Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

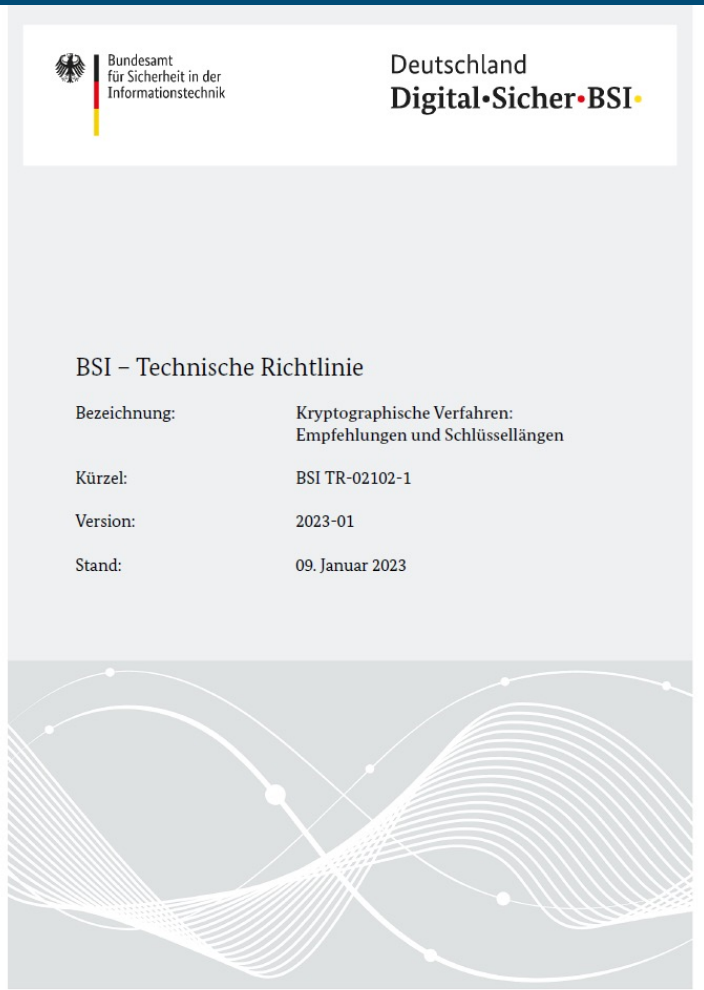
Die Technische Richtlinie TR-02102 und ihre Relevanz für VS-Zulassungsverfahren

Dr. Inga Paul, Referat KM 22

OMNISECURE 2023: Forum 18-B **Evaluierung im Rahmen von VS-Zulassungsverfahren**

Zielsetzung der TR-02102

- **Empfehlungen** zur Wahl von kryptographischen Verfahren und von Schlüssellängen
- Teil 1: Allgemeine Empfehlungen
- Teile 2 bis 4: Empfehlungen für Protokolle (TLS, IKEv2/IPsec, SSH)
- Vorhersagezeitraum 7 Jahre
- Jährliche Aktualisierung
- Verfügbar auf deutsch und englisch



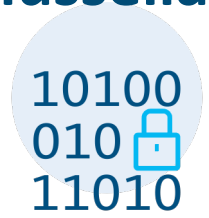
Zielsetzung der TR-02102

- TR-02102 liefert Sicherheit der Grundbausteine und Parameter
- Einschätzung des konkreten Einsatzszenarios durch Experten nötig

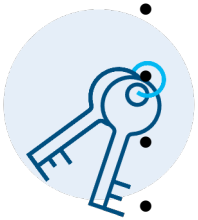
- Keine Vorgaben
  - Abweichungen nicht unbedingt unsicher
  - Keine vollständige Auflistung aller „sicheren Algorithmen“

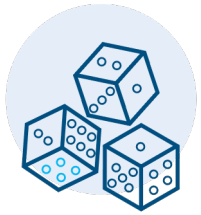
- Einige Empfehlungen der TR-02102 können in gewissen Kontexten verbindlich werden, z.B.
  - Mindeststandard TLS
  - TR-03116 (Vorgaben für Projekte der Bundesregierung)

BSI TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen



- Allgemeine Empfehlungen zu
  - Verschlüsselungsverfahren
  - Hashfunktionen
  - Daten- und Instanzauthentisierung
  - Schlüsseleinigungsverfahren, Schlüsseltransportverfahren
  - Secret Sharing
  - Zufallszahlengeneratoren



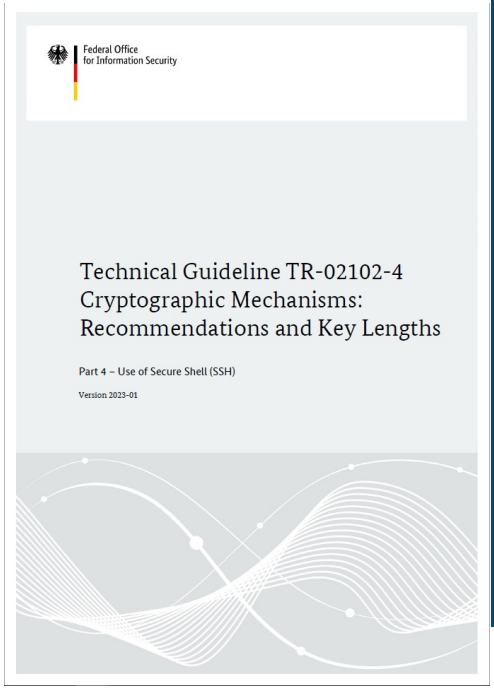


Teile 2 bis 4

TR-02102-2 Verwendung von Transport Layer Security (TLS)

TR-02102-3 Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)

TR-02102-4 Verwendung von Secure Shell (SSH)



- Empfehlungen zu
  - Protokollversion
  - kryptographischen Verfahren (Cipher-Suiten, Domain-Parameter, …)
  - Schlüssellängen

- Hinweise zu Schlüsselmanagement und Zufallszahlen

Aktuelle und zukünftige Änderungen

- 2023: Sicherheitsniveau angehoben von 100 auf 120 Bits

Symmetrische Verfahren		Asymmetrische Verfahren		
Ideale Blockchiffre	Idealer MAC	RSA	DSA/DLIES	ECDSA/ECIES
120	120	2800	2800	240

Tabelle 1.1: Beispiele für Schlüssellängen für ein Sicherheitsniveau von mindestens 120 Bits.

Für RSA werden mindestens 3000 Bits empfohlen

- 2020: erste Empfehlungen von PQ-Verfahren für quantensicheren Schlüsseltransport

- Zukünftig: Weitere PQ-Empfehlungen nach Ende des NIST-Standardisierungsprozesses zu erwarten

Relevanz für VS-Zulassungsverfahren

- Richtschnur für VS-NfD
- Sicherheit der Grundbausteine durch TR-Konformität abgedeckt
- Konkrete Verwendung der Mechanismen muss evaluiert werden
- TR-Konformität wird in VS-Anforderungsprofilen gefordert
- Abweichungen möglich
  - Sicherheit der Anwendung darf nicht eingeschränkt werden
  - Müssen gut begründet werden

Relevanz in Zertifizierung nach Common Criteria (CC)

- Die Stärke kryptographischer Mechanismen wird nicht im Rahmen von Zertifizierungsverfahren bewertet.
- Den in der TR-02102 empfohlenen Mechanismen kann ein Sicherheitsniveau von 120 Bits im Zertifizierungsreport attestiert werden.

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Kontakt

Dr. Inga Paul
Referentin

tr02102@bsi.bund.de

inga.paul@bsi.bund.de
Tel. +49 (0) 228 9582 6874

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•