Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

# Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS B5, Version 2.0

| | |
|---|---|
| Datum: | 01.03.2024 |
| Status: | Anleitung |
| Thema: | Anleitung zur Bestimmung des Aufwands für eine BSZ-Evaluierung |
| Herausgeber: | Zertifizierungsstelle des BSI |
| Verteiler: | Anerkannte BSZ-Prüfstellen (ITSEFs)[1]<br>BSI-intern<br>Webseite des BSI |

[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
© Bundesamt für Sicherheit in der Informationstechnik 2023

# Inhalt

# 1 Hintergrund

1 Vor der Durchführung einer BSZ-Produktevaluierung müssen sich die Prüfstelle für IT-Sicherheit (kurz Prüfstelle, Englisch: Evaluation Facility, ITSEF) und das BSI auf die Anzahl der für die Evaluierung benötigten Personentage einigen. Dieses Dokument enthält einige Richtwerte zur Berechnung dieser Zahl.

# 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 B3] Anforderungen an die Benutzeranleitung, BSI

7 [AIS B4] Anforderungen an die Evaluierung gemäß BSZ, 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 Allgemeine Hinweise

2 Diese Anleitung soll die Prüfstelle dabei unterstützen, die Anzahl der Personentage zu berechnen, die für die Durchführung einer Produktevaluierung eines bestimmten Evaluierungsgegenstand (Englisch: Target of Evaluation, TOE) erforderlich sind. Die Berechnung berücksichtigt dabei nicht den zusätzlichen Aufwand für die Vorbereitung (z. B. Schulungen, Einrichtung des TOE oder von Backend-Systemen), für die Erstellung von Reports und für die Dokumentation der Evaluierungsergebnisse im Evaluierungsreport (Englisch: Evaluation Technical Report, ETR). Laufzeiten automatisierter Tests sind ebenfalls nicht in diese Berechnung einzubeziehen.

3 Es liegt in der Verantwortung der Prüfstelle, die bereitgestellte Formel in geeigneter Weise anzuwenden. Die Prüfstelle kann von den empfohlenen Berechnungsgrößen abweichen, wenn sie dafür einen Grund sieht.

4 Das BSI wird das endgültige Berechnungsergebnis genehmigen oder ggf. Anpassungen verlangen.

5 Die Prüfstelle muss den geschätzten und den zusätzlichen Aufwand in der Auftaktbesprechung gesondert anführen und im Entwurf des initialen Zeitplans in angemessener Weise berücksichtigen (siehe Abschnitt 3.6). Der tatsächlich entstandene Aufwand für alle Evaluierungsaufgaben einschließlich Dokumentation ist im ETR und im Abschlussgespräch anzugeben (vgl. AIS B4 Unterabschnitte 3.2.1, 3.3.5 und 3.4.1).

6 Im Abschnitt 3.2 werden die in diesem Dokument relevanten Begriffe definiert. In den folgenden Abschnitten werden die vier Berechnungsschritte ausführlich beschrieben.

## 3.2 Definitionen

7 In diesem Dokument gelten die folgenden Definitionen:

8 Personentag (PT):
Eine Maßeinheit, die auf einem idealen Evaluierungsarbeit basiert, der von einer kompetenten und qualifizierten Person innerhalb von 8 Stunden geleistet wird (ohne Berücksichtigung von Pausen, Wartezeiten für Feedback, begrenzten Verfügbarkeiten usw.).

9 Schnittstelle:
Logische Verbindung zwischen der internen Verarbeitung des TOE und externen Instanzen (die menschlich oder technisch sein können).

**Beispiel**

10 *Management-Web-Schnittstelle, Dateneingabeschnittstelle.*

## 3.3 Schritt 1 - Ausgangswert

11 Start mit 25 PT + 10 PT (falls kryptographische Inhalte enthalten) als Grundwert.

## 3.4 Schritt 2 - Aufwandssteigernde und aufwandsmindernde Faktoren

12 Handelt es sich um eine **Rezertifizierung** oder **Reevaluierung**?
➜ -**3 PT**; falls kryptographische Inhalte unverändert bleiben, zusätzlich -**8 PT.**

13 Handelt es sich um eine **Rezertifizierung** oder **Reevaluierung** und liegt eine eindeutige Auswirkungsanalyse vor, die nur eine **begrenzte Anzahl gezielter Aktualisierungen** umfasst?
→ Zusätzlich -**3 PT**; falls kryptographische Inhalte nicht geändert wurden, zusätzlich -**5 PT**.

14 Verfügt die Prüfstelle über Protokoll-Testsuiten für die deutliche Mehrheit (> 60 %) der Protokolle?
→ -**5 PT**.

15 Falls das Vorstehende nicht zutrifft: verfügt die Prüfstelle über Protokoll-Testsuiten mit vollständiger Protokollabdeckung für einige Protokolle?
→ -**3 PT**.

16 Sind **mehr als drei Kommunikationsprotokolle** verfügbar?
→ +**3 PT** für jedes zusätzliche Kommunikationsprotokoll.

17 Existieren für den TOE-Typ **aktuelle Sicherheitspublikationen** (weniger als 3 Monate alt), die einen **zusätzlichen Evaluierungsaufwand** erfordern?
→ +**3 PT**.

18 Existieren **allgemeine Sicherheitspublikationen** (im Gegensatz zum vorherigen Punkt), die sich auf den TOE beziehen und **neue Angriffsvektoren** vorstellen, die in der Praxis nutzbar sind?
→ +**3 PT**.

19 Verfügt der TOE über **mehr als fünf Schnittstellen** (die im ST enthalten sind oder aufgrund der Angriffspfade einer Evaluierung bedürfen)?
→ +**2 bis** +**3 PT** für jede einzelne **zusätzliche Schnittstelle** (d. h. Schnittstellen, die mehrmals vorkommen, zählen nur einmal).

20 Ist der TOE mit **proprietären Modulen** ausgestattet, auf die **über Schnittstellen zugegriffen werden kann**, auf die potenzielle Angreifer direkt zugreifen können?
→ +**2 PT** für jedes solche Modul.

21 Setzt der TOE eine **unveränderte**, allgemein bekannte **Kryptobibliothek** ein (im Zweifelsfall wenden Sie sich an das BSI)?
→ -**3 PT**.

22 Ist ein Kommunikationsprotokoll (Version) verfügbar, das vor weniger als sechs Monaten veröffentlicht wurde?
→ +**3 PT**.

23 Benötigt der TOE eine **komplexe Betriebsumgebung**, z. B. Kommunikation mit Back-End-Systemen, Anbindung an ein Bussystem oder weitere Spezialhardware?
→ **+1 bis +2 PT.**

24 Verfügt die Prüfstelle **bereits über Erfahrungen** oder liegt ihr ein triftiger Grund vor, die einen **erhöhten** oder **geringeren Evaluierungsaufwand** für diesen TOE vermuten lassen?
→ Der Arbeitsaufwand bedarf einer **Einzelfallentscheidung** und muss in der Begründung berücksichtigt werden.

## 3.5 Schritt 3 - Begrenzende Faktoren

25 Handelt es sich um eine **Erstzertifizierung** einschließlich **Verschlüsselungsverfahren** und beläuft sich die Gesamtzahl der Tage auf < 25 PT?
→ **25 PT** einstellen.

26 Handelt es sich um eine **Erstzertifizierung** ohne **Verschlüsselungsverfahren** und beläuft sich die Gesamtzahl der Tage auf < 15 PT?
→ **15 PT** einstellen.

27 Handelt es sich um eine Rezertifizierung **mit mehr als 10 sicherheitsrelevanten Änderungen** und beläuft sich die Gesamtzahl der Tage auf < 10 PT?
➜ **10 PT** einstellen.

28 Beläuft sich die **Gesamtzahl der Personentage** > **50 PT**?
➜ Das BSI kontaktieren und um ein Bewertungsgespräch mit dem Antragsteller und dem BSI ersuchen.

## 3.6 Schritt 4 – Erstellung des initialen Zeitplans

29 Den Entwurf des initialen Zeitplans (Zuordnung von Personentagen und Kalendertagen, Berücksichtigung von weiteren Arbeiten, Feiertagen, erwarteten Gerätelaufzeiten, der Verfügbarkeit von Evaluatoren, möglichen Parallelisierung usw.) auf Grundlage der berechneten Anzahl der Personentage erstellen.