Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI zur Verwendung von Transport Layer Security

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.3 vom 15.03.2022

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.5	21.11.2014	Erstveröffentlichung
2.0	05.04.2019	Major Release – umfassende Überarbeitung
2.1	09.04.2020	Minor Release – Anpassungen und Konkretisierungen
2.2	03.05.2021	Minor Release – Anpassungen und Konkretisierungen
2.3	15.03.2022	Minor Release – Anpassungen und Konkretisierungen

Tabelle 1: Versionsgeschichte des Mindeststandards zur Verwendung von Transport Layer Security. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/dok/453390

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

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt Mindeststandards (MST) für die Sicherheit der Informationstechnik des Bundes[1] fest. Dies erfolgt auf der Grundlage des § 8 Absatz 1 BSIG im Benehmen mit den Ressorts. Als gesetzliche Vorgabe definieren Mindeststandards ein verbindliches Mindestniveau für die Informationssicherheit.

Bereits 2017 hat das Bundeskabinett mit dem Umsetzungsplan Bund 2017 (UP-Bund Bund 2017) eine Leitlinie für Informationssicherheit in der Bundesverwaltung in Kraft gesetzt. Damit wurde die Beachtung der Mindeststandards für den Bereich der Stellen des Bundes verbindlich. Durch das IT-Sicherheitsgesetz 2.0 wurde die Einhaltung der Mindeststandards des BSI auch gesetzlich geregelt. Die Umsetzungspflicht der Mindeststandards ergibt sich aus dem dadurch neu gefassten § 8 BSIG.

Die Mindeststandards richten sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe), Informationssicherheitsbeauftragte (ISB), IT-Betriebspersonal und Beschaffungsstellen. Die Gesamtverantwortung für die Informationssicherheit und damit auch für die Einhaltung der Mindeststandards trägt gemäß UP Bund 2017 die jeweilige Hausleitung.

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.[2] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Einrichtung[3] 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 Einrichtungen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Die von den Mindeststandards adressierten Stellen werden in § 8 Absatz 1 BSI-Gesetz (BSIG) definiert (siehe https://www.gesetze-im-internet.de/bsig_2009/__8.html). Zur besseren Lesbarkeit wird im weiteren Verlauf für alle dort genannten Stellen der Begriff „Einrichtung“ verwendet.

[2] Vgl. Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards (Bundesamt für Sicherheit in der Informationstechnik, 2022)

[3] Siehe Fußnote 1

Inhalt

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. Dieser Mindeststandard stellt konkrete Anforderungen an die sichere Verwendung und Konfiguration von TLS.

1.1 Einleitung und Abgrenzung

TLS wird verwendet, um Informationen während der Übertragung in Netzen kryptographisch durch Etablierung eines sicheren Kanals (verschlüsselt, authentisiert und integritätsgeschützt) abzusichern. So können Daten aus höheren Schichten des OSI-Referenzmodells[4] 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 geeignete Version in der richtigen Konfiguration einzusetzen, um die oben genannten Schutzziele zu erreichen.

Der Mindeststandard zur Verwendung von Transport Layer Security fordert nicht, dass TLS zur kryptographischen Absicherung von Informationen während der Übertragung in Netzen verwendet werden muss. Unter der Voraussetzung, dass keine Einschränkungen für das angestrebte Sicherheitsniveau entstehen, können auch andere Protokolle und/oder Verfahren zur Transportverschlüsselung verwendet werden.

Sobald TLS verwendet wird, müssen die in Kapitel 2 dieses Mindeststandards beschriebenen Sicherheitsanforderungen beachtet und umgesetzt werden.

Der Mindeststandard setzt die IT-Grundschutz-Vorgehensweise des BSI zum Management der Informationssicherheit voraus.[5] Er gilt für alle Schutzbedarfskategorien.

Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend. Unter Berücksichtigung des individuellen Schutzbedarfs muss die Prüfung sowie gegebenenfalls die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsmaßnahmen erfolgen.

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[6] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[7] und DIN 820-2: 2018[8].

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.

[4] Vgl. Basic Reference Model (ISO/IEC, 1994)
[5] Vgl. BSI-Standard 200-2 (Bundesamt für Sicherheit in der Informationstechnik, 2017)
[6] Vgl. BSI-Standard 200-2 (Bundesamt für Sicherheit in der Informationstechnik, 2017), S. 18
[7] Vgl. Key words for use in RFCs (Internet Engineering Task Force (IETF), 1997)
[8] Vgl. DIN-820-2: Gestaltung von Dokumenten (Deutsches Institut für Normung e.V. (DIN), 2018)

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. Die Begründung muss dokumentiert und bei einem Audit 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. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

KANN

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

2 Sicherheitsanforderungen

Die nachfolgenden Sicherheitsanforderungen sind zu erfüllen, wenn zur Transportverschlüsselung TLS eingesetzt wird. Dieser Mindeststandard stellt konkrete Anforderungen an die sichere Verwendung und Konfiguration von TLS. Die Möglichkeit, andere Protokolle und/oder Verfahren zur Transportverschlüsselung zu verwenden, bleibt davon unberührt.

Grundlage für die Sicherheitsanforderungen dieses Mindeststandards sind die in der Technischen Richtlinie TR-02102-2[9] formulierten Empfehlungen. Durch die Umsetzung der Empfehlungen der jeweils aktuellen Technischen Richtlinie TR-02102-2[10] wird eine sichere Verwendung von TLS erzielt.

TLS.2.0.01 – Verwendung von TLS-Protokoll-Versionen

a) Die Einrichtung MUSS TLS in der Version TLS 1.2 und/oder TLS 1.3 einsetzen.

b) TLS-Versionen, die nicht TLS.2.0.01 a) entsprechen, MÜSSEN deaktiviert werden.

c) Bei Neubeschaffungen, die für einen produktiven Einsatz gedacht sind, MUSS auf Kompatibilität mit TLS 1.3 geachtet werden.

TLS.2.0.02 - Verwendung von kryptografischen Verfahren

a) Die Einrichtung MUSS TLS mit kryptografischen Verfahren einsetzen, die in der Technischen Richtlinie TR-02102-2[11] empfohlen werden und die Eigenschaft „Perfect Forward Secrecy“ (PFS) erfüllen.

TLS.2.0.03 - Abweichungen und Risikomanagement

Ist der Einsatz von Versionen, abweichend von TLS.2.0.01 oder von kryptografischen Verfahren abweichend von TLS.2.0.02 zwingend erforderlich, kann dies ein Risiko für die Informationssicherheit darstellen.

a) Der Einsatz nicht konformer Versionen und/oder nicht konformer kryptografischer Verfahren[12] DARF NUR in sachlich begründeten Ausnahmefällen und nach Rücksprache mit dem BSI[13] erfolgen.

b) Die Einrichtung MUSS den Einsatz nicht konformer Versionen und/oder nicht konformer kryptografischer Verfahren identifizieren und im Rahmen des eigenen Risikomanagements behandeln.[14]

c) Die Einrichtung MUSS die Risiken, die sich durch den Einsatz nicht konformer Versionen und/oder nicht konformer kryptografischer Verfahren ergeben, bewerten und dokumentieren.

d) Die Einrichtung MUSS die zur Risikobehandlung zu ergreifenden Maßnahmen identifizieren, umsetzen und dokumentieren.

e) Die Einrichtung MUSS das nach der Umsetzung mitigierender Maßnahmen verbleibende Restrisiko dokumentieren.

f) Die Einrichtung MUSS einen dem Risiko angemessenen Zeit- und Maßnahmenplan zur Ablösung der nicht konformen Versionen und/oder der nicht konformen kryptografischen Verfahren erstellen.

[9] Vgl. TR-02102-2 (Bundesamt für Sicherheit in der Informationstechnik, 2022)
[10] Vgl. TR-02102-2 (Bundesamt für Sicherheit in der Informationstechnik, 2022)
[11] Vgl. TR-02102-2 (Bundesamt für Sicherheit in der Informationstechnik, 2022)
[12] Nicht konforme Versionen und/oder nicht konforme kryptografische Verfahren sind im Kontext dieses Mindeststandards Versionen, die von TLS.2.0.01 abweichen und/oder kryptografische Verfahren, die von TLS.2.0.02 abweichen.
[13] mindeststandards@bsi.bund.de
[14] Eine ausführliche Beschreibung der Vorgehensweise bei der Risikoanalyse auf der Basis von IT-Grundschutz bietet der BSI-Standard 200-3 (Bundesamt für Sicherheit in der Informationstechnik, 2017)

g) Die Dokumentation des Restrisikos sowie der Zeit- und Maßnahmenplan zur Ablösung der nicht konformen Versionen und/oder der nicht konformen kryptografischen Verfahren MÜSSEN der jeweiligen Leitung der Einrichtung zur Zustimmung vorgelegt werden.[15]

TLS.2.0.04 - 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[16]:

> „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, MÜSSEN alle Inhalte über HTTPS ausgeliefert werden. Sogenannter Mixed Content DARF NICHT verwendet werden."

Diese Basis-Anforderung wird nachfolgend konkretisiert:

a) Im Kontext dieses Mindeststandards sind veraltete Verfahren als Versionen und Verfahren zu verstehen, die nicht die Anforderungen von TLS.2.0.01 und TLS.2.0.02 erfüllen.

b) Werden Abweichungen von TLS.2.0.01 oder von TLS.2.0.02 umgesetzt, MUSS die Einrichtung diese nach TLS.2.0.03 behandeln.

TLS.2.0.05 - Sicherheitsanforderungen für Projekte des Bundes

Für die Authentisierung innerhalb von Projekten des Bundes verweist die Technische Richtlinie TR-02102-2[17] auf die Technische Richtlinie TR-03116-4[18].

a) Die Vorgaben der TR-03116-4[19] bezüglich der Authentisierung MÜSSEN eingehalten werden.

[15] Vgl. BSI-Standard 200-2 (Bundesamt für Sicherheit in der Informationstechnik, 2017) Kapitel 8.5
[16] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022)
[17] Vgl. TR-02102-2 (Bundesamt für Sicherheit in der Informationstechnik, 2022)
[18] Vgl. TR-03116-4 (Bundesamt für Sicherheit in der Informationstechnik, 2022)
[19] Vgl. TR-03116-4 (Bundesamt für Sicherheit in der Informationstechnik, 2022)

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

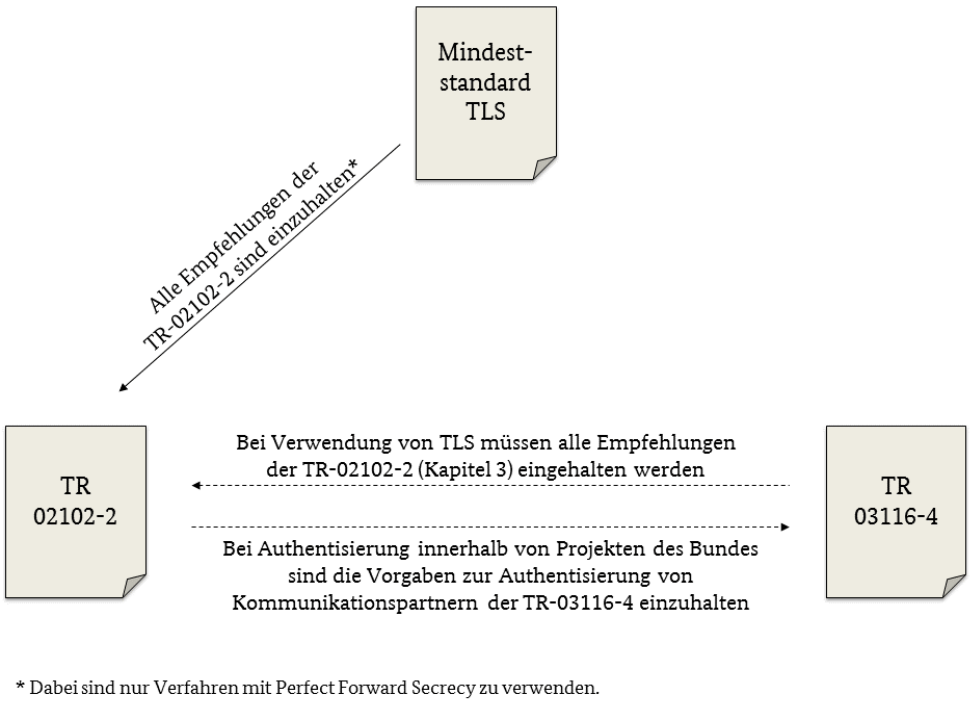

Abbildung 1: Mindeststandard zur Verwendung von Transport Layer Security und Technische Richtlinien

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik. 2022. BSI IT-Grundschutz-Kompendium, Edition 2022. [Online] 2022. [Zitat vom: 01. Februar 2022.] https://www.bsi.bund.de/dok/989376.

—. 2017. BSI Standard 200-2, IT-Grundschutz-Methodik. [Online] 2017. [Zitat vom: 01. Februar 2022.] https://www.bsi.bund.de/dok/128640.

—. 2017. BSI Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz. [Online] 2017. [Zitat vom: 01. Februar 2022.] https://www.bsi.bund.de/dok/407502.

—. 2022. Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards. [Online] 2022. [Zitat vom: 01. Februar 2022.] https://www.bsi.bund.de/dok/11916758.

—. 2022. TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 - Verwendung von Transport Layer Security (TLS). [Online] 2022. [Zitat vom: 01. März 2022.] https://www.bsi.bund.de/dok/405534.

—. 2022. TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4 - Kommunikationsverfahren in Anwendungen. [Online] 2022. [Zitat vom: 01. Februar 2022.] https://www.bsi.bund.de/dok/433402.

Bundesministerium des Innern und für Heimat. 2017. Umsetzungsplan Bund 2017. [Online] 2017. [Zitat vom: 01. Februar 2022.] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html.

Deutsches Institut für Normung e.V. (DIN). 2018. *DIN 820-2:2018-09: Normungsarbeit – Teil 2: Gestaltung von Dokumenten.* Berlin : Beuth Verlag GmbH, 2018.

Internet Engineering Task Force (IETF). 1997. RFC 2119: Key words for use in RFCs to Indicate Requirement Levels. [Online] 1997. [Zitat vom: 23. 07 2020.] https://tools.ietf.org/html/rfc2119.

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
DIN	Deutsches Institut für Normung e.V.
FTPS	File Transfer Protocol over SSL/TLS
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IMAPS	Internet Message Access Protocol over SSL/TLS
ISB	Informationssicherheitsbeauftragte
IT-SiBe	IT-Sicherheitsbeauftragte
LDAPS	Lightweight Directory Access Protocol over SSL/TLS
MST	Mindeststandard
OSI	Open Systems Interconnection
PFS	Perfect Forward Secrecy
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
RFC	Request for Comments
UP	Umsetzungsplan