Federal Office
for Information Security

Application Notes and Interpretation of the Scheme (AIS)

AIS B3, Version 2.0

Date:	30.09.2023
Status:	Mandatory
Subject:	Requirements for user guidance
Document Owner:	Certification body of BSI
Distribution:	BSZ-Licensed Evaluation Facilities (ITSEFs) [1] BSI internal

[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	2021-10-01	SZ 33	1st edition
1.1	2022-05-18	SZ 33	Introduced labels for examples and notes Section 4 Comments moved to Section 3.2 renamed to Form of the Secure User Guidance Added requirement on configuration of operational environment
1.2	2023-06-01	SZ 33	Change to the new BSI document template Editorial changes
1.3	2023-09-30	SZ 33	Added content in the subsection 3.1.6 for the evaluation of software applications and applications in virtualised environments. Editorial changes

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 Background

1 The Security Target (ST) describes the Target of Evaluation (TOE) with its security functionality. The described security functionality relies on the secure configuration of the TOE and its operational environment. It is of the utmost importance that users are able to achieve this secure configuration. Otherwise, functionalities or interfaces might (not) be activated which would jeopardize the secure operation, since the security claim in the certificate is only valid in exactly the evaluated configuration.

2 The Secure User Guidance (SUG) is the documentation of the secure configuration. It can either be part of the user documentation or provided as a separate document.

2 Specific references

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 IAR, BSI

5 [AIS-B2] Requirements for the evaluation of cryptographic mechanisms according to the BSZ, BSI

6 [AIS-B4] Requirements for evaluation according to the BSZ, BSI

7 [AIS-B5] Guideline for determining the efforts for a BSZ evaluation, BSI

8 [AIS-B6] Requirements for a TOE, BSI

9 [BSZ-ETR] BSZ – Vorlage für den Evaluierungsreport, BSI

10 [BSZ-ADA] BSZ - Agenda der Auftaktbesprechung, BSI

3 Application notes and interpretation

3.1 Requirements for Secure User Guidance

3 The SUG shall fulfil the following requirements.

3.1.1 Comprehensive

4 The SUG addresses the users of the TOE. Thus, it is essential that it provides sufficient guidance to enable users to properly set up the TOE according to the secure configuration.
Note: The comprehensibility of a document includes the words chosen and the complexity of the information given. For example, if a non-expert is expected to set up the TOE, it might be necessary to avoid technical terms or clearly explain them at the beginning.

5 The language of the SUG depends on the language of the expected user. It might be necessary to provide the SUG in multiple languages.

6 The following guideline may be used:

a) Layperson, e.g. commercial off-the-shelf (COTS) products: no specific IT or information security skills and knowledge,

b) Experienced user, e.g. products sold for a certain well described user group: knowledge of main IT (but not necessarily information security) concepts in the domain of the product,

c) Administrator, e.g. products targeting professional managed environments: general and domain specific knowledge of IT and network concepts, ability to configure connected devices, not necessarily information security knowledge and skills.

3.1.2 Concise

7 The SUG shall be limited to the information necessary to set up the TOE according to the secure configuration as evaluated in the BSZ.

8 If the TOE offers other configurations, this information shall be provided in a different guidance, which might be linked from SUG, e.g. in the introduction.

3.1.3 Clearly separated from other information

9 The SUG shall be clearly separated from all other information about the TOE.
Note: "Clearly separated" does not imply that it needs to be a separate document, but the user needs to clearly understand where it starts and where it ends.

Example

10 *The installation handbook contains a chapter entitled "Installation in the secure and certified configuration" that encompasses the SUG and other chapters which provide information not relevant to the certified configuration.*

3.1.4 Unambiguous

11 The SUG shall unambiguously describe how to set up the TOE according to the secure and evaluated configuration.
Note 1: This might be as simple as turning the TOE on (e.g. it automatically enters the secure configuration, requesting all necessary credentials etc.) or might describe certain menu settings to be made or commands to be entered.

Note 2: Even minor mistakes might confuse users, e.g. when the label of the menu is different from the one described in the SUG or the colours are different in the pictures from those in reality.

3.1.5 Easy to find

12 The SUG shall be easy to find by the expected users, this includes the format chosen for the SUG.
Note: Problems might arise if, for example, the user receives many documents, possibly with similar content, or if the SUG uses a different format or medium than the remaining user information.

Example

13 *The user only receives one document and the first chapter is the SUG. Alternatively, the TOE guides the users automatically into the secure configuration.*

3.1.6 Include necessary information about the operational environment

14 In the case that the ST contains assumptions that give rise to requirements for the configuration of a specific part of the operational environment that are necessary to operate the TOE, the SUG shall include the guidance for the secure configuration of this part of the operational environment.
Note: In this context the operational environment refers to the conditions and factors in which a TOE operates. It encompasses various elements such as physical locations, network configurations, user activities and external influences.

For software applications and applications in virtualised environments:

15 The applicant shall specify the expected degree of hardening to the system environment. The use of established standards for determining the degree of hardening is desirable.
Note: In this context the system environment refers to the technical components and infrastructures necessary to set up a software application or application in a virtualised environment. The system environment means a subset of the operating environment, including hardware, software, configurations and protocols, necessary for the secure operation of the TOE.

16 If specific set-up measures in the system environment are necessary for the TOE to perform its security functionality, the applicant shall describe them, including guidance on how to set-up the measures.

3.1.7 References to risk information if deviating from the secure state

17 If the TOE can be operated in a state which deviates from the secure state, the SUG shall refer to further information that clearly state the end-user risk management.
Note: This might be a different chapter or another document.

Example

18 *The TOE might offer another interface, which is rarely used and is deactivated in the secure configuration (or excluded via assumption) and hence was not part of the evaluation. In this case, the vendor could provide another document (or even a continuously updated website) where the risks expected for this interface are described and mitigation information is given.*

19 This additional information is not part of the evaluation, only the fact that it exists at all.

3.2 Format of the Secure User Guidance

20 The SUG may be provided in a format and delivered on a medium suitable for the TOE. For example, it may be delivered with the TOE as a hard copy, as part of an online user help system, or on a separate medium. The SUG shall fulfil the requirements stated in Section 3.1 in any case.