Federal Office
for Information Security

Application Notes and Interpretation of the Scheme (AIS)

AIS B8, Version 1.0.1

Date:	24.10.2024
Status:	Mandatory
Subject:	Requirements for evaluation according to the BSZ in the GB “Komponenten im HAN des SMGW”
Document Owner:	Certification body of BSI
Distribution:	BSZ-Licensed Evaluation Facilities (ITSEF)[1] BSI internal Website of the BSI

[1]All evaluators in the evaluation facilities licensed by the BSI for evaluations in accordance with the BSZ.

Document history

Version	*Date*	*Editor*	*Description*
1.0	2024-07-01	BSZ SZ33, BSI DI21	1st edition
1.0.1	2024-10-24	BSZ S26, BSI D21	Update the requirement of the TOE-casing paragraph 37 from shall to should and added a additional sentence to the requirement.

Table 1: History of changes

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
Tel.: +49 (0)800 247 1000
E-Mail: bsz@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Introduction

1.1 Background

The scope (“Geltungsbereich”, *short:* GB) “Komponenten im HAN des SMGW” of the BSZ addresses components in the Home Area Network (HAN) of the Smart-Meter-Gateway (SMGW) according to [BSI TR-03109-5], i.e., components that use the TLS proxy functionality provided by the SMGW to connect with external entities in the Wide Area Network (WAN) of the SMGW.

The SMGW provides its HAN (and the components therein) with protection from unregulated access via its WAN, see [PP-0073]. In case a component in the HAN of the SMGW itself has a connection to further Wide Area Networks apart from the connection via the SMGW, the SMGW is not able to provide protection for that component from unregulated access via said connection. This is already addressed in [PP-0073] via the security objective for the operational environment OE.Network, which states:

It shall be ensured that [...] if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

Therefore, within the certification according to the technical guideline [BSI TR-03109-5], a security certification in form of a BSZ is required for components that may establish connections to networks where that connection cannot be secured by the SMGW.

This certification is addressed in the GB “Komponenten im HAN des SMGW” of the BSZ by considering the context of the Smart Metering System and its SMGW. Therefore, in this GB, particular IT-security requirements have to be fulfilled by components in the HAN of the SMGW. Further, a given security problem has to be addressed by these components.

Thus, in addition to the existing requirements for TOEs in the BSZ, additional requirements are presented in this document. Note that this document, together with the documents listed in Chapter 2, forms the basis for a BSZ in the GB “Komponenten im HAN des SMGW”.

The targeted audience are certifiers, evaluators as well as developers[2] in the BSZ field and especially those in the GB “Komponenten im HAN des SMGW”.

As the addressees differ for each chapter, if necessary, the usage for each chapter is described separately therein.

1.2 Structure

The document is structured into the following chapters.

Chapter 2 lists all additional documents that are applicable for a BSZ in the GB “Komponenten im HAN des SMGW”.

Chapter 3 addresses additional requirements for the evaluation of a TOE in the scope of the GB “Komponenten im HAN des SMGW”. These requirements specify and add to the requirements in [AIS B4] and [AIS B2]. This chapter is directed mainly to the ITSEF.

Chapter 4 addresses the requirements for the TOE in the GB “Komponenten im HAN des SMGW”. It thereby replaces [AIS B6]. Further, it contains specific requirements to the cryptography of the TOE that add to the requirements in [AIS B2]. This chapter is relevant for the applicant as well as the ITSEF.

[2] Note that in the context of the BSZ process, the entity applying for a BSZ is called “applicant”. This may, but need not be the developer of the product/TOE the BSZ is conducted upon.

Chapter 6 addresses additional requirements for the ST in the style of a mandatory template. This chapter is addressed to the applicant as well as to the ITSEF. The template itself can be found in Chapter 9 (Appendix A: ST Template).

Chapters 7 and 8 respectively contain the glossary and a list of references.

Chapter 9 (Appendix A: ST Template) contains the normative ST Template as an appendix. The applicant shall base the ST for the TOE on this template.

2 BSI Documents for a BSZ in the GB “Komponenten im HAN des SMGW”

1. [BSZ-Prod] Produktzertifizierung: Programm Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Produkte, BSI
2. [BSZ-Prüf] Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Prüfstellen, BSI
3. [BSZ-EP] Programm [BSZ-Prüfstellen]: BSZ Evaluierungsprozess, BSZ-EP, BSI
4. [AIS B1] Requirements for ST and further documentation, BSI
5. [AIS B2] Requirements for the evaluation of cryptographic mechanisms according to the BSZ, BSI
6. [AIS B3] Requirements for user guidance, BSI
7. [AIS B4] Requirements for Evaluation according to the BSZ, BSI
8. [AIS B5] Guideline for determining the efforts for a BSZ evaluation, BSI
9. [BSZ-ETR] BSZ – Vorlage für den Evaluierungsreport, BSI
10. [BSZ-ADA] BSZ - Agenda der Auftaktbesprechung, BSI

3 GB-specific requirements to the evaluation

3.1 Introduction and usage of this chapter

This section is an addendum to [AIS B2] and [AIS B4] for the GB “Komponenten im HAN des SMGW”. It contains refined requirements as well as additional requirements for the evaluation according to the BSZ in the GB “Komponenten im HAN des SMGW”.

When conducting an evaluation according to the BSZ in the GB “Komponenten im HAN des SMGW”, evaluators shall adhere to these requirements in addition to those in [AIS B2] and [AIS B4].

The following sections contain tables with the refined or additional requirements. The tables are structured as follows: The first column contains an identifier for the requirement whereas the second column specifies whether the requirement stated is a new requirement (“new”) or whether it is a refined requirement within an existing paragraph in [AIS B4] or [AIS B2]. The third column addresses the scope of the requirement, i.e., the context in which evaluators shall adhere to the requirement. The last column states the refined or additional requirement.

3.2 List of refinements to the requirements in [AIS B4]

No.	Refined paragraph / new	Scope	Requirement
1	New	[AIS B4], Sect. 3.1: Phase 1	The ITSEF shall confirm that the ST is conformant to the ST Template.
2	New	[AIS B4], Sect. 3.1: Phase 1	The ITSEF shall receive at least 3 copies of the TOE. Note that it is at the discretion of the ITSEF to demand more than 3 copies of the TOE. However, this has to be communicated with the applicant as early as possible, and before the kick-off.
3	New	[AIS B4], Sect. 3.1: Phase 1	The ITSEF shall receive a vulnerability report as described in [AIS B1]. Note that for this scope, the vulnerability report is not optional but mandatory.
4	New	[AIS B4], Sect. 3.1: Phase 1	The ITSEF shall evaluate that the required items provided along with the ST are consistent. For example, all libraries used by the TOE are contained in the SBOM and the SBOM is up to date.
5	New	[AIS B4], Sect. 3.3: Phase 2	The ITSEF shall evaluate that the applicant’s justification in the vulnerability report as to why the vulnerabilities contained are not relevant to the TOE, is plausible, consistent, and complete.
6	New	[AIS B4], Sect. 3.3: Phase 2	When analysing the findings of the evaluation considering possible attack paths of Attacker.LocalPhys as defined in the ST, the ITSEF shall in particular take into account Assumption.PhysicalProtection as well as the fact that an attack of Attacker.LocalPhys is only considered successful if the manipulation of the TOE casing remains undetected.

No.	Refined paragraph / new	Scope	Requirement
7	New	[AIS B4], Sect. 3.3: Phase 2	The ITSEF shall include in the ETR the result of the conformance check of the ST with the ST Template.

Table 2: Added and refined paragraphs for AIS B4

3.3 List of refinements to requirements for the evaluation of cryptographic mechanisms in [AIS B2]

No.	Refined paragraph / new	Scope	Requirement
1	New	[AIS B2], Sect. 3.1.1, Cryptographic specification	Cryptographic mechanisms used by the TOE shall be in accordance with Sect 4.7 of this document, [AIS B8].
2	Refined paragraph 24	[AIS B2], Sect. 3.2, Conformity assessment and vulnerability analysis	The aim of conformity assessment in the context of BSZ cryptographic evaluation is to determine that the cryptographic mechanisms of the TOE are in accordance with SCES (SOG-IS Crypto Evaluation Scheme), with Sect. 4.7 of this document, [AIS B8], and with BSI policies, and that the implementation of the TOE is compliant with the applicant documentation.

Table 3: Added and refined paragraphs for AIS B2

4 GB-Specific requirements for the provision of the TOE and its environment

1 In the GB “Komponenten im HAN des SMGW”, the requirements of the [BSZ-Prod] for the provision of the TOE, including the required operating environment, apply. This means that the applicant must provide the required operating environment, including the SMGW and a system to control and configure the SMGW and the TOE.

2 In addition to the TOE, the applicant must provide the ITSEF with a debugging variant of the TOE. The purpose of the debugging variant is, among other things, to enable efficient testing of client services. The applicant and ITSEF determine exact specification of the debugging variant on a case-by-case basis between the applicant and ITSEF with the agreement of the certification body.

3 The debugging variant must contain all functions of the TOE. The functions must be implemented in the same way and version.

5 GB-specific requirements to the TOE

5.1 Introduction

This chapter defines requirements that each TOE and their documentation have to fulfil for a BSZ in the GB "Komponenten im HAN des SMGW". It thus replaces [AIS B6]. Note that requirements that are identical to requirements in [AIS B6] are marked by the symbol Δ.

It further contains additional requirements as well as refined requirements for the cryptography of the TOE in addition to the requirements in [AIS B2].

Note: The applicant has to state implementation details such as the limit of authentication attempts or the time after which a renewal of authentication is necessary in the guidance documents.

5.2 Authentication and authorization

4 The TOE shall identify and authenticate the user on each respective interface before the user can access the services. In the ST, the users of the TOE are mapped to assets they have access to and their respective kind of access. It shall be ensured that users can only access assets after successful authentication.
Note 1: Anonymous use may be possible if compromising the TOE is not possible and no critical configuration can be changed.

5 The TOE shall uniquely identify itself and be able to authenticate itself to the user. [Δ]

6 The TOE should allow administration of all existing user accounts. [Δ]

7 The TOE shall allow users to alter their own local authentication data, e.g., passwords and user names. In the case of certificate or pre-shared secret based authentication it is sufficient if the TOE allows an admin to change the authentication data. The TOE shall protect authentication data from unauthorized access.
Note: The users of the TOE that are allowed to modify these data have to be specified in the ST.

8 The TOE shall provide a role management for access to files, data, and services. Only necessary for users with different roles and the access rights shall be assigned restrictively.
Note: The assigned access rights have to be consistent with the information given in the ST as to which users have access to which assets.

9 The TOE shall provide administrative users with user management functionalities that at least comprise creating, editing, and revoking access rights.

10 The TOE shall not contain hard-coded cryptographic secrets (e.g., passwords, cryptographic keys, or other credentials) that are shared by multiple products.
Note: This does not include parts which are intended to be publicly known by design, e.g., public keys in asymmetric cryptography.

11 The TOE shall check for sufficient complexity and security of authentication data during creation or modification. The required configurable strength should be based on recognised security guidelines[Δ].

12 The TOE shall not leak or allow for inference about security relevant information as response to authentication. [Δ]

13 The TOE shall limit authentication attempts for password-based authentication to prevent brute force attacks.

14 The TOE shall request re-authentication on all interfaces intended for human user interaction after 10 minutes of inactivity, otherwise after 48 hours at latest.

5.3 Logging

15 The TOE shall as a minimum log the following events:

- Incorrect authentication
- Firmware update initialisation and successful / failed firmware update
- Backup and backup restoring
- Configuration changes

16 For the events mentioned above, the TOE shall save the following information:

- Time stamp
- Event ID
- Event type
- Event source (user identity or software process the event originated from)
- Result of the action triggering the event

17 The TOE shall provide sufficient local storage for event logs. [Δ]
Note: The minimal duration until the oldest events get overwritten is not specified. This information has to be included in the ST. It has to be kept in mind that a too short duration may result in undetected attacks on the TOE and its assets. It is recommended to retain log data for at least three months, see also [NIST SP 800-92].

18 The TOE shall maintain its security functionality (possibly with the exception of logging) even if insufficient local storage space is available.

19 The TOE shall limit access to logging data to authorized users with permission to access the information according to the description of the respective assets in the ST.

5.4 Services

20 The TOE shall respond robustly to incorrect or erroneous data of its services. The TOE shall not reach an undefined state at any time. [Δ]
Note: This requirement is independent from the attack path.

21 The TOE shall protect the integrity, authenticity, and confidentiality of transmitted data according to the security properties of the respective assets.
Note: The implemented security functions may depend on the security properties (such as integrity, confidentiality, and authenticity) of the assets. E.g., in cases where resulting data is not confidential, protection measures may solely focus on integrity and authenticity.

22 The TOE shall validate input and output before processing to avoid erroneous processing. [Δ]
Note: The input and output data from the TOE itself or external interfaces have to be checked for syntax, length, and content. This requirement is independent from the attack path.

23 The TOE shall treat errors adequately. [Δ]

24 The TOE shall not leak critical information in error messages. [Δ]
Note: Error messages shall not contain information relevant to potential attackers. Log files shall not contain authentication data.

25 The TOE shall provide a reset functionality to the default configuration, retaining the latest installed firmware version. For this purpose, a function shall be available that deletes all security relevant data and personally identifiable information securely and reliably.
Note 1: This function can also be security-critical and should be secured appropriately.

Note 2: The applicant has to provide a short technical description of the method used to delete the data.
Note 3: This functionality is necessary for decommissioning.

26 The TOE shall provide means for backups and recovery of the current configuration. [Δ]

27 In the default configuration, only services that are required to perform basic functions should be enable in the TOE. Users shall be provided with an option to disable services, which are not required. [Δ]
Note: In the default configuration, as few services as possible should be active to minimize the attack surface in accordance with the principle of security by design. The default configuration shall only provide the functions essential to the purpose of reaching the secure configuration[3].

28 Only services and software required to provide the functions of the TOE shall be present on the TOE. Development information shall be removed. [Δ]

29 The TOE shall provide the ability for firmware updates.

30 The TOE shall restrict the action to initiate a firmware update to administrators and the TOE itself.
Note 1: The firmware update file is an asset which shall be protected at least in its integrity and authenticity and has to be described as such in the ST. It has to be ensured that the initiation of the firmware update process can only be configured by users with the respective administrative rights using genuine update files.
Note 2: Automatically configured updates can pose a risk with respect to supply chain attacks on the development and update infrastructure. The way of introduction of the update into the TOE has to be described in the ST for the respective Security Function.

31 The TOE shall confirm the authenticity and integrity of update files before installation. [Δ]

32 The TOE shall confirm that the version of the firmware update to be installed is newer than the currently installed version.

33 Access to wireless interfaces of the TOE shall be robust and should be secured.

5.5 Basic physical protection

34 The TOE shall implement measures to impede physical attacks, meaning that the casing of the TOE shall be designed in a way that it protects internal components, prevents bypassing, and cannot be opened easily without detection. In particular, the TOE shall provide tamper evidence, that is, evidence (physical or digital) remains after a tampering event.
Note: The TOE may alternatively provide protection of undocumented interfaces from direct physical access e.g., by having an encapsulated PCB. In this case, the applicant should provide proof for this to facilitate the verification of the fulfilment of this requirement.

35 The TOE casing shall protect any interfaces not mentioned in the ST as accessible interfaces from direct physical access, i.e., the TOE-casing shall not expose critical conductor tracks or vital components (e.g., through ventilation slots).

36 If the TOE casing features visible screws, security screws shall be used.

37 Lids, flaps, and attachable components of the TOE casing should be secured to the TOE casing in a tamper evident manner. They should be secured via seals to the TOE casing. Alternative solutions are possible as long as requirement 35 still holds.

[3] That is, the configuration chosen by the applicant for the evaluation and certification according to BSZ.

5.6 Guidance documentation

38 The applicant shall provide a guidance documentation that describes the secure use of the TOE. This includes the installation, configuration, operation and decommissioning. Further, the intended use and operational environment shall be described. Δ
Note: This documentation is not limited to the Secure User Guidance and includes all user documentation for the product.

39 The applicant shall document the following features present in the default configuration:

- TOE's interfaces
- Users
- Roles
- Services and related functions
- Activation and deactivation status for the services Δ
  Note: The status of the features is not required to be provided in the documentation. Service information can also be provided using a designated service on the TOE.

40 The guidance documentation shall contain security relevant error messages at least for the firmware update and the status codes of the HTTP as well as a description of these and implications for the secure operation of the device.
Note: The documentation or configuration advice has to provide hints for possible security issues or implications.

41 The guidance documentation shall state how the user may gain information on how to identify the TOE and its version.

42 The guidance documentation shall contain an address for reporting security issues and bugs.

43 The guidance documentation shall contain the information on the expected end of support, in particular how long updates are provided by the developer and how these updates may be obtained.

5.7 Cryptography

44 The TOE shall perform cryptographic operations in accordance with the requirements in [AIS B2]. In addition, the TOE shall adhere to the following additional requirements that refine the requirements in [AIS B2] or add further specifics.

45 The TOE should not use algorithms from the SOG-IS catalogue [SCES-ACM] that are marked as "legacy".

46 The TOE should only use cryptographic mechanisms that follow the recommendations from [BSI TR-02102-1].

47 For communication with subsequent devices, the TOE should use TLS according to [BSI TR-02102-2].

48 If used, the TOE should implement the cryptographic protocols IPsec as well as SSH according to [BSI TR-02102-3] or [BSI TR-02102-4], respectively. Recommendations within these documents should be adhered to.

49 For communication with the SMGW, the TOE shall only use cryptographic mechanisms according to [BSI TR-03109-3].

50 If the TOE implements a protocol or standard for which there exists a security profile or extension, this extension should be used.
Note: For example, TOEs using wM-Bus should implement an appropriate secure mode.

6 GB-specific requirements to the ST

6.1 Introduction

This chapter is an addendum to [AIS B1] for the GB “Komponenten im HAN des SMGW” and introduces the Security Target (ST) template for the products addressed by this GB “Komponenten im HAN des SMGW” provided in Appendix A: ST Template. The structure of the ST Template follows the requirements from [AIS B1] and is depicted in Figure 1.

Applicants shall use this template to create an ST suitable for a certification process according to the BSZ in the GB “Komponenten im HAN des SMGW”. Note, however, that the usage of this template does not guarantee a pass on the evaluation of the ST by the ITSEF according to Phase 1 of the evaluation, see [AIS B4]. That is, the template does not prescribe a solution to the security problem as a set of security functions but rather constitutes a framework for the applicant to present their own solution. Adjustments for each individual product/TOE are to be expected and are reflected in the degrees of freedom throughout this document.

The ST Template itself may be found in Appendix A: ST Template.[4] Section 6.2 contains information on how to read and use this template. The use of this template is mandatory.

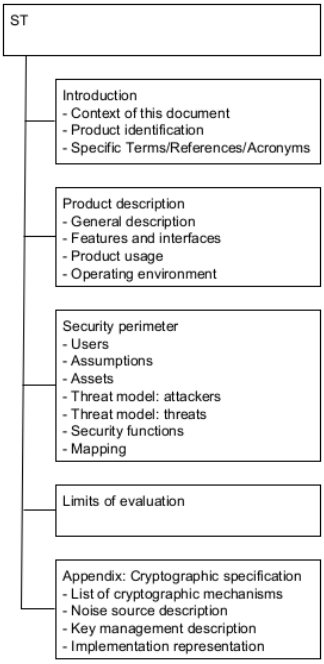

Figure 1: Structure of the ST

6.2 Usage of the ST Template

6.2.1 Notations

Content that shall be present in every ST is printed as normal text.

Content that shall be completed by the applicant with information specific to the TOE is marked in <chevrons>. For tables, this additionally means that further rows for additional entries shall be added if necessary.

[4] The ST Template may also be found in editable format on the BSZ web page for the GB “Komponenten im HAN des SMGW”.

Implementation details are marked bold und underlined. They contain information that the applicant shall comply with during implementation of the ST (e.g., when filling out operations marked with chevrons). They shall not be present in the applicant's ST.

Notes are marked in *italic* and give information on required contents of the respective chapters or sections. They may also be nested inside chevrons to give information concerning applicant actions. They shall not be present in the applicant's ST.

6.2.2 Applicants

The document [AIS B1] describes the structure of an ST suitable for a BSZ as well as general requirements on the contents of each described section. This ST Template specifies on mandatory content in the ST for products to be evaluated in the GB "Komponenten im HAN des SMGW". Therefore, applicants have to adhere to both [AIS B1] and this ST Template when implementing the ST for their product/TOE.

In terms of TOE functionality, this document focusses on security functions dedicated to mitigating the security problem. Keep in mind that further requirements on TOE functionality can be found in the respective BSZ documents and in Chapter 4.

Note that this template does not contain specific examples. For these, please refer to [AIS B1]. This is to avoid confusion among possible users of this template on how to fill in the necessary information.

6.2.3 ITSEF

Conformance of the ST to the ST Template shall be confirmed by the ITSEF during Phase 1 of the evaluation, see Chapter 3. Therefore, the ITSEF shall confirm that content marked as mandatory (by the notion "Implementation detail" as explained in Section 6.2.1) is actually included in the ST of the applicant.

6.3 SBOM

The SBOM provided by the applicant shall include the vulnerability report as described in [AIS B1].

7 Glossary

Term	Explanation
Default configuration	Configuration in which the TOE is being shipped to its final recipient/user and in which the TOE is initially started. All settings are set to values defined by the developer and no user specific settings exist. Not to be confused with the secure configuration after installation of the TOE according to the Secure User Guidance [AIS B3].
Guidance documentation	Documentation directed towards users of the TOE that contain information on the TOE as well as guidance on how to use the TOE.
Secure configuration	Configuration of the TOE the applicant chooses for the evaluation and certification according to BSZ. Has to coincide with the version reached after conducting installation procedures according to the SUG on the TOE in the default configuration. May also comprise aspects of the operational environment. Also referred to as “chosen configuration”.
Service	A service provides different functions using an interface. This might be for example a web server with corresponding web application for configuration.
State	Operating condition of the TOE at a given point in time. Comprises all reachable functions, processes, and data.
Applicant	Entity applying for a BSZ.
SUG	Secure User Guidance; necessary input for an evaluation according to BSZ. See [AIS B3]. It contains information directed at the secure installation and configuration of the TOE. After following the SUG, the TOE shall be in the secure configuration.
SMGW	Smart-Meter-Gateway; the external entity in whose HAN (Home Area Network) a TOE of the GB “Komponenten im HAN des SMGW” is situated and to which it is connected. For information on the SMGW, see e.g. [BSI TR-03109-1] and [BSI PP-0073].
TOE	Target of Evaluation; in the context of GB “Komponenten im HAN des SMGW”, it comprises a physical product as defined in the ST and supporting documents (e.g., guidance).
User	A user can either be a human or a service, for which access is granted over an interface.
wM-Bus	Wireless M-Bus

8 References

1. [BSI TR-02102] Technischen Richtlinien der Serie BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, current version
2. [BSI TR-03109] BSI TR-03109: Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb, current version
3. [GDPR] General Data Protection Regulation: Verordnung (EU) 2016/679, 2016, Version: ABI L 119 vom 4.5.2016, p. 1–88
4. [NIST SP800-92] Guide to Computer Security Log Management, 2006
5. [RFC 2119] RFC 2119, Key words for use in RFCs to Indicate Requirement Levels
6. [SCES-ACM] SOG-IS Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms, current version

9 Appendix A: ST Template

Note: For more information and guidance on how to write a Security Target (ST), see the document 'ST Template for BSZ scope "General Network Components and embedded IP Connected Devices"'. To be found on our website under the document section 'Further documents and templates'.

9.1 Introduction

9.1.1 Context of this document

This Security Target (ST) template was created for the BSZ certification of <TOE name and version> at BSI. The configuration of the TOE is based on the requirements arising from the technical guideline [BSI TR-03109-5] <*if applicable*: further reasons for the secure configuration the applicant chose for evaluation, e.g., market research>. For the key personnel involved in the development of the ST, see Table 4.

Name	Position / Affiliation	Function in development of ST
<Name>	<Position>, <Affiliation>	<Author/Review/QS/Release>
<*if applicable:* further names>	<*if applicable:* Position, Affiliation>	<*if applicable:* Author/Review/QS/Release>

Table 4: Key personnel involved in the development of the ST

Implementation detail 1: The applicant shall reference the exact version of the [BSI TR-03109-5] the security perimeter is based on.

9.1.2 Product identification

Product name	<TOE name> <*if applicable:* shorthand>
Product version	<TOE version> <*if applicable:* (sub-)versions of soft-/hardware used>
Supporting documents	<Guidance document>, <version and short description> <Secure User Guidance>, <version and short description> <*if applicable:* further supporting documents with version and short description>
Configuration	<Description of secure configuration with reference to the SUG>
GB version	<Version of the [AIS B8] that was used for the creation of this ST>

Table 5: Product identification

<Description of the procedure for unique identification of the TOE by the expected end customer>

Implementation detail 2: The applicant shall define the configuration chosen for evaluation by exact reference to the SUG.

9.1.3 Specific terms/references/acronyms

9.1.3.1 Specific terms

Term	Description
aEMT	External entity in the WAN of the SMGW that uses the transparent TLS-proxy function of the SMGW to establish a secure communication between the aEMT's IT-systems ("backend-systems") and the CLS. The backend-systems have to be included in a successfully certified ISMS audit (ISO 27001) by a third party (see [SM-PKI CP]). Additionally to the operation of the backend systems, an aEMT can assume different users regarding the CLS (see chapter Users).
<*if applicable*: controllable device>	Installation that produces or consumes power and whose input or output may be controlled via the TOE. <*if applicable:* information on the specific kind of controllable device>
CLS	Systems in the HAN of the SMGW that may use the TLS proxy functionality of the SMGW for dedicated communication purposes with entities in the WAN of the SMGW.
HAN (of the SMGW)	Network that is connected (on Layer 3) to the Interface IF_GW_HAN as defined by [PP-0073].
<*if applicable:* sensor data>	Data that are collected by sensors of the TOE itself or by sensors of subsequent devices.
<*if applicable*: subsequent device>	Physical device or system that interacts with <a component in the HAN of the SMGW/the TOE> but that is not part of the HAN of the SMGW itself.
TLS proxy	Proxying functionality of the SMGW to establish a secure communications channel between an aEMT in the WAN and a CLS device (i.e., component in the HAN). See [PP-0073], [BSI TR-03109-1] and [BSI TR-03109-5] for more information.
WAN (of the SMGW)	Network that is connected (on Layer 3) to the Interface IF_GW_WAN as defined by [PP-0073].
<*if applicable:* further used terms>	<*if applicable:* description of further terms>

Table 6: Specific Terms

Implementation detail 3: The applicant shall define all specific terms used throughout the document.

9.1.3.2 Acronyms

Acronym	Description
aEMT	Active external market participant (Aktiver Externer Marktteilnehmer)
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
BSZ	Fixed-time cybersecurity certification (Beschleunigte Sicherheitszertifizierung)

Acronym	Description
CLS	Controllable Local System
GB	Scope of the BSZ (Geltungsbereich)
GDPR	General Data Protection Regulation
HAN	Home Area Network (of the SMGW)
RFC	Request for Comments
SMGW	Smart Meter Gateway
TLS	Transport Layer Security
TOE	Target of Evaluation
USB	Universal Serial Bus
WAN	Wide Area Network (of the SMGW)
<*if applicable:* PKI>	Public Key Infrastructure
<*if applicable:* further used acronyms>	<description of further acronyms>

Table 7: Acronyms

Implementation detail 4: The applicant shall define all acronyms used throughout the document.

9.1.3.3 References

Identifier	Description
AIS B SMGW HAN	*Requirements for Components in the HAN of the SMGW,* <version>
BSI TR-03109-1	*Technische Richtlinie TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* 2021. Bundesamt für Sicherheit in der Informationstechnik, <version>
BSI TR-03109-3	*Technische Richtlinie BSI-TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen.* 2014. Bundesamt für Sicherheit in der Informationstechnik, <version>
BSI TR-03109-5	*Technische Richtlinie TR-03109-5: Kommunikationsadapter*. 2023. Bundesamt für Sicherheit in der Informationstechnik, <version>
BSI TR-03116-3	*Technische Richtlinie TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3 – Intelligente Messsysteme.* Bundesamt für Sicherheit in der Informationstechnik, <version>
GDPR	*https://gdpr.eu/*
PP-0073	*BSI-CC-PP-0073-2014: Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP).* Bundesamt für Sicherheit in der Informationstechnik, <version>

Identifier	Description
<guidance document reference>	<guidance document according to the requirements in Section 5.6>, <version>
<SUG reference>	<secure user guidance according to the configuration in Section 9.1.2 and [AIS B3]>, <version>
<*if applicable:* further references>	<further references>, <version>

Table 8: References

Implementation detail 5: The applicant shall list all references used throughout the document. They shall adjust the references to the respective version and therefore add or alter the references above, if necessary.

9.2 Product description

9.2.1 General description

The <TOE name> is a <product type>. <General information of the product>. It is designed to be used in the HAN of a certified SMGW. <Describe the main functionality of the product>.

It uses the TLS proxy functionality provided by the SMGW to connect with <external entities> in the WAN of the SMGW. As such, it contains a CLS communication adapter as defined in [BSI TR-03109-5].

<External entities> in the WAN use the <TOE name> to <high-level description of the main functionality of the TOE>.

Implementation detail 6: The applicant shall describe the main functionality of the product.

Implementation detail 7: The applicant shall describe the different possible external entities in context of the product usage.

<*if applicable*: further general information on the TOE/product>

<*if applicable*: further high-level information on further functionalities of the TOE/product>

9.2.2 Features and interfaces

<Description of features of the product.>

Implementation detail 8: The applicant shall add information on the basic physical protection required by Sect. 5.5.

Implementation detail 9: The applicant shall describe all functionalities of the product. The description should be short and precise and not use company-specific terms.

The <TOE name> provides the following interfaces:

Physical Interface	Logical Interface	Protocol	Description	Scope of evaluation
<name of physical interface that is connected to the SMGW>	<Indication as Client/Server:> <name of logical interface for	<Protocol for TLS-communication via the SMGW> using TLS <version> <if	Interface for TLS-communication via the SMGW using the TLS proxy	yes

Physical Interface	Logical Interface	Protocol	Description	Scope of evaluation
	communication with or via the SMGW>	applicable: with mTLS>	functionality of the SMGW. <*if applicable:* further information on the interface>	
<*if applicable:* name of physical interfaces for direct interaction with the TOE[5]>	<if applicable: Indication as Client/Server:> <name of logical interfaces for direct interaction with the TOE>	<name of the protocol> <*if applicable:* authentication method>	<information on the interfaces>	Is the interface in scope of the evaluation? Is it necessary for the typical usage? Is it active?

Table 9: Interfaces of the TOE

Implementation detail 10: In Table 9, the applicant shall provide a complete list of interfaces with a short description of each interface.

Implementation detail 11: The applicant shall differentiate interfaces on a physical and logical level.[6] The description shall therefore summarize the purpose of the interface.

Implementation detail 12: The applicant shall elaborate on the usage of the interfaces by reference to guidance documents or the appendix.

9.2.3 Product usage

The TOE is intended to be used as <high-level description of the main functionality of the TOE> via the TLS proxy channel provided by the connected certified SMGW.

<*if applicable:* further information on the usage of the TOE/product>

Implementation detail 13: According to [AIS B1], the applicant shall describe how and for which applications the TOE is intended to be used by which consumers.

9.2.4 Operating environment

The TOE is intended to be placed in <high-level description of the intended environment of the TOE>. It is connected to a certified SMGW <*if applicable*: further information regarding the SMGW, e.g., versions of the criteria according to which the SMGW has to be certified> via the HAN-interface (IF_GW_CLS) of said SMGW.

<*if applicable*: information on specific hard-/software necessary for operation of the TOE, aside from the certified SMGW>

<*if applicable*: information on connections to (local) devices>

<diagram of the system architecture>

[5] Simple power switches may be excluded.

[6] E.g., the interface that is intended to be used for communication with the TLS proxy of the SMGW (via IF_GW_CLS) shall be distinguishable from other logical interfaces that might use the same physical connection. Further examples are interfaces that are intended for communication with subsequent devices.

Implementation detail 14: The intended operating environment shall comply with the assumptions made in Section 9.3.2.

Note: The applicant should keep in mind the operating environment of the SMGW (cf. [PP-0073] and [BSI-TR-03109]), i.e., it should be possible to operate the TOE securely in the environment of an SMGW.

Implementation detail 15: The applicant shall provide a diagram with a level of abstraction sufficient to distinguish the interfaces listed in Section 9.2.2, as well as the expected users (that have to be consistent with Section 9.3.1) and connected devices.

9.3 Security perimeter

9.3.1 Users

1. SMGW:
   - The SMGW establishes a secure connection via TLS to the <TOE name> and provides a secured connection to the aEMT.
   - *<Indication of the Ethernet port to the SMGW>*
   - *Asset.Cert (r), <if applicable: further assets>*
2. <*if applicable:* Remote Administrator:>
   - *The administrator is responsible for configuration and secure operation of the TOE. <more detailed description of the user role>*
   - *<used interfaces>*
   - *<accessible assets/if applicable:* access rights>
3. <*if applicable:* Local Administrator:>
   - <description including used interfaces, accessible assets and *if applicable:* access rights>
   - ...
4. <*if applicable:* connected subsequent devices>
   - ...
5. <*if applicable*: users of the TOE>
   - ...

Implementation detail 16: The applicant shall provide a complete list of expected users, with descriptions, dedicated interfaces, accessible assets and privileges (e.g. access rights: read(r)/write(w)/execute(e)/delete(d)).

Implementation detail 17: If the TOE allows for anonymous use of certain functionality, where compromising the TOE is not possible and no critical configuration can be changed, the applicant shall include anonymous users. In this case, the accessible functionality shall be described in the 2nd column.

Implementation detail 18: The role of Administrator may be assumed by multiple entities or may be identical to one of the other users (e.g., the aEMT).

9.3.2 Assumptions

For the TOE to fulfil its security properties, the following assumptions[7] apply:

Assumption.CertifiedSMGW: The SMGW to which the TOE is connected is certified according to [BSI PP-0073] and [BSI TR-03109-1] and is operating in the certified state.

Assumption.TrustedAdmin: The Administrator of the TOE is trustworthy and well trained.

Assumption.TrustedDataHandling: Authorized users having access to or are receiving data from the TOE after the appropriate authentication and authorization are trustworthy (in the context of the data that they obtain).

Assumption.CertifiedUpdate: The firmware updates for the TOE, which can be provided by an authorized external entity, have a valid BSZ certificate for the GB "Komponenten im HAN des SMGW" before they are issued to show that the update is implemented correctly. The entity providing the update is trustworthy and ensure that no malware is introduced via a firmware update.

Assumption.PhysicalProtection: The TOE is installed in a non-public environment within the premises of the consumer, which provides a basic level of physical protection. In particular, this means:

- The Attacker.LocalPhys has limited physical access to the TOE. That is, the Attacker.LocalPhys has a limited total period of 10 minutes for trying to attempt an attack.
- The TOE is assumed to be inspected regularly by sight. This means that drilling, cutting, and milling attacks to permanently visible surfaces of the physical device can be neglected for an attack by Attacker.LocalPhys.

Assumption.Network: If devices connected to the TOE have a separate connection to parties in a Wide Area Network (besides using the communication channel of the SMGW provided by the TOE), this connection is appropriately protected.

Implementation detail 19: The applicant shall not add or alter assumptions.

Interpretation: Assumption.TrustedDataHandling does not exclude attacks in which an authenticated user tries to obtain data they are not authorized to access or otherwise gain additional rights (also known as privilege escalation).

Interpretation: The period of 10 minutes in Assumption.PhysicalProtection concerns the so-called window of opportunity for the attack at the TOE's installed location.

9.3.3 Assets

The TOE contains the assets described in Table 10.

ID	Asset	Description	Need for protection
Asset.PII	Personal identifiable information	Personal data according to GDPR. Any information relating to an identified or identifiable natural person. <detailed description of PII available on the TOE>	Confidentiality, Integrity, <*if applicable*: further needs for protection, e.g., those resulting from a data protection impact assessment according to GDPR>
Asset.Certs	Cryptographic certificates	Cryptographic material for verification of digital signatures.	Integrity, Authenticity

[7] Note that these assumptions are translated from the assumptions in [BSI TR-03109-5, Ch. 5] and are intended to be identical.

ID	Asset	Description	Need for protection
Asset.Keys	Cryptographic keys	Private key material for cryptographic operations of the TOE.	Confidentiality, Integrity, Authenticity
Asset.Config	Configuration data	Data containing configuration options for the operation of the TOE. This includes: <list of configuration present on the TOE> *Note: This includes for example access control rights as well as communication parameters such as Proxy IDs, network addresses of the SMGW or other entities in the HAN.*	Integrity, Authenticity
<*if applicable*: **Asset.ControlData**>	Control Data	Control Data for subsequent devices, steering their behavior or settings, generated by an authorized aEMT and provided via the CLS channel of the SMGW and the PUE to the corresponding device.	Integrity, Authenticity
Asset.AuthData	Authentication data (password hashes, cookies)	Data used by the TOE to authenticate its users. This includes: <list of authentication data present on the TOE> *Note: This might for example include user IDs, hashed passwords, session cookies or client certificates.*	Confidentiality, Integrity, Authenticity
Asset.FWUpdate	Firmware update	The binary representation suitable for storage and transmission of the data required to update the firmware.	Integrity, Authenticity
Asset.Time	System time	System time of the TOE. *Note: System time might be used for certificate validation.*	Integrity, Authenticity
Asset.SysLog	System log	Log of events that are relevant for the TOE or its security. The log is stored <append only/as a ring buffer/...> and has storage for at least <minimal duration for stored logs>. <*if applicable*: additional description of the system log>	Confidentiality, Integrity

ID	Asset	Description	Need for protection
<*if applicable*: additional asset IDs>	<*if applicable*: additional assets>	<*if applicable*: additional descriptions>	<*if applicable:* need for protection>

Table 10: Security perimeter – Assets[8]

Implementation detail 20: The applicant shall list any asset listed in Table 10 that is present on the TOE in the ST. The need for protection of any asset listed in the applicant's ST shall contain at least the needs for protection listed in Table 10 for said asset.

Implementation detail 21: Table 10 contains the minimal set of assets and security objectives. The applicant may add additional assets and security objectives for already established assets.

Note: Additional assets may be control data or sensor data.

9.3.4 Threat model: attackers

The threat model assumes the following attackers of the TOE:

- **Attacker.LocalIT**: An attacker with access to a local IT-interface of the TOE (e.g., an ethernet port).[9]
- <*if applicable:* **Attacker.Radio**: An attacker in range to use radio-based interfaces of the TOE (e.g., wM-Bus or Wi-Fi).>
- **Attacker.Remote**: An attacker in a Wide Area Network accessing the TOE via a remote interface (such as an LTE connection) or via a local IT-interface that is remotely available.
- **Attacker.LocalPhys**: An attacker with physical access to the TOE. The primary goal of this attacker is to circumvent the casing of the TOE to access undocumented interfaces (e.g., uncovering active debug ports or chip pins). The attacker only uses a selection of small-sized[10] tools that require little expertise to use and are easy to acquire[11]. This includes (but is not limited to) the following tools:
  - Screwdrivers
  - Heating guns, cooling sprays
  - Common solvents such as isopropyl alcohol or acetone
  - Soldering irons, wires, and clamps.
- <*if applicable*: additional attackers>

Interpretation: An attack of Attacker.LocalPhys is only considered successful if the manipulation of the TOE casing remains undetected.

Implementation detail 22: If the TOE provides any radio interface, the applicant shall include Attacker.Radio.

Implementation detail 23: The applicant shall not alter or remove attackers.
Note: If additional attackers are intended for the TOE, this shall be agreed with the certification body before the kick-off meeting.

[8] Note that this asset table is translated from the asset table in [TR-03109-5, Ch. 5] and is considered to be identical.
[9] This can be either via direct physical access to the respective interface or via the respective local network.
[10] i.e., tools that in total fit into a regular backpack.
[11] i.e., tools that can be acquired by a private customer.

9.3.5 Threat model: threats

The following threats are expected:

- **Threat.AccessFachanwendungsfälle (TR-03109-5)**: An attacker is getting access to Fachanwendungsfälle to manipulate the configuration of the TOE, to allow specific forbidden configurations.
- <*if applicable:* **Threat.AccessHAN**: An attacker uses the TOE, which is operated in a cascade or on a switch in the HAN, to access the HAN of the SMGW via the TOE such that the security of other HAN devices can no longer be guaranteed.>
- **Threat.AccessPhysical**: An attacker can access the local hood of the TOE such that the security of the TOE itself and the assets (confidentiality, integrity, or availability) stored on the TOE can no longer be guaranteed.
- <*if applicable:* **Threat.AccessRadio**: An attacker can access the radio-based interfaces via the TOE such that the security of other HAN devices can no longer be guaranteed.>
- **Threat.AuthenticationBypass**: An attacker is able to access the TOE without authentication.
- **Threat.CertsCompromise**: An attacker is sending modified cryptographic material for verification of digital signatures. The TOE is storing the cryptographic material and using it to verify the attacker with a valid digital signature.
- **Threat.CompromiseAssets**: An attacker breaches the confidentiality, integrity, or availability of an asset on the TOE, contrary to its need for protection.
- **Threat.ConfigurationManipulation**: An attacker is able to modify the TOE configuration without authentication.
- **Threat.DataManipulation**: An attacker is able to violate the integrity and confidentiality of transmitted data across the TOE.
- **Threat.DoS**: An attacker could try to overload the TOE with a high network traffic over a local, radio or WAN interface to compromise the communication with the SMGW or another CLS-device.
- **Threat.FirmwareManipulation**: An attacker is able to plant a malicious firmware to compromise the TOE.
- **Threat.MITM**: An attacker in the network channel (HAN, Radio) is able to read and manipulate the communication.
- **Threat.PrivateKeyCompromise**: An attacker is getting access to the TOE and retrieves the stored private keys.
- **Threat.TimeManipulation**: An attacker might try to modify the internal time (either directly or by manipulating the received external signal)
- <*if applicable*: additional threats>

Implementation detail 24: The applicant shall not alter or remove threats.

9.3.6 Security functions

The following security functions are present on the TOE in the configuration chosen for evaluation.

SF.Communication.SMGW: The TOE implements communication with the SMGW according to [BSI-TR-03109-3].[12]

SF.Phys.Protect: The TOE provides basic physical protection (tamper resistance) by <implemented basic protection against attacks from Attacker.LocalPhys>.

SF.Phys.TamperEvidence: The TOE provides tamper evidence against physical manipulation by <implemented tamper evidence>.

SF.Management.FirmwareUpdate: The TOE provides the functionality for a firmware update. Only the Administrator can initiate a firmware update. <*if applicable*: In addition, the TOE initiates a firmware update upon the following events: <events>.> The firmware update files are brought into the TOE in the following way: <description of import of firmware update files into the TOE>.

<further security functions>

Implementation detail 25: The applicant shall not remove security functions.

Implementation detail 26: The applicant shall model the basic physical protection used to mitigate threats by Attacker.LocalPhys. They may use the requirements for the TOE in Section 5.5 as a minimal set of requirements; however, further detail has to be included here on how the requirements are implemented in the TOE.

Implementation detail 27: The applicant shall specify the predefined security functions in this section and may add additional security-related functions for the TOE. I.e., functions the TOE uses to protect assets from the threats defined in Sect. 9.3.5 according to their needs (cf. Table 10). When possible, they shall reference technical information by referencing the appropriate standards.
Note: The structure of this section is left to the applicant. They may arrange the security functions e.g., within subsections.

9.3.7 Mapping

Threats	Attackers	Assets	Security Functions
<threats>	<associated attackers>	<affected assets>	<involved security functions>

Table 11: Mapping of threats, attackers, assets, and security functions

Implementation detail 28: In Table 11, the applicant shall provide a mapping that maps every possible combination of threats (cf. Sect. 9.3.5), attackers (cf. Sect. 9.3.4) and assets (cf. Sect. 9.3.3) to a (set of) security function(s) (cf. Sect. 9.3.6) that is able to mitigate the attack. For complex combinations, the applicant may also provide a short description of the attack and a rationale why the security function(s) counter the attack.[13]

9.4 Limits of evaluation

The following features, functions and services are outside the scope of the evaluation:

- <*if applicable:* The TOE security functions require <dynamic contents[14]> to operate. The <remote origin of the dynamic contents> providing the <dynamic contents> is not part of the evaluation.>

[12] In particular, this means that TLS shall be used according to [TR-03116-3, 4.2].
[13] Note, that there are of course combinations that may be disqualified by the basic design of the TOE (e.g., absence of the respective interface) or that are impossible by other means.
[14] Dynamic contents may e.g., be information or data from remote databases.

- <*if applicable:* The TOE uses the <PKI used by the TOE>. The PKI is not part of the evaluation.>
- <*if applicable*: function outside the scope of the evaluation>

Implementation detail 29: The applicant shall only exclude functions from the evaluation which are not essential for the purpose of the TOE. Furthermore, the TOE shall provide the means to deactivate the listed functions. In this state, the TOE shall be able to operate in accordance with its purpose. See [AIS B1] for more details.

9.5 Appendix: cryptographic specification

Note: The information in this appendix shall be provided in a separate deliverable and are not part of the ST.

9.5.1 List of cryptographic mechanisms

Table 12 contains a list of all cryptographic mechanisms used by the TOE, listed by interface, and including the security functionality they enforce.

Purpose	Cryptographic mechanism	Standard of implementation and application	Key size in bits
<name of logical interface for communication with or via the SMGW>			
cipher suites for TLS 1.2 for authenticity, authentication, key exchange, confidentiality, integrity	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, <*if applicable:* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384>, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, <*if applicable:* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384>	TLS 1.2: [RFC 5246] Cipher Suite: [RFC 5289] AES: [FIPS 197] CBC: [NIST SP800-38A] HMAC: [RFC 2104], GCM: [NIST SP800-38D] brainpoolPxyzr1: [RFC 7027] secpxyz1: [RFC 5114] SHA: [FIPS 180-4] [TR-03109-3]	AES: 128, 256 ECDHE_ECDSA: NIST P-256 (secp256r1), <*if applicable:* NIST P-384 (secp384r1)> brainpoolP256r1, brainpoolP384r1, <*if applicable:* brainpoolP512r1>
<*if applicable:* cipher suites for TLS 1.3	TLS_AES_128_GCM_SHA256, <*if applicable*: TLS_AES_256_GCM_SHA384,	TLS 1.3: [RFC 8446]	AES: 128, 256

Purpose	Cryptographic mechanism	Standard of implementation and application	Key size in bits
for authenticity, authentication, key exchange, confidentiality, integrity>	TLS_AES_128_CCM_SHA256 >	Cipher Suite: AES: [FIPS 197] CBC: [NIST SP800-38A] HMAC: [RFC 2104], GCM: [NIST SP800-38D] brainpoolPxyzr1: [RFC 7027] secpxyz1: [RFC 5114] SHA: [FIPS 180-4] [TR-03109-3]	ECDHE-ECDSA: secp256r1, <*if applicable:* secp384r1> brainpoolP256r1, brainpoolP384r1, <*if applicable:* brainpoolP512r1>
<random number generator / key generation>	<cryptographic mechanism>	<RFC / NIST / AIS ...>	<Key size> bits
<authenticity / authentication / key exchange / confidentiality / integrity / random number generator / key generation>	<cryptographic mechanism / cipher suite>	<RFC / NIST / AIS ...>	<Key size> bits

Table 12: List of cryptographic mechanisms

Implementation detail 30: The applicant shall provide a cryptographic specification for the cryptographic mechanisms that are used to enforce security functionality of the TOE. The cryptographic mechanisms shall be categorized by interfaces. Cf. [AIS B1] and [AIS B2] for more details.

Note: The ITSEF may support the applicant in creating this table (in accordance with [BSZ-Prüf, Chapter 5.2]). Please also consider the examples stated in [AIS B1].

Implementation detail 31: Regarding TLS 1.2, the standard of application contains additional information on the implementation of the protocol (e.g., for permitted extensions). The applicant should apply a similar procedure for the other cryptographic mechanisms.

9.5.2 Noise source description

<*if applicable:* The TOE contains a <physical/non-physical> noise source <name of the noise source> operating via <operating principle of the noise source> as described in <reference>. >

<*if applicable*: The noise source is certified according to CC <CC certification scheme> with certification ID <certification ID>.>

<*if applicable*: According to <source or justification> the random bits used for seeding have at least 125 bits of min-entropy.>

Implementation detail 32: If multiple noise sources are present in the TOE, the applicant shall repeat the above paragraph for each noise source.

<*if applicable*: Justification why the multiple noise sources are independent>

Implementation detail 33: If the cryptographic specification contains random number generators, the applicant shall provide a noise source description for the noise sources that are used for seeding (cf. [AIS B1] and [AIS B2] for more details).

Implementation detail 34: If multiple noise sources are present on the TOE, the applicant shall give a justification on why the multiple noise sources are independent.

9.5.3 Key management description

Table 13 contains a list of all keys used by the TOE, including their usage, key type, parameters, as well as information on the lifecycle and protection requirements.

Name	Usage	Type	Parameters	Lifecycle	Protection Requirements
<key name for firmware update signature verification>	Verification of the signature of the firmware update	<public key / certificate>	size: <size in Bits> Bits <*if applicable*: initialization vector, domain parameters, counters, further parameters>	The key is generated by <entity> on <event>. It is distributed to <entities>. The TOE stores this key <description of storage>. The key is valid for <validity period>. The key is destroyed by <destruction method> on <end of validity / other event>. <Description of relations to other keys>	Integrity, Authenticity, <*if applicable:* Confidentiality>

Name	Usage	Type	Parameters	Lifecycle	Protection Requirements
<key name>	<description and usage>	< <public/ private> key pair / symmetric key pair / ...>	size: <size in Bits> Bits <*if applicable*: initialization vector, domain parameters, counters, ...>	The key is generated by <entity> on <event>. It is distributed to <entities>. The TOE stores this key <description of storage>. The key is valid for <validity period>. The key is destroyed by <destruction method> on <end of validity / other event>. <Description of relations to other keys>	<*one or more of*: Confidentiality, Integrity, Authenticity>

Table 13: Key management description.

Implementation detail 35: The applicant shall provide a key management description containing information about cryptographic keys and parameters that are used by the TOE for cryptographic operations (cf. [AIS B1] and [AIS B2] for more details). The applicant should use Table 13 for that purpose.

Implementation detail 36: The applicant shall mention in the lifecycle description whether the key is part of a particular PKI.

9.6 <*if applicable:* Appendix: further information>