Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS B3, Version 2.0

Datum:	01.03.2024
Status:	Verbindlich
Thema:	Anforderungen an die Benutzeranleitung
Herausgeber:	Zertifizierungsstelle des BSI
Verteiler:	Anerkannte BSZ-Prüfstellen (ITSEFs) [1] BSI-intern

[1]Alle Evaluatoren in den vom BSI für Prüfungen im Rahmen der BSZ anerkannten Prüfstellen.

Änderungshistorie

Version	*Datum*	*Herausgeber*	*Beschreibung*
2.0	01.03.2024	SZ 33	Deutsche Erstausgabe

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 247 1000
E-Mail: bsz@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Hintergrund

1 Das Dokument Sicherheitsvorgaben (Englisch: Security Target, ST) beschreibt den Evaluierungsgegenstand (Englisch: Target of Evaluation, TOE) einschließlich seiner Sicherheitsfunktionalität. Die beschriebene Sicherheitsfunktionalität basiert auf der sicheren Konfiguration des TOE und seiner Betriebsumgebung. Es ist notwendig, dass die Nutzerinnen und Nutzer diese sichere Konfiguration einrichten können. Anderenfalls könnten Funktionalitäten oder Schnittstellen (nicht) aktiviert sein, die den sicheren Betrieb gefährden können, da die im Zertifikat getroffene Aussage zur Sicherheit ausschließlich für die evaluierte Konfiguration gültig ist.

2 Das Handbuch zur sicheren Benutzung (Englisch: Secure User Guidance, SUG) ist die Dokumentation der sicheren Konfiguration. Es kann entweder als Bestandteil des Benutzerhandbuches oder als separates Dokument bereitgestellt werden.

2 Spezifische Referenzen

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] Anforderungen an ST und IAR, BSI

5 [AIS-B2] Anforderungen an die Evaluierung kryptographischer Mechanismen gemäß BSZ, BSI

6 [AIS-B4] Anforderungen an die Evaluierung gemäß BSZ, BSI

7 [AIS-B5] Anleitung zur Bestimmung des Aufwands für eine BSZ-Evaluierung, BSI

8 [AIS-B6] Anforderungen an einen TOE, BSI

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

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

3 Anwendungshinweise und Interpretationen

3.1 Anforderungen an das Handbuch zur sicheren Benutzung

3 Das SUG muss die folgenden Anforderungen erfüllen.

3.1.1 Umfassend

4 Das SUG richtet sich an die Nutzerinnen und Nutzer des TOE. Daher ist es essentiell, dass das SUG eine hinreichende Anleitung liefert, die die Nutzerinnen und Nutzer des TOE befähigt, den TOE entsprechend der sicheren Konfiguration einzurichten.
Hinweis: Die Verständlichkeit eines Dokuments wird durch die richtige Wortwahl und die angemessene Komplexität der bereitgestellten Informationen gefördert. Wenn beispielsweise davon ausgegangen werden kann, dass der TOE von einen technischen Laien eingerichtet wird, könnte es notwendig sein, den Gebrauch von Fachbegriffen zu vermeiden oder sie zu Beginn verständlich zu erklären.

5 Die im SUG verwendete Sprache hängt von der Sprache der erwarteten Nutzerinnen und Nutzer ab. Es könnte notwendig sein, das SUG in mehreren Sprachen bereitzustellen.

6 Die aus dem SUG resultierende Vorgabe muss von folgenden Personenkreisen verwendet werden können:

a) Laie, z. B. für handelsübliche Standardprodukte (Englisch: commercial off-the-shelf products, COTS-Produkte): Keine spezifischen Fähigkeiten und Kenntnisse in Bezug auf IT oder Informationssicherheit.

b) Erfahrener Nutzer, z. B. Produkte, die an eine bestimmte, eindeutig beschriebene Nutzergruppe verkauft werden: Kenntnisse der wichtigsten IT-Konzepte (jedoch nicht unbedingt in Informationssicherheit) im Bereich des Produkts.

c) Administrator, z. B. Produkte für professionell verwaltete Umgebungen: Allgemeine und domänenspezifische Kenntnisse der IT- und Netzwerkkonzepte, Fähigkeit zur Konfiguration angeschlossener Geräte, nicht unbedingt Kenntnisse und Fähigkeiten im Bereich der Informationssicherheit.

3.1.2 Präzise

7 Das SUG muss sich auf die Informationen beschränken, die für die Einrichtung des TOE gemäß der im Rahmen der BSZ evaluierten sicheren Konfiguration erforderlich sind.

8 Wenn der TOE andere Konfigurationen anbietet, müssen diese Informationen in einer anderen Anleitung bereitgestellt werden, auf die im SUG verwiesen werden könnte (z. B. in der Einleitung).

3.1.3 Klar getrennt von anderen Informationen

9 Das SUG muss von allen anderen Informationen über den TOE eindeutig getrennt sein.
Hinweis: „Eindeutig getrennt" bedeutet nicht, dass es sich um ein separates Dokument handeln muss, aber die Nutzerin oder der Nutzer muss klar verstehen, wo das SUG beginnt und wo es endet.

Beispiel

10 *Das Installationshandbuch enthält ein Kapitel mit dem Titel „Installation in der sicheren und zertifizierten Konfiguration", welches das SUG und weitere Kapitel umfasst, in denen Informationen enthalten sind, die für die zertifizierte Konfiguration nicht relevant sind.*

3.1.4 Eindeutig

11 Das SUG muss eindeutig beschreiben, wie der TOE gemäß der sicheren und evaluierten Konfiguration eingerichtet werden muss.
Hinweis 1: Dies könnte schlicht mit Einschalten des TOE erfolgen (z. B.: der TOE geht automatisch in die sichere Konfiguration über, fordert alle erforderlichen Anmeldeinformationen an usw.) oder aber durch die Beschreibung von bestimmten Menü-Einstellungen, die vorzunehmen sind, oder den Befehlen, die einzugeben sind.
Hinweis 2: Nutzerinnen und Nutzer können selbst durch kleine Fehler verwirrt werden, z. B. wenn die Beschriftung des Menüs von der Beschreibung im SUG abweicht oder die Farben auf den Bildern von denen tatsächlich verwendeten Farben abweichen.

3.1.5 Problemlos verfügbar

12 Das SUG muss für die erwarteten Nutzerinnen und Nutzer leicht zu finden sein. Dies umfasst auch das für das SUG gewählte Format.
Hinweis: Es kann zu Problemen kommen, wenn die Nutzerin oder der Nutzer beispielsweise viele Dokumente mit ggf. ähnlichem Inhalt erhält oder wenn für das SUG ein anderes Format oder Medium verwendet wird als für die übrigen Benutzerinformationen.

Beispiel

13 *Die Nutzerin oder der Nutzer erhält nur ein Anleitungsdokument und das erste Kapitel umfasst das SUG. Alternativ führt der TOE die Nutzerinnen und Nutzer automatisch in die sichere Konfiguration.*

3.1.6 Verfügbarkeit erforderlicher Informationen über die Betriebsumgebung

14 Für den Fall, dass das ST Annahmen enthält, die Anforderungen an die Konfiguration eines bestimmten Teils der Betriebsumgebung nach sich ziehen, die für den Betrieb des TOE erforderlich sind, müssen im SUG entsprechende Anweisungen für die sichere Konfiguration dieses Teils der Betriebsumgebung enthalten sein.
Hinweis: In diesem Zusammenhang bezieht sich die Betriebsumgebung auf die Bedingungen und Faktoren, unter denen der TOE arbeitet. Sie umfasst verschiedene Elemente wie physische Standorte, Netzwerkkonfigurationen, Benutzeraktivitäten und externe Einflüsse.

Für Softwareanwendungen und Anwendungen in virtualisierten Umgebungen:

15 Der Antragsteller muss den erwarteten Grad der Absicherung der Systemumgebung angeben. Die Verwendung etablierter Standards zur Bestimmung des Absicherungsgrades ist wünschenswert.
Hinweis: In diesem Zusammenhang bezieht sich die Systemumgebung auf die technischen Komponenten und Infrastrukturen, die notwendig sind, um eine Softwareanwendung oder eine Anwendung in einer virtualisierten Umgebung einzurichten. Die Systemumgebung bedeutet eine Teilmenge der Betriebsumgebung, einschließlich Hardware, Software, Konfigurationen und Protokolle, die für den sicheren Betrieb des TOE erforderlich sind.

16 Wenn spezifische Einrichtungsmaßnahmen in der Systemumgebung erforderlich sind, damit der TOE seine Sicherheitsfunktionalität ausführen kann, muss der Antragsteller diese beschreiben, einschließlich der Anleitung zur Einrichtung der Maßnahmen.

3.1.7 Risikohinweise bei etwaigen Abweichungen vom sicheren Zustand

17 Wenn der TOE in einem vom sicheren Zustand abweichenden Zustand betrieben werden kann, muss das SUG auf weitere Informationen verweisen, die eindeutig das Endbenutzer-Risikomanagement darlegen.
Hinweis: Hierbei könnte es sich um ein anderes Kapitel oder ein anderes Dokument handeln.

Beispiel

18 *Der TOE enthält möglicherweise eine weitere Schnittstelle, die selten genutzt wird und in der sicheren Konfiguration deaktiviert (oder per Annahme ausgeschlossen) ist und daher nicht Teil der Evaluierung war. In diesem Fall könnte der Anbieter ein weiteres Dokument (oder sogar eine fortlaufend aktualisierte Webseite) bereitstellen, wo die für diese Schnittstelle zu erwartenden Risiken beschrieben und Informationen zur Risikominderung zur Verfügung gestellt werden.*

19 Diese zusätzlichen Informationen selbst sind nicht Bestandteil der Evaluierung, sondern nur die Feststellung, dass sie überhaupt vorhanden sind.

3.2 Format des Handbuchs zur sicheren Benutzung

20 Das SUG kann in jedem Format und über jedes für den TOE geeignete Medium bereitgestellt werden. Beispielsweise kann es zusammen mit dem TOE als Druckfassung, als Teil eines Online-Benutzerhilfesystems oder auf einem separaten Medium bereitgestellt werden. Es muss jedoch in jedem Fall die in Abschnitt 3.1 genannten Anforderungen erfüllen.