Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS B2, Version 2.0

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

Inhalt

1 Hintergrund

1 Dieses Dokument enthält Anforderungen an die Evaluierung kryptographischer Mechanismen im Rahmen der BSZ und richtet sich an die Evaluatorinnen und Evaluatoren der BSZ-Verfahren. Um eine vollständige Zusammenstellung der Anforderungen zur Evaluierung kryptographischer Mechanismen sicherzustellen, sind einige in diesem Dokument enthaltenen Anforderungen möglicherweise auch in anderen BSZ-Dokumenten zu finden.

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-B3] Anforderungen an die Benutzeranleitung, 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

3 Anwendungshinweise und Interpretationen

3.1 Eingaben der Antragstellerin

2 In diesem Abschnitt werden die Eingaben der Antragstellerin beschrieben, die für die Evaluierung kryptographischer Mechanismen erforderlich ist. Die Eingaben umfassen die Bereitstellung von Unterlagen und des Evaluierungsgegenstands (Englisch: Target of Evaluation, TOE).

3.1.1 Unterlagen

3 Die Antragstellerin muss die in [BSZ-Prod], [AIS-B1] und [AIS-B3] beschriebenen Unterlagen vorlegen. Der Vollständigkeit halber werden in diesem Unterabschnitt alle erforderlichen Antragstellerunterlagen aufgeführt und die Anforderungen an die kryptographische Spezifikation werden in gleicher Weise aufgeführt wie in [AIS-B1].

Sicherheitsvorgaben und Handbuch zur sicheren Benutzung

4 Die Antragstellerin muss das Dokument Sicherheitsvorgaben (Englisch: Security Target, ST) (gemäß [AIS-B1]), ein Handbuch zur sicheren Benutzung (Englisch: Secure User Guidance, SUG) (gemäß [AIS B3]) und einen Überblick über die TOE-Architektur vorlegen. Im Falle einer Reevaluierung oder Rezertifizierung muss die Antragstellerin außerdem eine Änderungsbeschreibung mit Auswirkungsanalyse (Englisch: Impact Analysis Report, IAR) (gemäß [AIS-B1]) vorlegen.

Kryptographische Spezifikation

5 Die Antragstellerin muss für die kryptographischen Mechanismen, die zur Gewährleistung der Sicherheitsfunktionalität des TOE verwendet werden, eine kryptographische Spezifikation vorlegen. Eine Übersicht über die verwendeten kryptographischen Mechanismen ist in Form der in Abschnitt 4 angeführten Tabelle bereitzustellen. Die kryptographische Spezifikation muss als separates Dokument mit der Bezeichnung „Krypto-Anhang“ bereitgestellt werden und die in den Zeilen 6–8 genannten Inhalte enthalten. Es darf nicht als ein Anhang zum Dokument Sicherheitsvorgaben bereitgestellt werden.

Hinweis: Zu den kryptographischen Mechanismen können unter anderem (symmetrische/asymmetrische) Verschlüsselungsverfahren, Hashfunktionen, Message Authentication Codes, (passwortbasierte) Schlüsselableitungsfunktionen, digitale Signaturverfahren, Schlüsselerstellungsverfahren, (symmetrische/asymmetrische) Verifikation der Quelle [und Integrität] von Daten, (symmetrische/asymmetrische) Verfahren zur Authentisierung von Instanzen, Verfahren für die authentifizierte Verschlüsselung, passwort-authentifizierte Verfahren zur Schlüsselerstellung, Verfahren für Secret-Sharing, kryptographische Protokolle und deterministische Zufallszahlengeneratoren gehören.

6 Die vom TOE verwendeten kryptographischen Mechanismen sollten den vereinbarten Algorithmen aus dem SOG-IS-Katalog entsprechen[SCES-ACM]. Abweichende Mechanismen (insbesondere kryptographische Protokolle) müssen vor Beginn der Evaluierung von der Zertifizierungsstelle genehmigt werden. Von der Zertifizierungsstelle empfohlene kryptographische Protokolle umfassen die Empfehlungen der Technische Richtlinie [BSI-TR-02102] (Teile 2–4).

7 Die Beschreibung eines kryptographischen Mechanismus muss nach Schnittstellen kategorisiert sein und die folgenden Informationen enthalten:

- Verweise auf verfügbare Normen, die den Mechanismus eindeutig definieren, zusammen mit ausgewählten Optionen oder Parametern (z. B. Schlüssellängen, Domänenparameter usw.).

- Die vom Mechanismus erzwungene Sicherheitsfunktionalität (Zuordnung zu den im Dokument Sicherheitsvorgaben vorgegebenen Sicherheitsfunktionen).
- Das durch den Mechanismus erreichte Sicherheitsziel (Vertraulichkeit, Integrität, Authentizität usw.).

8 Die Definition eines kryptographischen Verfahrens oder Protokolls erfordert üblicherweise die Definition mehrerer Algorithmen (z. B. erfordern Verschlüsselungsverfahren die Definition eines Schlüsselgenerierungsalgorithmus, eines Verschlüsselungsalgorithmus und eines Entschlüsselungsalgorithmus).

Beschreibung der Rauschquelle

9 Wenn in der kryptographischen Spezifikation Zufallszahlengeneratoren enthalten sind, muss die Antragstellerin für die Rauschquellen, die zum Seeding verwendet wurden, im „Krypto-Anhang“ ein Kapitel zur Rauschquellenbeschreibung einfügen.

10 Die Beschreibung einer Rauschquelle sollte Informationen zu deren Art (physikalisch oder nicht-physikalisch) und zur Wirkungsweise enthalten.

11 Wenn mehrere Rauschquellen verwendet werden, muss eine Begründung dafür vorgelegt werden, dass die Quellen unabhängig sind.

12 Die Beschreibung der Rauschquelle sollte eine Begründung dafür enthalten, dass die zum Seeding verwendeten Zufallsbits eine Mindestentropie von mindestens 125 Bits aufweisen. Bei Verwendung eines CC-zertifizierten physikalischen Zufallszahlengenerators genügt ein Verweis auf die Zertifizierungs-ID.

Beschreibung des Schlüsselmanagements

13 Die Antragstellerin muss eine Beschreibung des Schlüsselmanagements in Form eines Kapitels im „Krypto-Anhang“ vorlegen, in dem die Informationen über kryptographische Schlüssel sowie Parameter enthalten sind, die vom TOE für kryptographische Verfahren verwendet werden.

14 Die Beschreibung eines Schlüssels sollte Informationen über seinen Typ sowie seine Erzeugung, Verteilung, Verwendung, Speicherung, Zerstörung, Gültigkeitsdauer und Schutzanforderungen enthalten.

15 Die Beschreibung des Schlüsselmanagements muss zudem Informationen zu anderen relevanten Parametern enthalten, einschließlich Domänenparameter, Initialisierungsvektoren, Zähler und Tweaks.

16 Die Beschreibung des Schlüsselmanagements muss die zwischen Schlüsseln bestehenden hierarchischen Beziehungen hervorheben (z. B. ob ein Schlüssel von einem anderen Schlüssel abgeleitet ist oder ob ein Schlüssel mit einem anderen Schlüssel verschlüsselt ist).

Implementationsdarstellung

17 Die Antragstellerin muss der Prüfstelle für IT-Sicherheit (kurz Prüfstelle) für die kryptographischen Mechanismen, die zur Gewährleistung der Sicherheitsfunktionalität des TOE verwendet werden, eine Implementationsdarstellung vorlegen. Kann die Antragstellerin die Implementationsdarstellung für einen oder mehrere kryptographische Mechanismen nicht vorlegen, muss dies vor Beginn der Evaluierung mit der Zertifizierungsstelle erörtert werden.

18 Die Implementationsdarstellung sollte den Quellcode oder den Pseudocode umfassen. Bei Bereitstellung des Quellcodes muss es sich um den Code handeln, der bei der Erstellung des TOE verwendet wurde. Sollte ein Pseudocode bereitgestellt werden, muss dieser einen Detaillierungsgrad

aufweisen, der der tatsächlichen Implementierung sehr ähnlich ist (insbesondere muss er Seitenkanal-Gegenmaßnahmen umfassen, falls solche Maßnahmen implementiert wurden).

19 Die Implementationsdarstellung muss die Implementierung der kryptographischen Funktionalität selbst sowie jene Teile der Implementierung abdecken, in denen die kryptographische Funktionalität aufgerufen wird.

20 Wenn bei der Implementierung quelloffene kryptographische Bibliotheken verwendet werden, muss die Implementationsdarstellung Informationen über deren Herkunft, die Version und alle von der Antragstellerin vorgenommenen Änderungen enthalten.

3.1.2 Evaluierungsgegenstand

21 Die Antragstellerin legt der Prüfstelle den TOE zur Evaluierung vor. Dies umfasst eine für Prüfungen geeignete Konfiguration des TOE und seiner Betriebsumgebung.

Hinweis: Einzelheiten und weitere Regelungen sind unter [BSZ-Prod], [BSZ-EP] und [AIS-B4] zu finden.

22 Die Antragstellerin kann für die Firmware des TOE einen Simulator zu Prüfzwecken zur Verfügung stellen.

3.2 Evaluierungsmethodologie

23 Die kryptographische Evaluierung der BSZ setzt sich aus einer Konformitätsbewertung und einer Schwachstellenanalyse zusammen.

Konformitätsbewertung und Schwachstellenanalyse

24 Das Ziel der Konformitätsbewertung im Rahmen der kryptographischen Evaluierung der BSZ besteht in der Bestimmung, ob die kryptographischen Mechanismen des TOE mit den SCES (SOG-IS Crypto Evaluation Scheme) und BSI-Richtlinien im Einklang stehen und dass die Implementierung des TOE mit den Dokumentationsunterlagen der Antragstellerin übereinstimmt.

25 Das Ziel der Schwachstellenanalyse im Kontext der BSZ-Krypto-Evaluierung besteht in der Feststellung, dass die kryptographische Implementierung keine ausnutzbaren Implementierungsschwächen enthält. Um potenzielle Fehler in der Implementierung zu identifizieren, sollten die Evaluatorinnen und Evaluatoren ihre Erfahrung und alle ihnen zur Verfügung stehenden Informationen nutzen. Insbesondere sollten die Evaluatorinnen und Evaluatoren bereits während der Konformitätsbewertungsaktivitäten nach potenziellen Schwachstellen suchen.

26 Die Prüfstelle muss jede festgestellte Nichtkonformität im Prüfbericht (Englisch: Evaluation Technical Report, ETR) vermerken.

27 Die Prüfstelle muss Workunit 1 gemäß Abschnitt 6.12 [FiT CEM] (6.12.4.1) durchführen.

28 Die Prüfstelle muss die Beschreibung der Rauschquelle überprüfen, um zu bestimmen, ob die Entropieangabe des Antragstellers plausibel ist.

29 Die Prüfstelle muss Workunit 2 gemäß Abschnitt 6.12 [FiT CEM] (6.12.4.1) durchführen.

30 Die Konformitätstests sollten eine hohe Abdeckung der extern zugänglichen kryptographischen Algorithmen, Schemata und Protokolle erreichen.

31 Standardisierte kryptographische Protokolle, die für die Kommunikation über externe Schnittstellen verwendet werden, sollten mit automatisierten Testwerkzeugen getestet werden, um Evaluationszeit für Aspekte zu sparen, die menschliche Analyse erfordern.

32 Die Prüfstelle sollte die folgenden öffentlich verfügbaren Informationsquellen berücksichtigen:

- SCES-Richtlinien: [SCES-ACM]
- BSI-Richtlinien: [BSI-TR-02102], [BSI-RSA], [BSI-ECC], [BSI-TR-03116], [BSI-TR-03109],
- Sicherheitsüberlegungen in kryptographischen Standards,
- Wissenschaftliche Literatur,
- CVE-Einträge, Sicherheitsmitteilungen von CERTs oder Herstellern, Änderungsprotokolle von kryptographischen Bibliotheken, Blogs von Sicherheitsforschern,
- Informationen zu potenziellen Schwachstellen, die von der Zertifizierungsstelle selbst bereitgestellt werden.

33 Die Prüfstelle sollte die folgenden Arten von Angriffen in Betracht ziehen:

- Umgehung der kryptografischen Funktionalität,
- Logische Angriffe,
- Reaktions-/Orakel-Angriffe,
- Timing-Angriffe.

34 Die Prüfstelle muss die Auswirkungen der Betriebsumgebung der TOE auf die Identifizierung potenzieller Schwachstellen berücksichtigen.

Hinweis: Schwachstellen in kryptografischen Implementierungen können aufgrund von Missbrauch von Mechanismen, Implementierungsschwächen/Fehlern oder Seitenkanälen entstehen. Ob eine Schwachstelle oder ein Seitenkanal zu einem Angriff führt, hängt unter anderem von der Fähigkeit des Angreifers ab, in der Betriebsumgebung des TOE zu agieren. Dies könnte zu weiteren Arten von Angriffen führen, z. B.:

- *Seitenkanalangriffe: Stromverbrauch, elektromagnetische Abstrahlung, Schallemission usw.,*
- *Fehlerangriffe (Fault attacks),*
- *Mikroarchitektonische Angriffe: Cache-Angriffe, Vorhersage von Sprüngen (branch prediction), spekulative Ausführung (speculative execution) usw.,*
- *Kaltstartangriffe (cold boot attacks).*

Penetrationstest

35 Das Ziel von Penetrationstests besteht in der Bestimmung, ob die kryptografische Implementierung Angriffen widersteht, d. h. ob die kryptografische Implementierung keine Schwachstellen enthält, die von Angreifern mit "erweitert einfachem" (Englisch: enhanced-basic) Angriffspotenzial ausgenutzt werden könnten [FiT CEM] (5.4).

36 Die Prüfstelle muss versuchen, die kryptographische Sicherheitsfunktionalität zu umgehen oder zu durchbrechen. Die Evaluatiorin oder der Evaluator muss hierfür unter Berücksichtigung der für diesen Schritt vorgesehenen Zeit eine risikobasierte Stichprobenstrategie aufstellen. Die Teststrategie muss auf den Ergebnissen vorangegangener Evaluierungsschritte basieren, einschließlich der Konformitätsbewertung, der Identifizierung potenzieller Mängel und der in [AIS-B4] beschriebenen Evaluierungsschritte.

37 Die Teststrategie muss fortlaufend aktualisiert werden, insbesondere, wenn Ergebnisse (einschließlich der Ergebnisse aus den anderen Schritten) verfügbar werden. Sollte für diesen Schritt mehr Zeit benötigt werden als ursprünglich vorgesehen, muss die Prüfstelle dies dokumentieren und im ETR entsprechend begründen.

4 Tabelle der kryptographischen Mechanismen

1. Zweck	*2. Kryptographischer Mechanismus*	*3. Implementierungsnorm*	*4. Schlüsselgröße in Bit*
Trusted Channel an ... über HTTPS mit TLS 1.3 [RFC 8446]			
Authentizität	RSA-Signaturerstellung und -verifizierung (RSASSA-PSS) mittels SHA-256	[PKCS#1 v2.2] (RSA), [FIPS 180-4] (SHA)	Modullänge = 2048
Authentifizierung	RSA-Signaturerstellung und -verifizierung (für RSASSA-PSS)	[RFC 5246] (TLS) [RFC 3447] (PKCS#1 v2.1)	3072, 4096
Schlüsselvereinbarung	Elliptische Kurven (ECDHE): secp256r1, secp384r1	[RFC 5246] (TLS) [RFC 8422] (TLSECC) [IEEE P1363] (ECDH)	256, 384
Schlüsselvereinbarung	DHE- Gruppen: ffdhe3072, ffdhe4096	[RFC 5246] (TLS) [RFC 7919] (DHE)	3072, 4096
Vertraulichkeit	AES in GCM-Modus	[RFC 5246] (TLS) [RFC 5288] (AESGCM) [RFC 5289] (AES-GCM) [FIPS 197] (AES) [SP800-38D] (GCM)	128, 256
Vertraulichkeit	AES in CBC-Modus	[RFC 5246] (TLS) [FIPS 197] (AES) [SP800-38A] (CBC)	128, 256
Integrität	HMAC mit SHA-2	[RFC 5246] (TLS) [FIPS 180-2] (SHA)	256, 384
Zufallszahlengenerator	Deterministischer RNG DRG.3	[AIS-20]	
Trusted Channel an Command Line Interface (CLI) mit SSH [4251]			
Schlüsselaustausch	diffie-hellman-group15-sha512	[RFC 4253] (Schlüsselaustauschverfahren) [RFC 8268] (mehr DH für SSH) [RFC 3526] (Gruppenspezifikation)	3072
Authentifizierung	Elliptic Curve Digital Signature Algorithm mit SHA-256 und nistp256 (ecdsa-sha2-256)	[RFC 5656]	256
Vertraulichkeit	AES in CTR-Modus	[RFC 4344] (SSH Encryption Modes)	128, 192, 256
Integrität	HMAC mit SHA-2 (hmac-sha2-256)	[RFC 4253] (SSH) [RFC 6668] (SHA-2-Integration) [RFC6234] (SHA-2-Definition)	256
Zufallszahlengenerator	/dev/urandom		

Tabelle 2: Beispiel für eine Tabelle mit kryptographischem Mechanismus

5 Referenzdokumente

1 [FiT CEM] Zeitlich festgelegte Cybersicherheitsevaluations-methodologie für IKT-Produkte (Fixed-time cybersecurity evaluation methodology for ICT products, FiT CEM), EN 17640:2022

2 [SCES-ACM] SOG-IS Crypto Evaluation Scheme, Agreed Cryptographic Mechanisms, aktuelle Version

3 [BSI-TR-02102] Technischen Richtlinien der Serie BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI

4 [BSI-RSA] RSA-Leitfaden: Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_BSI_guidelines_SCA_RSA_V1_0_e_pdf.pdf?__blob=publicationFile&v=1

5 [BSI-ECC] ECC-Leitfaden: Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations, BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_ECCGuide_e_pdf.pdf?__blob=publicationFile&v=3

6 [BSI-TR-03116] Technischen Richtlinien der Serie BSI-TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung, BSI

7 [BSI-TR-03109] BSI TR-03109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb, BSI

8 [AIS-20] Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, BSI