during validation of login credentials; • Failures when entering data (wrong data format, wrong data length, invalid commands, etc.). 3. The manufacturer SHOULD provide design evidence for which relevant failures are covered and how these were tested. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance of the design robustness. 2. Analysis of the design documentation provided by the manufacturer is recommended.

SRR_03.M	**Requirement**
	Physical manipulations of the Meter SHALL be recognizable. • The meter case SHALL provide sufficient protection against physical manipulations. • The Meter case SHALL be sealed where possible. • Additionally, the opening of the terminal cover and separately the case of the Meter SHALL be recognized using suitable means such as contacts or sensors. Any opening of the terminal cover or case SHALL generate an event in the security log. • If the Meter possesses any removable parts, the removal of such a part SHALL generate an event in the security log. An independent penetration test of the physical security MUST be conducted.
	Recommendation and Implementation Guidance
	1. The security log is defined in Requirement SLR_01.M. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification. 3. It SHOULD be possible to seal the meter case and the terminal cover. 4. The penetration tests SHOULD be conducted over a period of at least 2 weeks by an experienced tester.
	Recommended Assurance Activity
	1. Analysis of the vulnerabilities reported in the penetration test is recommended.
SRR_03.GW	**Requirement**
	Physical manipulations of the Gateway SHALL be recognizable. • The case SHALL provide sufficient protection against physical manipulations. • If the Gateway possesses any removable parts, the removal of such a part SHALL generate an event in the security log.

	Recommendation and Implementation Guidance
	1. The security log is defined in Requirement SLR_01.GW. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SRR_04.CS	**Requirement**
	1. The Central System SHALL support separation into at least the following four zones: a. Head-End System b. Key-Management System (KMS) c. Meter-Data Management System (MDMS) d. Customer Portal 2. It MUST be possible to limit communication between the zones.
	Recommendation and Implementation Guidance
	1. Generic examples for mechanisms to separate zones are: • Firewalls: A firewall controls the information flow between two components. Note that wrong configuration of firewalls can be disastrous: the configuration flexibility provided by a firewall can easily lead to misconfigurations, making way for an attacker. • Network gateways[4]: A gateway regulates which components may communicate with each other. • Data diodes: A data diode enforces traffic flowing only in one direction. The receiving end has no permissions to send data to the sender and thus cannot be abused as entry point for an attack. Data diodes are more secure but also much less flexible than firewalls or gateways.

[4] Here the term “gateway” should be understood as a classical means to connect computer networks.

	• Micro kernels: a micro kernel or hypervisor enables the separation of processes and thus provides the possibility to enable zoning without hardware separation. 2. If possible, the separation functionality should be implemented as an individual component.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SRR_05.CS	**Requirement**
	It SHALL be possible to store cryptographic keys in a secured environment of a Key Management System. This secured environment SHALL at least comply with Level 3 in FIPS 140-2 [12].
	Recommendation and Implementation Guidance
	1. Usage of cryptographic functions and keys is detailed in SPR_01. 2. Critical cryptographic keys SHOULD never exist outside this secured environment. 3. It SHOULD be possible to generate new cryptographic keys within the secured environment. 4. The interface connecting the secured environment and the Key Management System SHOULD use an open interface standard, such as PKCS #11 [20]. 5. All interfaces of the secured environment SHOULD be clearly documented. 6. It SHOULD be possible to limit the intervals of access to the secured data. 7. It SHOULD be possible to secure selected data (and keys in particular) using the four-eyes principle.
	Recommended Assurance Activity
	1. Analysis of the design documentation and certifications provided by the manufacturer is recommended.

SRR_06.CS	**Requirement**
	It SHALL be possible to secure the customer data and authentication data on the Customer Portal within the Central System.
	Recommendation and Implementation Guidance
	1. Password-hashing functions such as PBKDF2 [21] (or higher security) SHOULD be used to protect password databases from attacks. 2. It SHOULD be possible to separate the application server and webserver within the Customer Portal. For example, this enables the customer data to be stored on the application server, which can be protected more easily.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance of the design robustness. 2. Analysis of the design documentation provided by the manufacturer is recommended.

C.4 Access Control

Req._ID	
SAR_01.M	**Requirement**
	The Meter SHALL support Role Based Access Controls (RBAC) to protect the device from unauthorized access. • The Meter SHALL support at least the roles defined in Section B.3. • It MUST be possible to configure the privileges of individual roles. • It MUST be possible to assign individual key material to each role. These keys MUST be updatable. • It MUST be possible to bind roles to interfaces. • It MUST be possible to define more roles for future applications that are implemented remotely or via firmware updates.

	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should specifically ensure that each role has only the defined and necessary privileges.
SAR_01.GW	**Requirement**
	The Gateway SHALL support Role Based Access Controls (RBAC) to protect the device from unauthorized access. • The Gateway SHALL support at least the roles defined in Section B.3. • It MUST be possible to configure the privileges of individual roles. • It MUST be possible to assign individual key material to each role. These keys MUST be updatable. • It MUST be possible to bind roles to interfaces. • It MUST be possible to define more roles for future applications that are implemented remotely or via firmware updates.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should specifically ensure that each role has only the defined and necessary privileges.
SAR_01.CS	**Requirement**

	The Central System SHALL support Role Based Access Controls (RBAC) to protect against unauthorized access. • The Central System SHALL support at least the roles defined in Section B.3. • It MUST be possible to configure the privileges of individual roles. • It MUST be possible to assign individual key material to each role. These keys MUST be updatable. • It MUST be possible to bind roles to interfaces. • It MUST be possible to define more roles for future applications that are implemented remotely or via firmware updates.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification. 2. The connection between user authorization (e.g., passwords or smartcards) and the roles SHOULD be implemented using a suitable system, such as LDAP. 3. It SHOULD be possible to set up roles to enable access using the four-eyes principle.
	Recommended Assurance Activity
	1. It is recommended to conduct a functional test of the appropriate role-based access controls. This is to ensure that in the implementation of each role only the necessary permissions were provided.
SAR_02.M	**Requirement**
	The Meter SHALL support mechanisms to prevent and detect unauthorized access.
	Recommendation and Implementation Guidance
	1. The Meter SHOULD implement mechanisms to detect unauthorized access attempts. Where possible, the Meter SHOULD log the incident as a security event. An example of such an event would be the attempt to access a data object for which the user does not have

	permission. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of detection mechanisms can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_02.GW	**Requirement**
	The Gateway SHALL support mechanisms to prevent and detect unauthorized access.
	Recommendation and Implementation Guidance
	1. The Gateway SHOULD implement mechanisms to detect unauthorized access attempts. Where possible, the Gateway SHOULD log the incident as a security event. An example of such an event would be the attempt to access a data object for which the user does not have permission. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of detection mechanisms can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_02.CS	**Requirement**
	The Central System SHALL support mechanisms to prevent and detect unauthorized access.

	This specifically includes intrusion detection and monitoring systems on all interfaces of the Central System.
	Recommendation and Implementation Guidance
	1. The Central System SHOULD implement mechanisms to detect unauthorized access attempts. Where possible, the Central System SHOULD log the incident as a security event. An example of such an event would be the attempt to access a data object for which the user does not have permission. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of detection mechanisms can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_03.M	Requirement
	The Meter SHALL log successful logins as well as failed authentication attempts in the security log.
	Recommendation and Implementation Guidance
	1. The implementation of the security log SHOULD ensure that the entries do not overwrite other security-relevant entries. 2. The Meter SHOULD notify the Central System after a configurable number of failed login attempts. 3. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of correct event logging can be verified in a

	functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_03.GW	**Requirement**
	The Gateway SHALL log successful logins as well as failed authentication attempts in the security log.
	Recommendation and Implementation Guidance
	1. The implementation of the security log SHOULD ensure that the entries do not overwrite other security-relevant entries. 2. The Gateway SHOULD notify the Central System after a configurable number of failed login attempts. 3. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of correct event logging can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_03.CS	**Requirement**
	The Central System SHALL log successful logins as well as failed authentication attempts in the security log.
	Recommendation and Implementation Guidance
	1. The implementation of the security log SHOULD ensure that the entries do not overwrite other security-relevant entries. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.

	Recommended Assurance Activity
	1. The implementation of correct event logging can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.

C.5 Confidentiality

Req._ID	
SCR_01.M	**Requirement**
	The following interfaces of the Meter SHALL support application-layer encryption with an allowed algorithm: • LAN between the electricity meter and Central System, • WAN between the electricity meter and Central System, • Multi-Utility Interface between the electricity meter and other utility meters. • Customer Interface.
	Recommendation and Implementation Guidance
	1. Allowed encryption algorithms are defined in SPR_01. 2. Communication SHOULD be encrypted using symmetric algorithms, and preferably using an authenticated cipher.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should specifically ensure that each interface supports the allowed cryptographic algorithms.
SCR_01.GW	**Requirement**
	The WAN-interface of the Gateway SHALL support application-layer encryption with an allowed algorithm if it is used for maintenance purposes.

	Recommendation and Implementation Guidance
	1. Allowed encryption algorithms are defined in SPR_01. 2. Communication SHOULD be encrypted using symmetric algorithms, and preferably using an authenticated cipher.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should specifically ensure that each interface supports the allowed cryptographic algorithms.
SCR_01.CS	Requirement

	The following interfaces of the Central System SHALL support application-layer encryption with an allowed algorithm:
	• WAN_M between the electricity meter and Central System,
	• WAN_GW:
	  o between the electricity meter and the Central System,
	  o between the Gateway and Central System if the interface is used for maintenance purposes;
	• User Interfaces (UI);
	• All internal interfaces of the Central System (zone-to-zone);
	• Web Interface (WWW) of the customer portal;
	• Interface to the Back-End System in the MDMS.

	Recommendation and Implementation Guidance
	1. Allowed encryption algorithms are defined in SPR_01. 2. Requirement SRR_04.CS provides details on zoning in the Central System. 3. Section B.2 provides details on the interfaces of the Central System.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should in particular ensure that each interface supports the allowed cryptographic algorithms.

C.6 Audits and Logs

Req._ID	
SLR_01.M	**Requirement**
	The Meter SHALL provide a local audit trail for all security events. In addition to the existing log files, a dedicated security log SHALL exist to store security-relevant events. The Meter SHALL be equipped with dedicated registers counting the number of occurrences of security events during a particular interval. This interval SHALL be configurable. The Meter SHALL log at least the security events described in Section B.4.
	Recommendation and Implementation Guidance
	1. Each security event SHOULD record, where possible, the user or system identification (ID), the interface, the timestamp, as well as the result of the event. 2. The manufacturer SHOULD provide a list of all supported security events.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test of the security log. 2. Carrying out a penetration test is recommended to provide assurance that this requirement is adequately implemented.
SLR_01.GW	**Requirement**
	The Gateway SHALL provide a local audit trail for all security events. In addition to the existing log files, a dedicated security log SHALL exist to store security-relevant events.

	The Gateway SHALL log at least the security events described in Section B.4.
	Recommendation and Implementation Guidance
	1. Each security event SHOULD record, where possible, the user or system identification (ID), the interface, the timestamp, as well as the result of the event. 2. The manufacturer SHOULD provide a list of all supported security events.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test of the security log. 2. Carrying out a penetration test can provide assurance that this requirement is adequately implemented.
SLR_01.CS	**Requirement**
	The Central System SHALL provide a local audit trail for all security events. In addition to the existing log files, a dedicated security log SHALL exist to store security-relevant events.
	Recommendation and Implementation Guidance
	1. Each security event SHOULD record, where possible, the user or system identification (ID), the interface, the timestamp, as well as the result of the event. 2. The manufacturer SHOULD provide a list of all supported security events.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test of the security log. 2. Carrying out a penetration test is recommended to provide assurance that this requirement is adequately implemented.

SLR_02	**Requirement**
	Entries of all log files SHALL be protected from unauthorized changes.
	Recommendation and Implementation Guidance
	1. Role-Based Access Controls SHOULD protect the security log.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SLR_03.M	**Requirement**
	The Meter SHALL provide enough memory for the security log to store at least the last 100 security events. The security log file SHALL be set up as a rolling log file.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The requirement is verified by a functional test to ensure that the security log has sufficient capacity.
SLR_03.GW	**Requirement**
	The Gateway SHALL provide enough memory for the security log to store at least the last 1000 security events. The security log file SHALL be set up as a rolling log file.

	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The requirement is verified by a functional test to ensure that the security log has sufficient capacity.
SLR_03.CS	**Requirement**
	The components of the Central System SHALL support a connection to an external logging server.
	Recommendation and Implementation Guidance
	1. The Central System SHOULD support a dedicated logging server (e.g., a syslog server). This log server SHOULD log all security events of all components of the Central System. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The requirement is verified by a functional test to ensure that log server manages the security events correctly.

C.7 Product Lifecycle and Governance

Req._ID	
SDR_01	**Requirement**
	The manufacturer MUST be able to present an ISO/IEC 27001 certification

	for all security-related development processes, manufacturing processes, and provisioning processes for devices and products deployed in the Smart Metering system. Proof of certification must be provided upon delivery at the latest.
	Recommendation and Implementation Guidance
	1. The requirement applies in particular to all security-relevant development processes, manufacturing processes, and provisioning processes for the Meter and Gateway. 2. Moreover, this requirement applies to the development processes and provisioning processes for the Central Systems. 3. If security-related components are purchased from third-party suppliers, then the related areas and hand-over processes SHOULD be ISO/IEC 27001 certified. 4. Moreover, the ISO/IEC 27001 norm SHOULD be applied to any security-related tools and devices used in the Smart Metering architecture, e.g., the handheld terminal or maintenance software. 5. The manufacturer SHOULD share the corporate security policies.
SDR_02	**Requirement**
	The manufacturer SHALL use a secure configuration management system for managing products. All changes of deposited information SHALL be appropriate, comprehensible and documented. 1. The manufacturer SHALL implement adequate measures to guarantee IT security and physical security of the configuration management system. 2. The manufacturer SHALL provide an audit mechanism identifying the author of each change made. 3. Third party suppliers of security-relevant functions and products SHALL implement comparable processes.
	Recommendation and Implementation Guidance
	1. The requirement applies in particular to the development processes, manufacturing processes, and provisioning processes for the Meter, the Gateway and the Central System. 2. The following examples of a secured configuration management system SHOULD be considered:

	• Administration of hardware configurations of devices and their changes. • Administration of source code and firmware and their changes. • Administration of (customer-related) parameters of devices and their changes.
SDR_03	**Requirement**
	Secured versioning process: 1. All released versions (hardware and firmware) of a device or product MUST be uniquely identifiable. 2. Firmware SHALL be uniquely identifiable by its hash value. 3. The manufacturer SHALL be able to reproduce released versions for devices within the product lifecycle, with traceability provided by the hash value(s) as identifier(s). 4. Exchangeable hardware modules SHALL be versioned separately. 5. Software and software updates SHALL be uniquely identifiable by their hash value.
	Recommendation and Implementation Guidance
	1. The requirement concerns the versioning processes for developing the firmware of the Meter and the Gateway. 2. Moreover, the requirement concerns the versioning processes for developing software that is used in the Central System. 3. Requirement SPR_01 lists the allowed cryptographic hash algorithms. 4. Appendix A.2 describes an example process for generating digital signatures.
SDR_04	**Requirement**
	The manufacturer SHALL implement a flaw remediation and reporting process: 1. The manufacturer SHALL actively participate in the monitoring and testing of vulnerabilities. The manufacturer SHALL immediately provide information about vulnerabilities and promptly provide updates fixing vulnerabilities reflecting all technical possibilities. 2. The manufacturers SHALL implement a process for externally reported vulnerabilities.

	Recommendation and Implementation Guidance
	1. The requirement concerns the flaw remediation and reporting processes for the development and manufacturing of the Meter, the Gateway and the Central System. 2. The following examples of a flaw remediation and reporting process SHOULD be considered: • Identification and addressing of security flaws found by the manufacturer. • Identification and addressing of security flaws found by the grid operator. • Identification and addressing of security flaws found by external parties, e.g., security flaws published by researchers.
SDR_05	**Requirement**
	The manufacturer SHALL carry out extensive testing of products. These tests MUST include security tests. 1. All equipment MUST comply with the specifications of the documentation supplied by the manufacturer. 2. Using non-trivial test cases the manufacturer SHALL be able to demonstrate evidence of correct behavior under security and functional testing. 3. The tests MUST cover the entire scope of functions of the product and specifically include tests of the entire communication chain. 4. The tests SHALL cover adequate testing of both regularly-used as well as rarely-used functions, such as software updates. 5. The manufacturer SHALL provide the results of the conducted security tests at the time of release to the grid operator.
	Recommendation and Implementation Guidance
	1. The requirement concerns security testing of the Meter, the Gateway and the Central System. 2. The following examples of security tests SHOULD be considered: • Fuzzing tests • Robustness tests • Penetration tests Appendix B lists details for the above mentioned test types.

SDR_06	**Requirement**
	The manufacturer SHALL have a high ICT security awareness and provide training on ICT security for the staff. The manufacturer SHALL demonstrate possession of the necessary knowledge to develop and produce secure products. The manufacturer SHALL designate a technical contact for security-related matters.
	Recommendation and Implementation Guidance
	1. Example: • Documented professional experience in the area of IT security or a security certification, such as CISSP or CISM.
SDR_07	**Requirement**
	Security-enhancing features of the underlying platform, implementation language and tool chain SHALL be deployed. The manufacturer SHALL provide evidence if this is not necessary or possible.
	Recommendation and Implementation Guidance
	1. Examples of security-enhancing features are: • Secure boot process where the boot loader verifies the authenticity of the firmware. • Deactivation of hardware debug interfaces, such as JTAG interfaces. • Activation of microcontroller functions that enable read-out protection.
SDR_08	**Requirement**
	The manufacturer SHALL ensure secure provisioning of cryptographic keys during the manufacturing process. The manufacturer SHALL ensure a secure hand-over process to the grid operator.

	Recommendation and Implementation Guidance
	1. Examples: • The manufacturer SHOULD provide a secured production area to ensure the secure initial provisioning of cryptographic keys. • A secure hand-over process of the provisioned information to the Central System SHOULD be established. • Appendix A.1 describes an example process for secured provisioning.
SDR_09	**Requirement**
	The manufacturer SHALL present a security concept and detailed documentation of the components of the Central System that provide a remote maintenance function to a third party.
	Recommendation and Implementation Guidance
	1. Remote maintenance functions SHOULD be avoided where possible. 2. An example for securing the remote maintenance function would be a terminal server.

Appendix A Example Processes

The processes described are examples of how selected requirements can be implemented in the context of end-to-end security. The following sections with example processes are not normative but are meant to be interpreted as an aid for understanding.

Appendix A.1 Process for Provisioning of Cryptographic Key Material

One of the main requirements for the security architecture of the Smart Metering System is the use of cryptographic key material, which must be unique per device and per role configured on the device. The cryptographic key material must be generated randomly and securely provisioned for the device.

To optimize the installation process while maintaining security, it is suggested to perform the provisioning of key material at the manufacturers as one of the final steps in the manufacturing process. This initial cryptographic key material is used to perform a first, secure connection with the devices, for example, from the central system or handheld terminal. The security of the communication between these devices is therefore based on the established processes at the manufacturer for provisioning the cryptographic key material.

This results in the following main points which have to be considered:

- Requirements for the trustworthiness of the process environment
- Process requirements for generating and provisioning the cryptographic key material
- Requirements for the transfer processes of the provisioned cryptographic key material

It is strongly recommended to certify the areas in scope using ISO27001.

Appendix A.1.1 Requirements for the Process Environment

The process environment itself must meet several requirements to establish trustworthiness of the provisioned cryptographic key material.

First, the trustworthiness of the hardware to be provisioned with cryptographic key material must be guaranteed by the manufacturer. The manufacturer shall demonstrate that no manipulation of the hardware has occurred.

Furthermore, the trustworthiness of the firmware on the device must be ensured. The manufacturer must be able to prove the authenticity of the firmware of the device to be provisioned.

As a third point, the security of the provisioning area itself must be ensured. This includes in particular the security of the IT components being used and the physical access controls of the provisioning area.

Appendix A.1.2 Requirements for Generation and Provisioning

Generating, provisioning and storing cryptographic key material shall occur in a secure process environment.

To generate the cryptographic key material an approved random number generator shall be used as described in requirement SPR_02.

A distinction must be made whether a symmetric key or public/private key pair will be used:

- Initial symmetric keys should be generated outside of the device, within the secure process environment using an external random number generator. The key generated in this way is then provisioned to the device.
- A public/private key pair shall be generated within the device and within the secure process environment. Parts of entropy for the generation of the private key should be generated by an external random number generator. Corresponding random seed should be provisioned for the device. After generating the key pair it shall only be possible to obtain the public key in the form of a Certificate Signing Requests (CSRs) from the device. After processing the CSRs into a valid device certificate, it must be securely imported into the device together with other information (such as root certificates).

Appendix A.1.3 Requirements for the Transfer Process

The manufacturer and the operator of the Central System must share secure procedures for the exchange of provisioned cryptographic key material. The confidentiality and authenticity of provisioned cryptographic key material must be guaranteed at the transfer.

Such a transfer process can be modelled with the use of encryption mechanisms and digital signatures, for example:

> Manufacturers and operators of the Central System each may generate a public/private key pair and exchange their public keys in a secure fashion, i.e., using a public key infrastructure (PKI).
>
> The authenticity of the exchanged public keys must be strictly verified and documented.
>
> The manufacturer now uses the received public key to encrypt of all of the devices' provisioned sensitive data (e.g., all keys individually generated per role on a device).
>
> This encrypted data is inserted by the manufacturer into an electronic shipment file or an equivalent document that can be processed by the operator of the Central System. The serial number (or other unique device identifier) of a device is assigned to the

encrypted information. Before this electronic shipment file is provided to the operator of the Central System, the manufacturer signs the file using their own private key.

Upon receipt, the operator of the Central System checks the manufacturer's digital signature of the electronic shipment file by using the manufacturer's public key and thus verifies the authenticity of the received document.

As a second step, the operator of the Central System can decrypt the information encrypted by the manufacturer and import the data into the Central System.

Similar requirements apply as described in "Firmware Update Process" regarding securing access to the respective private key.

Appendix A.2 Firmware Update Process

The integrity of firmware is ensured by attaching a digital signature. The device can verify that the firmware actually is from the manufacturer on the basis of the digital signature. The device may only accept the firmware if it can clearly verify the manufacturer's authorship based on the digital signature.

To ensure the trustworthiness of a digital signature, the manufacturer shall establish a process for securely generating digital signatures.

Appendix A.2.1 Background Digital Signatures

When creating a digital signature first a hash value of the firmware is calculated. The digital signature is the result of the encryption of the hash value using the private key of the manufacturer. Upon receipt of the firmware, the device verifies the digital signature using the public key and then compares the hash value of the received file.

This results in the following main points that have to be considered:

- Requirements for the release process for firmware updates.
- Requirements for the access procedures and the security of the secret cryptographic key material, with which the digital signature of the firmware file is created (see requirements for key management).
- Requirements for the process of securely provisioning public cryptographic key material on the device (see requirement SDR_07).
- Requirements for the update process of the device itself (see requirements SIR_03. *).

It is strongly recommended that the areas described are certified according to ISO27001 (see requirement SDR_01).

This section describes suitable sample processes and relevant requirements in terms of ICT security.

Appendix A.2.2 Release Process

The manufacturer should establish a release process for new firmware versions. The manufacturer should appoint a person responsible for the approval process.

The release process should be documented by the manufacturer. The process must generate relevant evidence of the release process of firmware versions. It is important to note which person at which time authorized the release of firmware updates.

The version of the firmware updates must be documented on the basis of its hash value. If a firmware update is comprised of several components (i.e., different files), they must be individually named and documented based on their hash value. By authorizing the release of a firmware update, the manufacturer documents that the firmware file can be uniquely identified with its hash value.

Appendix A.2.3 Managing and Securing Secret Key Material

After releasing a firmware a digital signature must be created. If a firmware update consists of several components (i.e., different files), they must be individually signed.

The manufacturer must operate a system that controls access to the secret key material that is used for signature generation of firmware updates.

This system shall be operated in a secure IT environment.

The manufacturer should designate a person who is responsible for the generation of digital signatures. This person must then use the system to create a digital signature for the firmware.

It must not be possible for the responsible person to have direct access to the signing keys. The system shall only provide functions that digitally sign the firmware. Furthermore, the system must provide an audit mechanism that provides proof of time, responsible person, firmware version, and hash of the firmware when generating a signature.

In addition, the system shall protect the secret key material sufficiently with respect to physical access, for example, by storing the key on a secure hardware module.

After successfully creating the signature, the released firmware version can be combined along with the signature to form the final firmware update. This firmware update will be made available to the operator of the Central System.

Appendix A.2.4 Provisioning Process

To enable the automated verification of the digital signature of a firmware update, the corresponding public key material must be provisioned on the device.

This provisioning process of the public key material must be initially performed at the manufacturer in a secure environment. This process ensures the authenticity of the public key material that is provisioned on the device.

The public key material may be changeable afterwards by an authorized (digitally signed) firmware update.

Ideally, this provisioning process is performed together with the provisioning of all required cryptographic keys.

Appendix A.2.5 Update Process of the Device

Before a device is allowed to accept a firmware file to update from, it must verify the file's digital signature. Should the verification fail or if a digital signature is missing entirely, the device shall not accept the firmware. The device can thus ensure that the received firmware update is authentic, meaning it is actually supplied by the vendor.

Appendix A.3 Firmware Update Process

Multicast is a useful method to send firmware updates, which require significant bandwidth, to multiple devices at the same time. According to the IMA-VO the relevant data must be encrypted and authenticated when using multicast. Therefore, the multicast process is initiated by individual unicasts.

This results in the following example process:

1. The Central System creates a temporary multicast key. This multicast key will be the same for all devices, but must be encrypted with the individual key of the device, authenticated, and then can be sent to the appropriate device via unicast.
2. The Central System sends the firmware update via multicast to all initialized devices. The firmware update is encrypted and authenticated with the multicast key previously generated. Then the Central System discards the multicast key.
3. The Central System sends an activation message via unicast to all initialized devices. Each activation message is encrypted and authenticated with the individual key of the device.
4. The device decrypts and verifies the integrity of the message that contains the firmware update. Then, the device discards the multicast key.
5. Next, the device checks the integrity of the firmware file on the basis of the digital signature and the validity of the version number (see also Appendix A.2).
6. The device activates the firmware after it receives the activation message, decrypts it, and verifies the integrity.

Appendix A.4 Secured Calibration or Verification Process

The following process description is an example for ensuring the security of the Meter when it is passing through a calibration or test process. This example process can be used both for the company's internal calibration or testing procedures as well as for the calibration or testing procedures of a third party.

Appendix A.4.1 Transfer to Calibration or Testing Organization and Transfer of Key Material

The Meter and the associated key material of the "Calibration and Testing" role are made available for the calibration or testing organization.

In the Key Management System, the key material for the "Calibration and Testing" role is marked as *active*. *Active* means that the key material was issued for this role and that an update of this issued key material must be carried out as soon as this meter is put back into operation mode.

The transfer of the key material to a calibration or testing organization can be realized via a direct connection to the Key Management System, for example. Alternatively, the provisioned key material of the meter can be exported and passed through a secure "offline process". For example, this can be similar to the described transfer process in "Process for provisioning of cryptographic key material (at the manufacturer)".

Appendix A.4.2 Providing a Secure Calibration and Test Mode

Authentication between the calibration or testing organization and the Meter must be performed. For this, the provided key material is used. After successful authentication, the calibration or testing organization may put the Meter in a calibration mode or a test mode using the corresponding commands. All communication between the Meter and calibration or testing organization has to be authenticated. The given key material is used.

In this state, the calibration or testing of the Meter can take place.

After a successful calibration or test, the Meter must be reset into the "*normal operation*" mode with a corresponding command. The calibration or testing organization shall perform this last step, as the secured calibration mode may not be available outside of the calibration or testing organization.

The Meter has to automatically disable the "Calibration and Testing" role when entering normal operation mode.

Appendix A.4.3 Transfer into Operation Mode

The Meter is returned from the calibration or testing organization and can be used normally again. When returning, the key material for the role of "Calibration and Testing" is marked as "*update*" in the Key Management System.

Once the Meter is installed in the field and can be reached by the Central System, the key material for “Calibration and Testing” is updated by the "Central System Read-Write” role. Furthermore, the role of "Calibration and Testing" is activated again by the Central System.

For Meters that do not have an online connection at installation, the role of "Calibration and Testing" can be provisioned with new key material and reactivated using a Handheld Terminal through the "Maintenance" role.

Appendix B Glossary

The glossary is intended to explain special terms and abbreviations in the document. For detailed descriptions of test procedures, background information, or details about cryptographic methods, see the recommended literature.

Application Layer	**OSI**-Layer 5-7.
Authentication	For authentication one distinguishes between **entity authentication** (e.g., a person or a device) and **message authentication**. Authentication is used to verify the **integrity** of the communication partners or to verify **data integrity**.
Authenticity	Truthfulness of origin.
Bidirectional	Functioning in two directions. See also **bidirectional interface**.
Bidirectional interface	The signals can move in both directions during data transmission.
Block cipher	A cryptographic encryption method used to encrypt messages of fixed (block) length.
Broadcast	Data transmission technique in which a message is simultaneously transmitted to all subscribers on the network. Using a **multicast**, the message is sent to a group of selected participants in the network. Using a **unicast**, the message is sent to exactly one network participant.
BSI	The Federal Office for Information Security in Germany (German: Bundesamt für Sicherheit in der Informationstechnik).
Certificate	A digital certificate is a file that allows the verification of the authenticity of a communication participant or a message. See **Public Key Infrastructure**.
Confidentiality	Only selected users are allowed to access confidential messages. This is often done by **encryption** of messages, where only authorized persons get access to the secret **key material**.
Configuration Management System	The Configuration Management System is the system at the manufacturer that manages the lifecycle of the device from its development through manufacturing and procurement. In particular, the system includes the management of software and

	sources of (customer-specific) configurations of a device.
Cryptographic Hash Function	Cryptographic hash functions must behave like one-way functions and be collision resistant and strong collision resistant. Changes in the input message must lead to a significant change in the hash value. Example: SHA-256. See also ENISA [6].
Cryptography	ENISA's Algorithms, Key Sizes and Parameters Report [6] provides details on the state of the art in cryptography.
Data Integrity	See **integrity** and **message authentication**.
DAVID-VO	Austrian legislation: Datenformat- und VerbrauchsinformationsdarstellungsVO 2012. This catalog refers to the version DAVID-VO 2012 Design.
Device	The term “device" may refer to both the Gateway and the Meter. The Recommendation and Implementation Guidance provides further details.
Digital Signature	To ensure the **integrity** of the source. When generating a digital signature, first a **hash value** of the file is calculated. The sender generates the digital signature by encrypting this hash value using the secret key. The recipient verifies the digital signature using the public key and compares the **hash value** of the received file. In practice, digital signatures are generated using **elliptic curve** (**EC**) based algorithms.
Display	See *Chapter B*.
EC	Elliptic Curve. See also ENISA [6].
Encryption	The message is converted using a cryptographic method into a string called a ciphertext that is unreadable for an attacker. Decryption is the transformation of the ciphertext back into the original message text; it is performed with the same key (symmetric cryptography) or using the private key (**public key cryptography**).
Engineering Menu	A functionality of the device that allows a service engineer to change settings and perform information retrieval on the local display using keyboard inputs.
ENISA	European Union Agency for Network and Information Security.
Entity	Verification of the identity and **integrity** of the communication partners (e.g., users on the Meter). Moreover, verification that the

Authentication	communication partners are still alive throughout a session. See also **password authentication** and **strong authentication**.
EPRI	Electric Power Research Institute.
Fail-Secure	Construction principle in which security-relevant designs can guarantee confidentiality and integrity of the system in case of failures.
Four-Eyes Principle	Double checking. Decisions must be made by more than one person.
Fuzzing Test	A fuzzing test is carried out for quality assurance of software for secure network communications. This is done by generating a large, mostly random data volume, and may also contain erroneous data packets that are introduced in a structured manner in the data traffic. A detailed introduction to fuzzing can be found in [22].
Gateway	See Chapter B.
GPRS	General Packet Radio Service.
HAN	Home Area Network.
Handheld Terminal	A tool used by a service engineer to change settings and send information queries through the Maintenance Interface of a Meter or Gateway.
Hash Function	A function mapping a message to a bit sequence (i.e., **hash value**) of fixed length. See **Cryptographic Hash Function**.
Hash Value	Output of a **(cryptographic) hash function**.
Hybrid Encryption	Since **public-key cryptography** is resource-intensive in terms of key length, computational power, etc., algorithms, such as RSA, are used only in so-called hybrid methods. First a random symmetric session key is generated (for example, a 128-bit AES key). Then the session key is sent encrypted under the public key of the recipient. The actual messages are then encrypted and decrypted using the session key with the corresponding symmetric cipher (e.g., AES).
ICT Security	Information and Communications Technology Security.
IETF	Internet Engineering Task Force.

IMA-VO	Austrian legislation: Intelligente Messgeräte-AnforderungsVO. This catalog refers to the “339. Verordnung ausgegeben am 25. Oktober 2011 Teil II” version.
Integrity	The integrity of a message means protection against tampering. See also **authentication**.
Intrusion Detection System	An intrusion detection system monitors the behavior of components either on the component itself, or by monitoring the communication. Known attack patterns or anomalies can be detected and reported.
ISO 27001	ISO standard for ICT Security.
Key Material	**Key material** includes all cryptographic keys. Examples are master keys, symmetric keys, **session keys**, private keys and public keys (in **public-key cryptography**).
LAN	Local Area Network.
Log File	Events in the operation of meters are recorded in one or more log files. Another term is log. In a rolling log file, entries can (with appropriate permissions) be overwritten after exhausting the reserved storage space for logs.
MAC	Message Authentication Code. For verification of data integrity. Examples: CMAC, GMAC. See also ENISA [6].
Maintenance Interface	See Chapter B.
Message authentication	The **authenticity** of the message, i.e., that the message is genuine, must be guaranteed. This is done either by appending a message authentication code (e.g., AES-CBC-CMAC) or by using a block cipher in an authenticating mode of operation (e.g., AES-CCM, AES-GCM).
Meter	**Meter** refers primarily to the electricity meter. If necessary, electricity meter and **utility meter** will be explicitly distinguished.
Monitoring System	See **Intrusion Detection System**.
Multicast	Using a **multicast**, the message is sent to a group of selected participants in the network. A **multicast** is a special case of a **broadcast**.

NESCOR	National Electric Sector Cybersecurity Organization Resource. Program by the US organization **EPRI**. See also [23].
NIST	National Institute of Standards and Technology.
Nonce	A nonce is a unique, randomly generated string that must be used exactly once (in medieval English the common term "for the nonce" means "for this one time"). Appended to message to detect or prevent **replay attacks**.
OSI	Open Systems Interconnection. Reference model for network communication.
Password Authentication	The user logs into the device with the username and password or PIN. The device itself does not need to authenticate. This method is particularly vulnerable to stealing passwords using social engineering attacks. For critical areas mutual/strong authentication is recommended.
Penetration Test	The **EPRI** Program **NESCOR** is one of the organizations that provides guidelines on penetration testing with their “AMI Penetration Test Plan”.
Personal data	See Data Protection Regulation. Example: load profile values.
PLC	Power Line Communication.
Product Lifecycle	The product lifecycle includes the stages of design, development, production and procurement, operation and decommissioning of an appliance.
Public Key Infrastructure	System to issue, distribute and verify certificates.
Public-Key Cryptography	A cryptographic method in which a public key is provided for **encryption** as well as the verification of **digital signatures**. There exists a corresponding private key for each public key; this private key must not be made public under any circumstances (i.e., the private key needs to be kept secret). The private key is used to decrypt and **digitally sign** messages. Public-key cryptography is not used for direct encryption of messages. Rather, using so-called hybrid encryption a symmetric session key is sent encrypted under the public key. The authenticity of a public key is to be ensured with certificates in a **Public Key Infrastructure** (PKI). See also ENISA [6].

	The best known method of public-key encryption is RSA. In principle it is possible to digitally sign with RSA; in practice, however, digital signatures are created using elliptic curve (**EC**) based algorithms.
Read-Only	The user may read data. It is not allowed to write new information or to change existing information.
Read-Write	The user has read and write permissions.
Replay Attack	The attacker records the data of a session and uses it later to impersonate a different identity.
RFC	Requests for Comments. Published by the **IETF**.
Robustness Test	A robustness test is carried out for quality assurance of the stability of the system design. In particular, fault tolerance is tested.
Role	See Section B.3.
Session Key	Symmetric key used for encryption of all messages within a limited time frame (session).
Strong Authentication	In strong authentication, both sides need to authenticate themselves and thus prove their identity. Challenge-response protocols are often applied. Other common methods use certificates.
Unicast	Using a **unicast**, the message is sent to exactly one participant in the network. See also **Broadcast**.
Unidirectional	Functioning in only one direction. See also **unidirectional interface**.
Unidirectional Interface	The signals can move in only one direction during data transmission, e.g., from the Meter to the Customer on the Customer Interface.
Utility Meter	For example, meters for gas, water and heat consumption.
Versioning Process	A versioning process is part of **Configuration Management**.
WAN	Wide Area Network.

Appendix C References

[1] E-Control Austria. *Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft*, 27.Februar 2014. http://www.e-control.at/de/publikationen/publikationen-strom/studien/IKT_Risikoanalyse (last accessed on 11-November-2014)

[2] German Federal Office for Information Security. TR-03109-1. *Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* Version 1.0, Bonn, Germany, March 2013.

[3] Internet Engineering Task Force. *RFC 2119: Key words for use in RFCs to Indicate Requirement Levels*, 1997. http://www.ietf.org/rfc/rfc2119.txt

[4] National Institute of Standards and Technology. Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revision 3)*, July 2012.

[5] German Federal Office for Information Security. TR-03116, Teil 3, *Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme*. Adapted annually. Bonn, Germany, Version: 2014.

[6] ENISA. *Algorithms, Key Sizes and Parameters Report, 2013 recommendations*, version 1.0, October 2013. https://www.enisa.europa.eu/ (last accessed on 11-November-2014)

[7] National Institute of Standards and Technology. Special Publication 800-38D. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. November 2007.

[8] Internet Engineering Task Force. *RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards*, 2008. http://www.ietf.org/rfc/rfc5114.txt

[9] German Federal Office for Information Security. ECC Brainpool. *ECC Brainpool Standard Curves and Curve Generation*. Version 1.0 (2005), Bonn, Germany, http://www.ecc-brainpool.org (last accessed on 11-November-2014)

[10] Internet Engineering Task Force. *RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2*, 2008. http://www.ietf.org/rfc/rfc5246.txt

[11] Internet Engineering Task Force. *RFC 5289: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), 2008.* http://www.ietf.org/rfc/rfc5289.txt

[12] National Institute of Standards and Technology. *FIPS PUB 186-2, Digital Signature Standard (DSS)*, 2000.

[13] National Institute of Standards and Technology. *FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, May 2001.

[14] National Institute of Standards and Technology. *Annex C: Approved Random Number Generators for FIPS PUB 140-2* [13], February 2012.

[15] German Federal Office for Information Security. *Anwendungshinweise und Interpretationen zum Schema, AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*, Version 3.0, Bonn, Germany, May 2013.

[16] German Federal Office for Information Security. *Anwendungshinweise und Interpretationen zum Schema, AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren*, Version 3.0, Bonn, Germany, May 2013.

[17] National Institute of Standards and Technology. *Cryptographic Algorithm Validation Program.* http://csrc.nist.gov/groups/STM/cavp/ (last accessed on 11-November-2014)

[18] ÖNORM A 7700. *Sicherheitstechnische Anforderungen an Webapplikationen*. 2008.

[19] Open Web Application Security Project. https://www.owasp.org/index.php/Data_Validation (last accessed on 11-November-2014)

[20] *RSA. PKCS #11: Cryptographic Token Interface Standard.* For Updates see OASIS https://www.oasis-open.org/standards (last accessed on 11-November-2014).

[21] Internet Engineering Task Force. *PKCS #5: Password-Based Cryptography Specification Version 2.0*, 2000. http://tools.ietf.org/rfc/rfc2898.txt

[22] Ari Takanen, Jared DeMott, and Charlie Miller. *Fuzzing for Software Security Testing and Quality Assurance* (1 ed.). Artech House, Inc., Norwood, MA, USA, 2008.

[23] Electric Power Research Institute. *National Electric Sector Cybersecurity Organization Resource*. http://smartgrid.epri.com/NESCOR.aspx (last accessed on 11-November-2014)