Ciphermeter · Leseprobe

Kryptokonzept

Vorlage zum Ausfüllen: Konzept und Verfahren für den Einsatz kryptographischer Verfahren

Einrichtung	[Name der Einrichtung]
Dokumentversion	[z. B. 1.0]
Verantwortlich für das Dokument	[Rolle, z. B. Informationssicherheitsbeauftragte/r]
Freigegeben durch / am	[Geschäftsleitung] / [Datum]
Nächster Prüftermin	[Datum, spätestens nach Erscheinen der nächsten TR-02102-1]
Stand der Algorithmenliste	BSI TR-02102-1, Version 2026-01 (Stand 23.01.2026)
Gliederung orientiert an	§ 30 Abs. 2 Nr. 8 BSIG; Anhang Nr. 9 der Durchführungsverordnung (EU) 2024/2690

Was diese Leseprobe enthält: Teil A (Rahmen) vollständig und aus Teil B das Kapitel 3.1 (symmetrische Verschlüsselung). Die Leseprobe dürfen Sie im eigenen Unternehmen verwenden und anpassen.

Was das vollständige Paket zusätzlich enthält: Teil B vollständig (Schutzbedarf-Matrix, Protokolle, Hash/MAC, asymmetrische Verfahren und Schlüsseleinigung, Zufallszahlen, ausgeschlossene Verfahren, Krypto-Agilität und Post-Quanten-Umstieg, Ausnahmen), Teil C Schlüsselmanagement (Nr. 9.2 c i–xii), Teil D Überprüfung, ein eigenes Dokument zum Schlüssel-Lebenszyklus, Krypto-Inventar und Ausnahmeregister als Tabelle sowie eine Ausfüllhilfe mit Zuordnungstabelle (BSIG, Durchführungsverordnung, IT-Grundschutz CON.1, ISO/IEC 27001:2022 A.8.24).

So lesen Sie die Vorlage: [gelb markierte Felder] füllen Sie aus. Kursive Absätze sind Hinweise zum Ausfüllen und werden vor der Freigabe gelöscht. Diese Vorlage ist nicht vom BSI geprüft oder anerkannt und ersetzt keine Rechtsberatung (siehe letzte Seite).

Teil A – Rahmen

1. Zweck und Geltungsbereich

Dieses Dokument legt fest, wie [Name der Einrichtung] kryptographische Verfahren einsetzt: welche Verfahren und Schlüssellängen zugelassen sind, wie Schlüssel erzeugt, verteilt, gespeichert, gewechselt und vernichtet werden und wie das Konzept überprüft wird. Ziel ist, Vertraulichkeit, Authentizität und Integrität von Daten entsprechend ihrem Schutzbedarf zu schützen.

Geltungsbereich: [Standorte, Organisationseinheiten, IT-Systeme und Dienste, z. B. „alle IT-Systeme der Einrichtung einschließlich ausgelagerter Dienste, soweit sie Daten der Einrichtung verarbeiten"]. Ausgenommen: [z. B. Systeme in fremder Verantwortung, für die vertragliche Regelungen gelten].

Bezug: Das Dokument dient der Umsetzung von

> § 30 Abs. 2 Nr. 8 BSIG: „Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren"

und orientiert sich in der Gliederung an Anhang Nr. 9 der Durchführungsverordnung (EU) 2024/2690:

> „9.1. Für die Zwecke von Artikel 21 Absatz 2 Buchstabe h der Richtlinie (EU) 2022/2555 legen die betreffenden Einrichtungen ein Konzept und Verfahren in Bezug auf Kryptografie fest, setzen sie um und wenden sie an, um eine angemessene und wirksame Nutzung von Kryptografie sicherzustellen, damit die Vertraulichkeit, Authentizität und Integrität der Daten im Einklang mit der Anlagen- und Werteklassifizierung der betreffenden Einrichtungen und den Ergebnissen der gemäß Nummer 2.1 durchgeführten Risikobewertung geschützt sind."

Hinweis zum Ausfüllen: Die Durchführungsverordnung (EU) 2024/2690 ist nur für die Einrichtungsarten verbindlich, die in ihrem Art. 1 genannt sind (u. a. DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-, Rechenzentrums- und Content-Delivery-Dienste, Managed Service Provider und Managed Security Service Provider, Online-Marktplätze, Online-Suchmaschinen, Plattformen für soziale Netzwerke, Vertrauensdiensteanbieter). Für alle anderen Einrichtungen ist die Gliederung eine Orientierung, keine Vorgabe. Ob und in welcher Form das BSIG für Ihre Einrichtung gilt, beurteilt diese Vorlage nicht. Streichen Sie den zweiten Bezug, wenn Sie ihn nicht verwenden wollen.

Maßstab für Verfahren und Schlüssellängen: BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen", Version 2026-01, für Protokolle zusätzlich TR-02102-2 (TLS), TR-02102-3 (IPsec) und TR-02102-4 (SSH) in der jeweils [genannten / aktuellen] Fassung. Die TR-02102-1 spricht ihre Empfehlungen nur für einen Zeitraum bis Ende 2032 aus (TR-02102-1, Abschnitt 1.2, S. 21); das Konzept wird deshalb mindestens jährlich überprüft (Teil D).

Mitgeltende Dokumente: [Leitlinie zur Informationssicherheit], [Schutzbedarfsfeststellung / Klassifizierungsrichtlinie], [Risikobewertung], Krypto-Inventar (Anlage), Ausnahmeregister (Anlage), Dokument „Schlüssel-Lebenszyklus".

2. Rollen und Zuständigkeiten

Rolle	Aufgaben in diesem Konzept	Besetzung
Geschäftsleitung	gibt das Konzept frei, stellt Mittel bereit, entscheidet über Ausnahmen mit hohem Restrisiko	[Name/Funktion]
Informationssicherheits-beauftragte/r (ISB)	pflegt das Konzept, verfolgt Änderungen der TR-02102, prüft Ausnahmen, berichtet an die Geschäftsleitung, plant die Überprüfung (Teil D)	[Name]
IT-Betrieb	setzt die Festlegungen in Systemen um (z. B. TLS-Konfiguration, Festplattenverschlüsselung), pflegt das Krypto-Inventar, meldet Abweichungen	[Team/Name]
Schlüsselverantwortliche	verantworten je Schlüssel bzw. Schlüsselsystem Erzeugung, Speicherung, Wechsel, Widerruf und Vernichtung (Teil C)	je Eintrag im Krypto-Inventar
Einkauf / Dienstleistersteuerung	nimmt die Festlegungen in Ausschreibungen und Verträge mit Dienstleistern auf	[Name]
Datenschutz	wird bei Verfahren beteiligt, die personenbezogene Daten schützen	[Name]

Hinweis zum Ausfüllen: In kleinen Einrichtungen fallen Rollen oft zusammen. Halten Sie trotzdem fest, wer welche Aufgabe hat; unbesetzte Rollen sind ein Befund für die Risikobewertung.

3. Begriffe

Begriff	Bedeutung in diesem Dokument
Schutzbedarf	Einstufung von Daten und Systemen nach den möglichen Schäden bei Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit. Kategorien: [z. B. normal / hoch / sehr hoch, wie in Ihrer Schutzbedarfsfeststellung].
Kryptographisches Verfahren	Algorithmus mit festgelegten Parametern (z. B. AES-256 im GCM-Modus), eingesetzt in einem Protokoll oder einer Anwendung.
Zugelassenes Verfahren	Verfahren, das nach Teil B dieses Konzepts ohne Ausnahme eingesetzt werden darf.
Ausnahme	befristeter, begründeter und freigegebener Einsatz eines nicht zugelassenen Verfahrens; steht im Ausnahmeregister.
Kryptoperiode	Zeitraum, in dem ein Schlüssel verwendet werden darf; danach wird er gewechselt oder deaktiviert (Teil C, Nr. 9.2 c xii).
Krypto-Inventar	Verzeichnis, wo welche Verfahren, Schlüssel und Zertifikate eingesetzt werden; Grundlage für Wechsel und Umstieg.
Krypto-Agilität	Fähigkeit, ein Verfahren oder eine Schlüssellänge ohne grundlegenden Umbau des Systems auszutauschen (Nr. 9.2 b).
AEAD	Authenticated Encryption with Associated Data: Verschlüsselung, die zugleich die Daten authentisiert, z. B. AES-GCM (TR-02102-1, Bemerkung 3.1).
KEK	Key Encryption Key: Schlüssel, der anderes Schlüsselmaterial bei Transport oder Speicherung schützt (Key-Wrapping).

Begriff	Bedeutung in diesem Dokument
Hybrides Verfahren	Kombination eines klassischen mit einem quantensicheren Verfahren, sodass die Sicherheit erhalten bleibt, solange eines der beiden sicher ist.
„Store now, decrypt later“	Angriff, bei dem verschlüsselte Daten heute gespeichert und später, etwa mit einem Quantencomputer, entschlüsselt werden (TR-02102-1, Abschnitt 2.1).

Teil B – Festlegungen (Auszug)

Im vollständigen Paket: Kapitel 1 Schutzbedarf → Maßnahmen (Nr. 9.2 a), Kapitel 2 Protokolle, Kapitel 3 Verfahren und Schlüssellängen (3.1 bis 3.6), Kapitel 4 ausgeschlossene Verfahren, Kapitel 5 Krypto-Agilität und Post-Quanten-Umstieg, Kapitel 6 Ausnahmen. Diese Leseprobe enthält Kapitel 3.1.

3. Zugelassene Verfahren und Schlüssellängen

Die Einrichtung setzt für neue Systeme nur die in diesem Kapitel zugelassenen Verfahren ein. Bestehende Systeme mit anderen Verfahren werden im Krypto-Inventar erfasst und bis [Datum] umgestellt oder als Ausnahme geführt. Grundlage ist BSI TR-02102-1, Version 2026-01; die Spalte „Fundstelle“ nennt Abschnitt und Seite.

3.1 Symmetrische Verschlüsselung

Bereich	Zugelassen	Bedingungen für den Einsatz	Fundstelle TR-02102-1	Festlegung
Blockchiffre	AES-128, AES-192, AES-256	Für neue Anwendungen nur Blockchiffren mit mindestens 128 Bit Blockgröße. Andere Blockchiffren empfiehlt die TR nicht. Bei hohem oder langfristigem Schutzbedarf und langlebigen Systemen rät die TR zu 256 Bit Schlüssellänge.	3.1, Tabelle 3.1, S. 43–44; Einleitung Kap. 3, S. 43	[ja / nein] ab [128 / 256] Bit
Betriebsart mit Authentisierung (AEAD)	GCM, CCM, AES-GCM-SIV	Bevorzugt einsetzen. CCM und GCM: Tag-Länge mindestens 96 Bit. GCM: IV-Länge 96 Bit, ein IV darf sich unter demselben Schlüssel nicht wiederholen; Schlüsselwechsel spätestens nach 2^{32} Aufrufen. AES-GCM-SIV: IV 96 Bit, zufällig erzeugt; nur mit AES-128 oder AES-256, nicht mit AES-192.	3.1.1, Tabelle 3.2, Bemerkung 3.1, S. 45; 3.1.2, S. 45–46	[ja / nein]
Betriebsart ohne Authentisierung	CBC, CTR	Nur zusammen mit einem separaten Mechanismus zur Datenauthentisierung (z. B. MAC im Encrypt-then-MAC-Verfahren); nicht authentisierte Daten möglichst nicht entschlüsseln oder weiterverarbeiten. CTR: IV darf sich innerhalb einer Schlüsselwechselperiode nicht wiederholen. CBC: nur unvorhersagbare IVs.	3.1.1, Bemerkung 3.1, S. 45; 3.1.2, S. 46	[ja / nein / nur mit Ausnahme]
Datenmenge je Schlüssel	alle Betriebsarten mit AES	Höchstens 2^{59} Blöcke je Schlüssel; bei GCM zusätzlich höchstens $2^{32} - 2$ Blöcke je IV und Schlüssel.	3.1.2, Bemerkung 3.2, S. 46	[ja / nein]

Bereich	Zugelassen	Bedingungen für den Einsatz	Fundstelle TR-02102-1	Festlegung
Padding (nur bei CBC)	ISO-Padding (ISO/IEC 9797-1, Padding Method 2), Padding nach RFC 5652 Abschnitt 6.3, ESP-Padding (RFC 4303 Abschnitt 2.4)	Fehlermeldungen und andere Seitenkanäle dürfen nicht verraten, ob das Padding eines Datenpakets gültig war.	3.1.3, Tabelle 3.3, Bemerkung 3.3, S. 47	[ja / nein]
Stromchiffren	keine eigene Stromchiffre; AES-CTR gilt als Stromchiffre	Die TR empfiehlt derzeit keine dedizierte Stromchiffre. Bei Einsatz einer Stromchiffre die Integrität separat schützen.	3.2, S. 47	[ja / nein]
Schutz von Schlüsseln (Key-Wrapping)	zugelassene Verschlüsselung im AEAD-Modus; oder Verschlüsselung nach 3.1 mit MAC (Encrypt-then-MAC); bei besonders hohen Anforderungen KW oder KWP (NIST SP 800-38F)	Der KEK genügt mindestens denselben Anforderungen wie das geschützte Schlüsselmaterial. Ein Schlüssel wird nicht mehrfach mit demselben KEK gewrappt; erfolglose Prüfversuche je Schlüssel sind begrenzt.	3.3, S. 48	[ja / nein]

Hinweis zum Ausfüllen: Die Normverweise in der Spalte „Zugelassen“ (ISO/IEC 9797-1, RFC 5652, RFC 4303) sind die Quellen, die die TR an der genannten Stelle angibt; prüfen Sie im Zweifel dort. Die Spalte „Festlegung“ ist Ihre Entscheidung. Wenn Sie strenger sein wollen als die TR (z. B. nur AES-256, nur AEAD), tragen Sie das hier ein. Abweichungen nach unten gehören ins Ausnahmeregister.

Kapitel 3.2 bis 3.6 (Hashfunktionen und MAC, asymmetrische Verschlüsselung, Signaturen, Schlüsseleinigung einschließlich ML-KEM-Hybriden und Fristen bis Ende 2031 bzw. 2035, Zufallszahlen) sind im vollständigen Paket enthalten.

Was diese Vorlage nicht ist

- **Keine Rechtsberatung.** Ob und wie das BSIG oder die Durchführungsverordnung (EU) 2024/2690 für Ihre Einrichtung gilt, beurteilt die Vorlage nicht. Dafür ist eine Rechtsberatung nötig.
- **Keine Zusage, dass eine Pflicht erfüllt ist.** Ein ausgefülltes Konzept ist eine Grundlage; ob es den Stand der Technik einhält und zu Ihrer Risikobewertung passt, hängt von Ihren Festlegungen und deren Umsetzung ab.
- **Nicht vom BSI geprüft oder anerkannt.** Die Algorithmenangaben geben Fakten aus der TR-02102-1 in eigenen Worten mit Fundstelle wieder. Maßgeblich ist der Text der TR.
- **Stand:** TR-02102-1 Version 2026-01. Das BSI überarbeitet die TR in der Regel jährlich; prüfen Sie bei jeder neuen Fassung Teil B.

Quellen

- BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Version 2026-01, Stand 23.01.2026, bsi.bund.de
- § 30 BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik), gesetze-im-internet.de
- Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024, Art. 1 und Anhang Nr. 9, eur-lex.europa.eu

Ciphermeter · ciphermeter.com · info@ciphermeter.com