Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS)

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.1 vom 09.04.2020

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de/mindeststandards

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Siehe Umsetzungsplan Bund 2017, (BMI 2017), S. 4
[2] Analog „Informationssicherheitsbeauftragte (ISB)“
[3] Siehe FAQ zu den Mindeststandards, (BSI 2019)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

Inhaltsverzeichnis

1 Beschreibung

Im Rahmen der stetig zunehmenden Digitalisierung und der damit verbundenen Übertragung von Informationen über Kommunikationsnetze ist es eine zwingende Notwendigkeit, Informationen während der Übertragung abzusichern, um die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleisten zu können.

Eine zuverlässige Absicherung der Übertragung in Netzen kann durch den Einsatz des Protokolls Transport Layer Security (TLS) erreicht werden. TLS wird verwendet, um Informationen während der Übertragung in Netzen kryptographisch abzusichern.

Dabei dient TLS zur Etablierung eines sicheren Kanals (verschlüsselt, authentisiert und integritätsgeschützt). So können Daten aus höheren Schichten des OSI-Referenzmodells[5] sicher über TCP/IP-basierte Verbindungen übertragen werden (z.B. HTTPS, FTPS, IMAPS, LDAPS). Es existieren jedoch unterschiedliche Versionen von TLS, wobei nicht jede Version heute als sicher eingestuft werden kann. Daher ist es wichtig, die korrekte Version in der richtigen Konfiguration einzusetzen, um die oben genannten Schutzziele zu erreichen.

In Kapitel 2 dieses Mindeststandards werden Mindestsicherheitsanforderungen bei der Verwendung von TLS festgelegt.

Der Mindeststandard setzt die IT-Grundschutz-Vorgehensweise des BSI zum Management der Informationssicherheit voraus.[6] Er gilt für alle Schutzbedarfskategorien.

Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend.

Unter Berücksichtigung des individuellen Schutzbedarfs muss die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsmaßnahmen erfolgen.

[5] Vgl. Basic Reference Model: The Basic Model, ISO/IEC 7498-1, (ISO/IEC 1994)
[6] Vgl. BSI-Standard 200-2, (BSI 2017a)

In Anlehnung an den IT-Grundschutz[7] werden die Prüfaspekte in den Nutzerpflichten mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird analog zu den Umsetzungshinweisen des IT-Grundschutzes das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[8] und DIN 820-2: 2018.[9]

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung oder Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

[7] Vgl. IT-Grundschutz-Kompendium, (BSI 2020a), S. 1ff.
[8] Vgl. Key words for use in RFCs, (IETF 1997)
[9] Vgl. DIN-820-2: Gestaltung von Dokumenten, (DIN 2018)

2 Sicherheitsanforderungen

Die nachfolgenden Sicherheitsanforderungen sind umzusetzen, wenn zur Transportverschlüsselung TLS eingesetzt wird. Dieser Mindeststandard stellt konkrete Anforderungen an die Verwendung von TLS und definiert die korrekte Konfiguration. Die Möglichkeit zur Verwendung anderer Protokolle und/oder Verfahren zum Transport und zur Verschlüsselung bleibt davon unberührt.

TLS.2.1.01: Verwendung von TLS

a) Beim Einsatz von TLS bei der Übertragung von Daten MUSS die Version TLS 1.2 in Kombination mit Perfect Forward Secrecy (PFS) oder die Version TLS 1.3 mit PFS eingesetzt werden. Für den korrekten Einsatz MÜSSEN die Empfehlungen der Technischen Richtlinie TR-02102-2[10] umgesetzt und eingehalten werden.

b) Es MUSS geprüft werden, ob mehrere unterschiedliche TLS-Versionen aktiviert sind. TLS-Versionen, die älter sind als TLS 1.2 mit PFS, MÜSSEN deaktiviert werden.

c) Ist der Einsatz von TLS-Versionen, die älter sind als TLS 1.2 mit PFS, abweichend von TLS.2.1.01 a) und b), in Ausnahmefällen zwingend erforderlich (z. B. aus Gründen der Abwärtskompatibilität), stellt dies ein Risiko für die Informationssicherheit dar. Diese Fälle sind daher zu identifizieren und im Rahmen des behördeneigenen Risikomanagements zu behandeln. Hierzu zählen in erster Linie die Dokumentation und die Bewertung des Risikos und der zu ergreifenden mitigierenden Maßnahmen. Die dokumentierte Beschreibung und Bewertung des Restrisikos und der zu ergreifenden Maßnahmen MUSS der Leitungsebene zur Zustimmung vorgelegt werden.[11, 12] Eine ausführliche Beschreibung der Vorgehensweise bei der Risikoanalyse auf der Basis von IT-Grundschutz bietet der BSI-Standard 200-3.[13] Das Ziel MUSS die Ablösung der unsicheren TLS-Versionen sein.

d) Bei Neubeschaffungen, die für eine längere Einsatzphase gedacht sind, SOLLTE bereits heute auf Kompatibilität mit TLS 1.3 geachtet werden.

TLS.2.1.02: TLS für Webserver

Webserver bieten eine exponierte Angriffsfläche und sind durch geeignete Schutzmaßnahmen abzusichern. Das IT-Grundschutz-Kompendium adressiert dies in der Basis-Anforderung APP.3.2.A11[14]:

> „Der Webserver MUSS für alle Verbindungen durch nicht vertrauenswürdige Netze eine sichere Verschlüsselung über TLS anbieten (HTTPS). Falls es aus Kompatibilitätsgründen erforderlich ist, veraltete Verfahren zu verwenden, SOLLTEN diese auf so wenige Fälle wie möglich beschränkt werden. Wenn eine HTTPS-Verbindung genutzt wird, DÜRFEN alle Inhalte NUR über HTTPS verfügbar sein. Sogenannter Mixed Content DARF NICHT verwendet werden."

Die Basis-Anforderung wird nachfolgend konkretisiert:

a) Als veraltete Verfahren MÜSSEN TLS-Versionen eingestuft werden, die nicht TLS.2.1.01 Buchstabe a) erfüllen.

b) Werden aus Kompatibilitätsgründen dennoch veraltete TLS-Versionen eingesetzt, MÜSSEN diese nach TLS.2.1.01 Buchstabe c) behandelt werden.

[10] Vgl. TR-02102-2: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2, (BSI 2020b)
[11] Vgl. Umsetzungsplan Bund 2017, (BMI 2017), Kap. 3.2.3
[12] Vgl. BSI-Standard 200-2 – IT-Grundschutz-Methodik, (BSI 2017a), Kapitel 8.5
[13] Vgl. BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, (BSI 2017b)
[14] Vgl. IT-Grundschutz-Kompendium, (BSI 2020a), S. 1ff.

TLS.2.1.03: Sicherheitsanforderungen für Projekte des Bundes

Für die Authentisierung innerhalb von Projekten des Bundes verweist die Technische Richtlinie TR-02102-2[15] auf die Technische Richtlinie TR-03116-4.[16] Die Vorgaben der TR-03116-4 bezüglich der Authentisierung MÜSSEN eingehalten werden (insbesondere das Kapitel 5 "Identifizierung von Kommunikationspartnern"). Bezüglich SHA-224 und elliptischer Kurven mit einer Schlüssellänge von 224 Bit gelten in Abweichung zur TR-02102-2 die Anforderungen der TR-03116-4 für Projekte des Bundes.

Abbildung 1 veranschaulicht die Beziehungen des Mindeststandards zu den technischen Richtlinien und die damit verbundenen Auswirkungen:

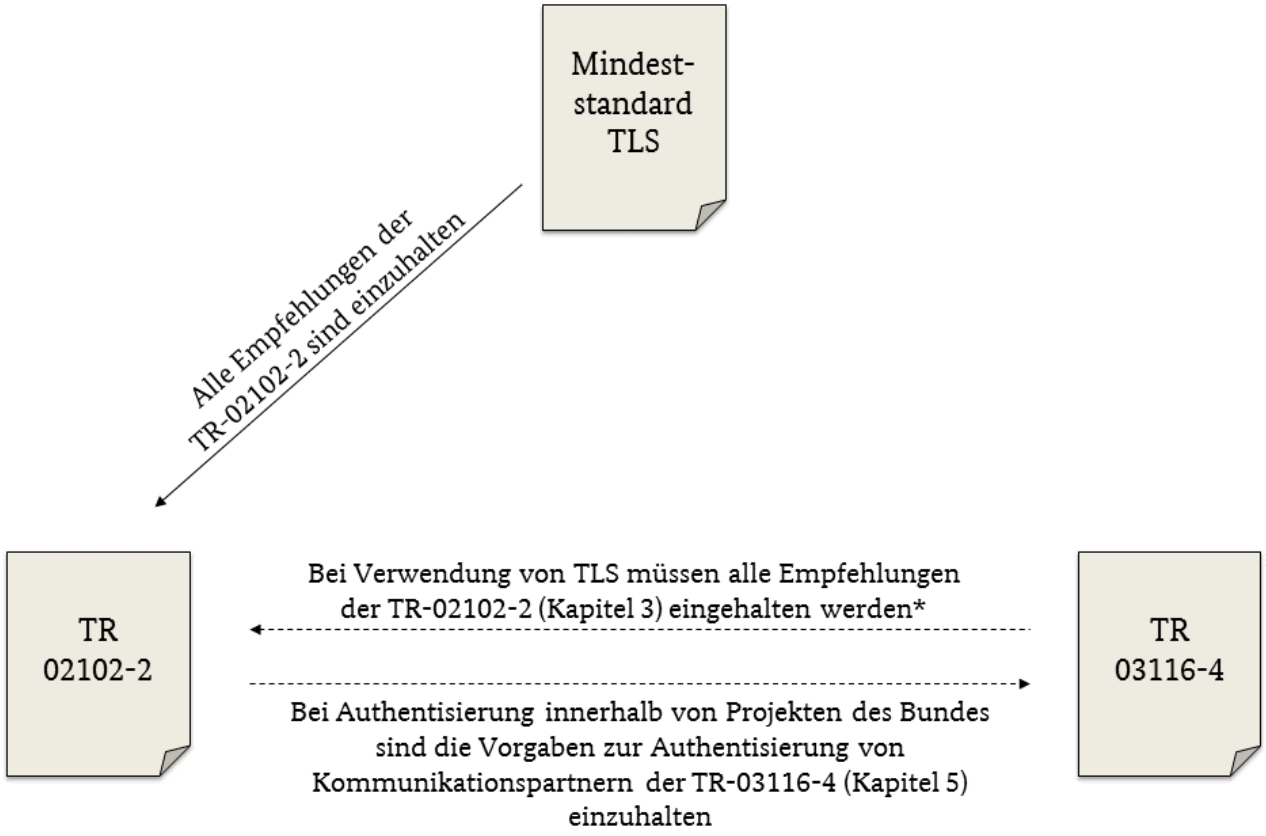

Abbildung 1: Mindeststandard und Technische Richtlinien

[15] Vgl. TR-02102-2: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2, (BSI 2020b)
[16] Vgl. TR-03116-4: „Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4, (BSI 2020c)

Literaturverzeichnis

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund 2017, Stand: September 2017

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0

BSI (2019) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/11916758, abgerufen am 09.03.2020

BSI (2020a) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 3. Edition, 2020

BSI (2020b) Bundesamt für Sicherheit in der Informationstechnik: TR-02102-2: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)“, Version 2020-01

BSI (2020c) Bundesamt für Sicherheit in der Informationstechnik, TR-03116-4: „Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4 - Kommunikationsverfahren in Anwendungen“, Version 10. Januar 2020

DIN (2018) Deutsches Institut für Normierung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://tools.ietf.org/html/rfc2119, abgerufen am 09.03.2020

ISO/IEC (1994) Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model, ISO/IEC 7498-1, 1994

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
FTPS	File Transfer Protocol over SSL/TLS
HTTPS	Hypertext Transfer Protocol Secure
IMAPS	Internet Message Access Protocol over SSL/TLS
LDAPS	Lightweight Directory Access Protocol over SSL/TLS
OSI	Open Systems Interconnection
PFS	Perfect Forward Secrecy
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security