

CHECKLISTE · TOMORIS TOOLBOX

TLS und Zertifikate: Checkliste für Server und Websites

Protokolle, Schlüssel, Laufzeiten bis 47 Tage, ACME, Inventar, HSTS und CAA nach BSI TR-02102-2, CA/Browser Forum und IETF, mit Konfiguration und Prüfbefehlen

STAND

25.10.2026

UMFANG

PDF, 12 Seiten

ONLINE

tomoris.com/downloads/tls-zertifikate-checkliste

AUF EINEN BLICK

200 Tage

Höchstlaufzeit öffentlicher Zertifikate seit 15.3.2026

47 Tage

Höchstlaufzeit ab 15.3.2029 (CA/Browser Forum)

TLS 1.3

bevorzugen; TLS 1.2 laut BSI nur noch bis Ende 2031

10 Tage

gilt eine Domain-Prüfung ab 15.3.2029 höchstens

FÜR WEN

- Administration von Web-, Mail- und VPN-Servern, Reverse Proxys und Load Balancern
- Webagenturen und Hoster, die Websites und Zertifikate für Kunden betreiben
- Website-Verantwortliche und IT-Leitung, die Zertifikate, Dienstleister und Fristen im Blick behalten müssen

WORUM ES GEHT

Öffentliche TLS-Zertifikate laufen seit 15. März 2026 höchstens 200 Tage, ab März 2029 nur noch 47 Tage, und die Prüfung der Domain gilt dann nur noch 10 Tage. Wer Zertifikate von Hand erneuert, bekommt damit ein Betriebsproblem. Diese Checkliste führt durch Protokolle, Cipher Suites und Schlüssel nach BSI TR-02102-2 (Version 2026-01) und TLSRef, Automatisierung mit ACME, Inventar und Ablaufüberwachung, HSTS, CAA, interne Dienste und die Sperrprüfung nach dem Ende von OCSP bei Let's Encrypt. Dazu kommen Beispielkonfigurationen für nginx und Apache und Prüfbefehle mit OpenSSL.

Diese Checkliste ist eine Empfehlung von TOMORIS nach den genannten Quellen, Stand 25.10.2026. Verbindlich sind für Zertifizierungsstellen die Baseline Requirements in der geltenden Fassung, für wesentliche und wichtige Einrichtungen das NISG 2026; die BSI TR-02102-2 ist eine Empfehlung. Sie ersetzt keine Rechtsberatung. Standardwerte und Bezeichnungen können sich ändern. Testen Sie Änderungen zuerst in einer Testumgebung, zu strenge Einstellungen können ältere Clients aussperren.

INHALT

01	Worum es geht und was vorgegeben ist	3
02	Laufzeiten: der Stufenplan bis 2029	3
03	Protokolle, Cipher Suites und Schlüssel	4
04	Automatisieren mit ACME	6
05	Inventar und Ablaufüberwachung	7
06	HTTPS erzwingen: Weiterleitung, HSTS und CAA	7
07	Beispielkonfiguration und Prüfbefehle	8
08	Interne Dienste und Sperrprüfung	10
09	Checkliste zum Abhaken	11
10	Quellen	12

01

Worum es geht und was vorgegeben ist

Warum Zertifikate kürzer laufen, was das NISG 2026 verlangt und was nur Empfehlung ist.

TLS verschlüsselt Verbindungen zu Websites, Mail- und VPN-Servern und Geräten; das Zertifikat belegt, dass der Server zum Namen gehört. Neben den Laufzeiten (Abschnitt 02) ändert sich 2026 die BSI-Empfehlung: Die TR-02102-2, Version 2026-01 vom 27. Jänner 2026, empfiehlt TLS 1.2 nur noch bis Ende 2031, weil dafür voraussichtlich keine quantensicheren Schlüsseleinigungsverfahren standardisiert werden (Abschnitt 3.2).

Was vorgegeben ist und was empfohlen wird

VORGABE	FÜR WEN	GRUNDLAGE
Kryptografiekonzept: Protokolle, Algorithmen, Schlüssel und Zertifikate, nach dem Stand der Technik	wesentliche und wichtige Einrichtungen, seit 1. Oktober 2026	§ 32 Abs. 4 lit. h NISG 2026; § 2 NISV 2026 mit Anhang Nr. 9 DVO (EU) 2024/2690
Laufzeit, Domain-Prüfung, CAA, Sperrung	öffentliche Zertifizierungsstellen, wirkt auf alle Nutzer	Baseline Requirements 2.3.1 vom 4. Oktober 2026
TLS 1.0 und 1.1 nicht verwenden, TLS 1.3 bevorzugen	Betreiber von TLS-Diensten (IETF-Empfehlung, nicht gesetzlich verbindlich)	RFC 8996; RFC 9325 Abschnitt 3.1.1, geändert durch RFC 9852 und RFC 10015 (Juli 2026)
Versionen, Cipher Suites, Schlüssellängen	Empfehlung, in Österreich nicht verbindlich	BSI TR-02102-2, Version 2026-01
alle weiteren Punkte	alle Betreiber	Empfehlung von TOMORIS

Die Baseline Requirements binden Zertifizierungsstellen, sobald Browser- und Softwarehersteller sie durchsetzen (Abschnitt 1.1). § 32 NISG 2026 schreibt kein bestimmtes Verfahren vor, verlangt aber geeignete, verhältnismäßige Maßnahmen nach dem Stand der Technik (Abs. 1 und 2).

02

Laufzeiten: der Stufenplan bis 2029

Höchstlaufzeit und Domain-Prüfung sinken in drei Stufen; die erste gilt seit 15. März 2026.

Stufenplan nach Ballot SC-081v3 (Baseline Requirements 2.3.1, Abschnitte 6.3.2 und 4.2.1)

ZERTIFIKAT AUSGESTELLT	HÖCHSTLAUFZEIT	DOMAIN-PRÜFUNG GILT HÖCHSTENS
vor dem 15. März 2026	398 Tage	398 Tage
ab 15. März 2026 (gilt jetzt)	200 Tage	200 Tage
ab 15. März 2027	100 Tage	100 Tage

ab 15. März 2029

47 Tage

10 Tage

Die CAs sollen jeweils einen Tag darunter bleiben (199, 99, 46 Tage), weil ein Tag 86 400 Sekunden hat und schon Bruchteile darüber als weiterer Tag zählen (Abschnitt 6.3.2). Geprüfte Unternehmensangaben für OV-Zertifikate dürfen seit 15. März 2026 höchstens 398 statt 825 Tage wiederverwendet werden (4.2.1); für EV gelten nach den EV Guidelines (3.2.2.14.3) schon seit 2021 höchstens 398 Tage. SC-081v3 wurde am 11. April 2025 ohne Gegenstimme angenommen.

- Bei 47 Tagen braucht jeder Name mindestens acht Zertifikate im Jahr, und bei 10 Tagen ist die Domain-Prüfung praktisch jedes Mal neu fällig. Let's Encrypt rät von manueller Erneuerung ab; auch der Nachweis muss automatisch laufen (Abschnitt 04).
- Bei kompromittiertem Schlüssel und einigen weiteren Gründen, etwa unzuverlässiger Domain-Prüfung, muss die CA binnen 24 Stunden sperren, in anderen Fällen binnen 5 Tagen (Abschnitt 4.9.1.1). Ein Tausch muss also jederzeit kurzfristig gehen.

Let's Encrypt verkürzt früher (Ankündigung vom 2. Dezember 2025): Profil tlsserver seit 13. Mai 2026 mit 45 Tagen; Standardprofil classic ab 10. Februar 2027 mit 64 Tagen und 10 Tagen Wiederverwendung der Domain-Prüfung (bestätigt am 7. Oktober 2026), ab 16. Februar 2028 mit 45 Tagen und 7 Stunden; Profil shortlived mit rund 6 Tagen.

03

Protokolle, Cipher Suites und Schlüssel

TLS 1.3 bevorzugen, TLS 1.2 nur mit Forward Secrecy, Älteres abschalten, Schlüssel richtig wählen.

TLS-Versionen nach BSI TR-02102-2 (Tabelle 2), RFC 8996, RFC 9325 und RFC 9852

VERSION	EMPFEHLUNG	FUNDSTELLE
TLS 1.3	bevorzugt verwenden; BSI: bis 2032, möglicherweise länger (Angabe 2032+)	TR-02102-2 Abschnitt 3.2; RFC 9325 Abschnitt 3.1.1; RFC 9852: neue Protokolle müssen TLS 1.3 verlangen
TLS 1.2	für ältere Clients aktiv lassen; BSI: nur noch bis Ende 2031	TR-02102-2 Abschnitt 3.2; RFC 9325 Abschnitt 3.1.1 verlangte es, RFC 9852 (Juli 2026) macht es optional
TLS 1.0, 1.1	abschalten	RFC 8996: „MUST NOT be used“; vom BSI nicht empfohlen
SSL 2.0, 3.0	abschalten	RFC 9325 Abschnitt 3.1.1; TR-02102-2 Abschnitt 3.2

TLS 1.3

TLS_AES_128_GCM_SHA256

Nur noch AEAD-Verfahren, jeder Schlüsseltausch über öffentliche Schlüssel mit Forward Secrecy (RFC 9846, Abschnitt 1.3; ersetzt seit Juli 2026 RFC 8446). BSI: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_AES_128_CCM_SHA256 (Tabelle 13). TLSRef ergänzt TLS_CHACHA20_POLY1305_SHA256, das die TR-02102-2 nicht nennt; nicht Genanntes hält das BSI nicht unbedingt für unsicher (Kapitel 1). 0-RTT-Daten weder senden noch annehmen (Abschnitt 3.4.1).

TLS 1.2

ECDHE+AESGCM: ECDHE+CHACHA20

Nur ECDHE mit AES-GCM oder ChaCha20-Poly1305, die sechs Suiten von TLSRef Intermediate. Seit RFC 10015 (Juli 2026, ändert RFC 9325 Abschnitt 4.1) dürfen TLS_RSA_*, TLS_DH_* und TLS_DHE_* in TLS 1.2 nicht mehr ausgehandelt werden (MUST NOT), von statischem ECDH wird abgeraten. BSI: CBC nur mit Encrypt-then-MAC, DHE bis 2029 (die IETF ist hier strenger), Extended Master Secret ja (3.3.1, 3.3.4). Kompression aus (RFC 9325 Abschnitt 3.3), Heartbeat aus (BSI 3.3.4.6).

Gruppen

TLSRef 6.0: X25519MLKEM768 (hybrid, quantensicher, ab OpenSSL 3.5), X25519, P-256, P-384. BSI: secp256r1, secp384r1, secp521r1, Brainpool, ffdhe3072/4096 (Tabelle 10), nicht X25519; klassisch allein nur bis Ende 2031. Seit RFC 10024 (August 2026) dürfen laut BSI SecP256r1MLKEM768 und SecP384r1MLKEM1024 TR-konform eingesetzt werden (Empfehlung für die nächste TR-Fassung angekündigt), zusätzlich X25519MLKEM768.

Schlüssel und Signaturen öffentlicher Zertifikate

THEMA	MINDESTMASS	EMPFEHLUNG
ECDSA	nur P-256, P-384 oder P-521 (Baseline Requirements 6.1.5)	P-256 (TLSRef) oder P-384; BSI: mindestens 250 Bit. Die vom BSI bevorzugten Brainpool-Kurven sind für öffentliche Zertifikate nicht zulässig.
RSA	2048 Bit (6.1.5; RFC 9325)	BSI: mindestens 3000 Bit (Tabelle 14), etwa 3072 Bit; TLSRef Intermediate: 2048 Bit
Signatur	kein SHA-1; für Server-Zertifikate seit Langem ausgeschlossen, die letzten Ausnahmen für CA-Zertifikate und Sperrlisten endeten am 15. September 2026 (Baseline Requirements 1.2.2, 7.1.3.2.1)	SHA-256 oder stärker; RSA mit PKCS #1 v1.5 empfiehlt das BSI nur bis 2025, RSA-PSS und ECDSA weiter (Tabellen 7 und 12)

TLSRef ist der Nachfolger des Mozilla SSL Configuration Generator (ssl-config.mozilla.org leitet weiter, laut Mozilla betreut eine Community-Arbeitsgruppe außerhalb von Mozilla das Projekt). Intermediate erlaubt die Signatur sha256WithRSAEncryption (PKCS #1 v1.5); wer der TR-02102-2 eng folgt, prüft die Kette und wählt ECDSA bei einer CA mit ECDSA-Zwischenzertifikat.

04 —

Automatisieren mit ACME

Antrag, Domain-Nachweis und Erneuerung ohne Handarbeit, mit Überwachung.

ACME (RFC 8555) ist der IETF-Standard für Antrag, Domain-Nachweis und Erneuerung ohne Handarbeit; ob Ihre CA ihn anbietet, steht in ihrer Dokumentation. Die gebräuchlichsten Wege für den Nachweis per ACME (weitere wie dns-account-01, Baseline Requirements 3.2.2.4.21, kommen hinzu):

http-01

`/.well-known/acme-challenge/`

Die CA ruft eine Datei über HTTP auf TCP-Port 80 ab (RFC 8555, Abschnitt 8.3); Port 80 muss offen bleiben. Nicht für Wildcards (Baseline Requirements 3.2.2.4).

dns-01

`_acme-challenge TXT`

TXT-Eintrag (RFC 8555, Abschnitt 8.4), auch für Wildcards und Systeme ohne Zugang aus dem Internet. Braucht Schreibzugriff auf die DNS-Zone; TOMORIS empfiehlt, ihn eng zu begrenzen.

tls-alpn-01

Nachweis über einen eigenen TLS-Handshake mit ALPN (Baseline Requirements 3.2.2.4.20, nach RFC 8737), wenn Port 80 zu bleiben soll. Nicht für Wildcards.

Dauerhafter Eintrag

`_validation-persist TXT`

Neu (Baseline Requirements 3.2.2.4.22, Ballot SC-088v3): nennt CA und Konto und bleibt bei Erneuerungen gleich; eine Prüfung damit gilt höchstens 10 Tage. Let's Encrypt hat dafür DNS-PERSIST-01 angekündigt.

- Erneuerung terminieren: am besten nach ACME Renewal Information (ARI, RFC 9773), dann schlägt die CA ein Zeitfenster vor, etwa früher vor einer Massensperrung. Ohne ARI nennt Let's Encrypt die Erneuerung nach etwa zwei Dritteln der Laufzeit als geeignet; feste 60 Tage reichen bei 45 Tagen nicht.
- Einsetzen und neu laden: Der Dienst muss das neue Zertifikat laden, auch auf Load Balancer, Firewall oder Appliance. Nach der ersten automatischen Erneuerung mit den Befehlen aus Abschnitt 07 prüfen.
- Ausfälle melden lassen: Let's Encrypt empfiehlt eine Überwachung, die Alarm gibt, wenn nicht wie erwartet erneuert wird. TOMORIS empfiehlt, von außen zu prüfen, was der Dienst ausliefert.

Bestätigung per Telefon oder E-Mail läuft aus: Die Baseline Requirements schließen die Domain-Prüfung per Telefon ab 15. März 2027 aus (3.2.2.4.16, 3.2.2.4.17), per E-Mail an Kontakte wie admin@ ab 15. März 2028 (3.2.2.4.4, 3.2.2.4.13, 3.2.2.4.14; Ballot SC-090).

05 —

Inventar und Ablaufüberwachung

Jedes Zertifikat mit Ablauf und Zuständigkeit erfassen und von außen überwachen.

Für Einrichtungen nach dem NISG 2026 verlangt die DVO (EU) 2024/2690 (über § 2 NISV 2026) ein Konzept für das Schlüsselmanagement, soweit angemessen unter anderem für Ausstellung und Erlangung von Public-Key-Zertifikaten, Schlüsselwechsel, Widerruf und Aktivierungsfristen (Anhang Nr. 9.2 lit. c, Punkte ii, v, vii und xii). Ein Inventar ist dafür die einfachste Grundlage und nützt jedem Unternehmen.

Vorlage: Zertifikatsinventar (je Name und Dienst eine Zeile)

DIENT UND NAME	AUSSTELLER	LÄUFT AB	ERNEUERUNG	ZUSTÄNDIG
Website: [www.domain]	_____	_____	_____	_____
Mail: SMTP, IMAP, Webmail	_____	_____	_____	_____
VPN, Firewall, Proxy	_____	_____	_____	_____
Drucker, NAS, Geräte	_____	_____	_____	_____
Interne Anwendungen	_____	_____	_____	_____

- ☐ Alle Namen erfasst, auch Subdomains, Fernzugänge und Zertifikate bei Hostern oder Dienstleistern; unter Erneuerung steht „ACME“ oder der manuelle Ablauf mit Termin.
- ☐ Unbekannte Zertifikate gesucht: Certificate Transparency (RFC 6962) protokolliert ausgestellte Zertifikate öffentlich; eine Suche nach Ihren Domains zeigt Zertifikate außerhalb des Inventars.
- ☐ Überwachung von außen je Dienst und Port; TOMORIS empfiehlt eine Warnung bei einem Drittel Restlaufzeit und Alarm bei sieben Tagen, an eine Gruppe statt an eine Person.

06 —

HTTPS erzwingen: Weiterleitung, HSTS und CAA

HTTP dauerhaft umleiten, HSTS in Stufen einführen, per CAA die Aussteller festlegen.

Drei Bausteine sorgen dafür, dass Besucher nur verschlüsselt verbinden und nur die gewünschte Zertifizierungsstelle ausstellen darf: Weiterleitung, HSTS und CAA.

- Weiterleitung: Port 80 leitet dauerhaft auf dieselbe Adresse mit https um, etwa mit Status 301 (RFC 6797, Abschnitt 7.2) oder 308 wie bei TLSRef; die Apache-Vorlage nimmt `/.well-known/acme-challenge/` aus.
- HSTS: Strict-Transport-Security mit max-age (Pflicht) und optional includeSubDomains, nur über HTTPS senden (RFC 6797, Abschnitte 6.1 und 7.2); RFC 9325 empfiehlt es Webservern (Abschnitt 3.2).

- In Stufen einführen: hstspreload.org nennt 5 Minuten, 1 Woche und 1 Monat, vorher alle Subdomains prüfen, auch interne. Danach empfiehlt TOMORIS ein Jahr (31536000 Sekunden), TLSRef setzt zwei Jahre. Von der Preload-Liste rät hstspreload.org inzwischen ab.

Mit HSTS wird jeder Zertifikatsfehler zur Sperre: Der Browser muss etwa bei einem abgelaufenen Zertifikat abbrechen und soll kein Fortfahren anbieten (RFC 6797, Abschnitte 8.4 und 12.1). HSTS braucht deshalb eine Ablaufüberwachung.

CAA-Einträge (RFC 8659) legen fest, welche Zertifizierungsstellen für eine Domain ausstellen dürfen; sie gelten auch für Subdomains ohne eigenen Eintrag (Abschnitt 3). Öffentliche CAs müssen sie prüfen, seit 15. März 2026 mit DNSSEC-Validierung, wo eingerichtet, und ab 15. März 2027 accounturi und validationmethods auswerten (RFC 8657; Baseline Requirements 4.2.2.1 und 4.2.2.2). Den Namen Ihrer CA nennt deren Certification Practice Statement.

CAA-Einträge (Beispiel, Werte anpassen)

```
; nur diese Zertifizierungsstelle darf ausstellen, keine Wildcards
example.at. IN CAA 0 issue "ca.example.net"
example.at. IN CAA 0 issuewild ";"
example.at. IN CAA 0 iodef "mailto:security@example.at"

; enger (RFC 8657): STATT der ersten issue-Zeile, nicht zusätzlich, da CAA additiv wirkt
; (RFC 8659, 4.2); accounturi=<Konto-URL> bindet zusätzlich an ein ACME-Konto
example.at. IN CAA 0 issue "ca.example.net; validationmethods=dns-01"
```

07

Beispielkonfiguration und Prüfbefehle

nginx und Apache nach TLSRef Intermediate, Windows-Server und Prüfbefehle mit OpenSSL.

nginx: Profil Intermediate mit HSTS und Umleitung

```
# nach TLSRef Configurator (Leitlinien 6.0), Profil Intermediate (nginx 1.27.3, OpenSSL 4.0.1, HSTS)
http {
    server {
        listen 443 ssl;
        listen [::]:443 ssl;
        http2 on;
        ssl_certificate /pfad/zertifikat_plus_zwischenzertifikate;
        ssl_certificate_key /pfad/privater_schlüssel;
        add_header Strict-Transport-Security "max-age=63072000; includeSubDomains" always;
    }

    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ecdh_curve X25519MLKEM768:X25519:prime256v1:secp384r1;
    ssl_ciphers ECDHE+AESGCM:ECDHE+CHACHA20;
    ssl_prefer_server_ciphers off;
    ssl_session_timeout 1d;
    ssl_session_cache shared:MozSSL:10m;

    # HTTP dauerhaft auf HTTPS umleiten
    server {
        listen 80 default_server;
```

```
listen [::]:80 default_server;
return 308 https://$host$request_uri;
}
}
```

Apache httpd 2.4: dieselben Einstellungen

```
# nach TLSRef Configurator (Leitlinien 6.0), Apache 2.4.60; braucht mod_ssl, mod_rewrite, mod_headers
<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{REQUEST_URI} !^/\..well-known/acme-challenge/
    RewriteRule ^.*$ https://%{HTTP_HOST}%{REQUEST_URI} [R=308,QSA,L]
</VirtualHost>
<VirtualHost *:443>
    SSLEngine on
    # SSLCertificateFile und SSLCertificateKeyFile wie gewohnt
    Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains"
</VirtualHost>

SSLProtocol -all +TLSv1.2 +TLSv1.3
SSLOpenSSLConfCmd Curves X25519MLKEM768:X25519:prime256v1:secp384r1
SSLCipherSuite ECDHE+AESGCM:ECDHE+CHACHA20
SSLCipherSuite TLSv1.3 TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
SSLHonorCipherOrder off
SSLSessionTickets off
```

Die Cipher-Liste steht in OpenSSL-Kurzform (+ heißt „und“) und ergibt dieselben sechs Suiten wie im Configurator, prüfbar mit `openssl ciphers -v`. X25519MLKEM768 erst ab OpenSSL 3.5. Die Zertifikatsdatei enthält auch die Zwischenzertifikate. Eng nach TR-02102-2: ohne ChaCha20 und reines X25519, SecP256r1MLKEM768 oder SecP384r1MLKEM1024 voranstellen (ab OpenSSL 3.5), mit ECDSA.

Windows-Server mit IIS nutzen Schannel. Laut Microsoft Learn sind TLS 1.0 und 1.1 auch unter Windows Server 2025 standardmäßig aktiviert; TLS 1.3 gibt es ab Windows Server 2022. Abschalten mit dem DWORD-Wert `Enabled = 0` in den Unterschlüsseln `TLS 1.0\Server` und `TLS 1.1\Server` unter `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`; danach kann ein Neustart des Dienstes nötig sein. Microsoft rät, möglichst Gruppenrichtlinien statt direkter Registry-Änderungen zu nutzen.

Prüfen mit OpenSSL 3.x: Protokolle

```
# Verbindung: Protokoll, Cipher Suite, Gruppe, Zertifikat
openssl s_client -connect www.example.at:443 -servername www.example.at -brief </dev/null

# Gegenprobe, muss scheitern (erwartet: "alert protocol version"). OpenSSL 3.x sperrt
# TLS 1.0/1.1 schon ab Sicherheitsstufe 1 (Standard 2), daher nur hier Stufe 0
openssl s_client -connect www.example.at:443 -tls1_1 -cipher 'DEFAULT:@SECLEVEL=0' -brief </dev/null
openssl s_client -connect www.example.at:443 -tls1 -cipher 'DEFAULT:@SECLEVEL=0' -brief </dev/null
```

Prüfen mit OpenSSL 3.x: Zertifikat, Kette, Mailserver

```
# Aussteller, Namen, Ablauf; Exit-Code ungleich 0, wenn es in 14 Tagen abläuft
openssl s_client -connect www.example.at:443 -servername www.example.at </dev/null 2>/dev/null \
| openssl x509 -noout -subject -issuer -enddate -ext subjectAltName -checkend 1209600

# vom Server gesendete Kette (ungeprüft, in Senderreihenfolge)
openssl s_client -connect www.example.at:443 -servername www.example.at -showcerts </dev/null

# Mailserver mit STARTTLS
openssl s_client -connect mail.example.at:25 -starttls smtp -brief </dev/null
```

08

Interne Dienste und Sperrprüfung

Mail, VPN und Geräte nicht vergessen; was sich bei OCSP und Sperrlisten geändert hat.

- Mail: Gibt es einen eigenen TLS-Port und STARTTLS, ist laut RFC 9325 der TLS-Port vorzuziehen, bei reinem STARTTLS eine strikte Richtlinie ohne Klartext-Rückfall (Abschnitt 3.2); zwischen Mailservern nennt RFC 9325 MTA-STS.
- VPN: in geschlossenen Systemen ist laut BSI meist eine beidseitige Authentisierung notwendig (TR-02102-2, Abschnitt 3.5). Drucker, NAS, Hypervisor, Switches: Weboberfläche prüfen, Firmware aktualisieren, TLS 1.0 und 1.1 abschalten, wo möglich.
- Interne Namen wie server.firma.local: Dafür stellen öffentliche CAs nicht aus (Baseline Requirements 4.2.2). Eigene PKI oder öffentliche Namen nutzen; für eine eigene PKI gelten die Baseline Requirements nicht (1.1).

Sperrprüfung: was seit 2025 gilt

Sperrliste (CRL)

Pflicht für öffentliche CAs: per HTTP veröffentlichen, für Endnutzer-Zertifikate mindestens alle 7 Tage (mit OCSP-Adresse) bzw. 4 Tage (ohne) und binnen 24 Stunden nach einer Sperrung erneuern (Baseline Requirements 4.9.7).

OCSP

Die OCSP-Adresse im Zertifikat ist nur noch erlaubt, nicht vorgeschrieben (7.1.2.7.7). Let's Encrypt hat sie am 7. Mai 2025 entfernt, Must-Staple abgelehnt und OCSP am 6. August 2025 abgeschaltet, vor allem aus Datenschutzgründen; es bleiben CRLs. Ohne OCSP-Adresse entfällt Stapling (im TLSRef Configurator standardmäßig abgewählt). Let's Encrypt rät, VPN und andere Software darauf zu testen.

Kurzlebige Zertifikate

Bis 7 Tage Laufzeit (seit 15. März 2026): Die CA muss sie nicht sperren können, eine CRL-Adresse ist optional (Baseline Requirements 4.9.1.1, 7.1.2.11.2).

09 —

Checkliste zum Abhaken

Alle Punkte in einer Liste zum Abhaken.

- ☐ TLS 1.3 aktiv und bevorzugt, TLS 1.2 nur mit ECDHE und AEAD; TLS 1.0, 1.1, SSL 2.0 und 3.0 auf allen Diensten aus und mit `openssl s_client` gegengeprüft.
- ☐ Keine Suiten mit RSA-Schlüsseltransport, DH oder DHE (TLS_RSA_*, TLS_DH_*, TLS_DHE_*, RFC 10015), kein statisches ECDH, kein RC4, 3DES oder NULL; 0-RTT, Kompression und Heartbeat aus.
- ☐ Schlüssel ECDSA P-256 oder P-384 oder RSA ab 3000 Bit (BSI), mindestens 2048 Bit; Signatur SHA-256 oder stärker; privater Schlüssel geschützt gespeichert (BSI, Abschnitt 4.1).
- ☐ Vollständige Kette ausgeliefert (`-showcerts`); subjectAltName deckt alle genutzten Namen ab.
- ☐ Jedes öffentliche Zertifikat samt Domain-Nachweis per ACME, Erneuerung nach ARI oder bei zwei Dritteln der Laufzeit, danach neu laden; Ausnahmen bis 15. März 2027 umstellen.
- ☐ Inventar mit Ablauf, Erneuerungsweg und Zuständigkeit, auch bei Hostern; CT-Logs geprüft.
- ☐ HTTP leitet dauerhaft auf HTTPS um; HSTS mindestens ein Jahr, includeSubDomains erst, wenn alle Subdomains HTTPS können.
- ☐ CAA-Einträge für alle Domains mit den genutzten Zertifizierungsstellen und einer iodef-Adresse.
- ☐ Mail, VPN, Drucker, NAS und weitere Geräte geprüft und im Inventar; interne Namen über eine eigene PKI; Software kommt ohne OCSP aus.
- ☐ Jährlich gegen TR-02102-2 und TLSRef geprüft; hybride Schlüsseleinigung bis Ende 2031 geplant.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

SSL/TLS-Check

tomoris.com/tools/ssl-tls-check

Security-Header-Check

tomoris.com/tools/security-header-check

DNS-Sicherheits-Check

tomoris.com/tools/dns-security-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

10 —

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **BSI TR-02102-2: Verwendung von TLS, Version 2026-01**
PDF vom 27.01.2026: Kap. 1, 3.2 bis 3.6, 4.1; Hinweis zu TLS 1.3 (RFC 10024) auf der Seite
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards
- 2 **CA/Browser Forum: TLS Baseline Requirements 2.3.1**
vom 4.10.2026; 1.1, 1.2.2, 3.2.2.4, 4.2.1, 4.2.2, 4.9, 6.1.5, 6.3.2, 7.1.2
cabforum.org/working-groups/server/baseline-requirements/requirements
- 3 **CA/Browser Forum: EV Guidelines 2.0.4**
13.8.2026; 3.2.2.14.3 (398 Tage seit SC042, 2021)
cabforum.org/working-groups/server/extended-validation/guidelines
- 4 **CA/Browser Forum: Ballot SC-081v3**
Stufenplan, Abstimmung vom 11.4.2025
cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-revisions
- 5 **RFC 9846: TLS 1.3 (ersetzt RFC 8446)**
Juli 2026; Abschnitte 1.2 und 1.3
www.rfc-editor.org/rfc/rfc9846.html
- 6 **RFC 8996: Deprecating TLS 1.0 and TLS 1.1**
Abschnitte 4 und 5
www.rfc-editor.org/rfc/rfc8996.html
- 7 **RFC 9325 (BCP 195): Secure Use of TLS**
Abschnitte 3.1.1, 3.2, 3.3, 4.1 und 4.5
www.rfc-editor.org/rfc/rfc9325.html
- 8 **RFC 9852 und RFC 10015 (Juli 2026): Änderungen an RFC 9325**
9852: 4, 5; 10015: 2 bis 4, 6 (www.rfc-editor.org/rfc/rfc10015.html)
www.rfc-editor.org/rfc/rfc9852.html
- 9 **RFC 10024: PQ/T Hybrid Key Agreement for TLS 1.3**
August 2026; X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024
www.rfc-editor.org/rfc/rfc10024.html
- 10 **RFC 8555: ACME**
Abschnitte 8.3 und 8.4
www.rfc-editor.org/rfc/rfc8555.html
- 11 **RFC 8737: ACME TLS-ALPN-01**
Abschnitt 3
www.rfc-editor.org/rfc/rfc8737.html
- 12 **RFC 9773: ACME Renewal Information (ARI)**
Abschnitt 1
www.rfc-editor.org/rfc/rfc9773.html
- 13 **RFC 6797: HSTS**
Abschnitte 6.1, 7.2, 8.4 und 12.1
www.rfc-editor.org/rfc/rfc6797.html
- 14 **RFC 8659 und RFC 8657: CAA**
8659: 3, 4.1 bis 4.4; 8657: 4, Anhang A
(www.rfc-editor.org/rfc/rfc8657.html)
www.rfc-editor.org/rfc/rfc8659.html
- 15 **RFC 6962: Certificate Transparency**
experimentell, formal ersetzt durch RFC 9162; Zusammenfassung
www.rfc-editor.org/rfc/rfc6962.html
- 16 **TLSRef Configurator (vormals Mozilla) und Leitlinien 6.0**
Vorlagen nginx, Apache (Build 6bcb595); docs.tlsref.org/server-side-tls.html; Umzug:
github.com/mozilla/ssl-config-generator
configurator.tlsref.org
- 17 **Let's Encrypt: Ende von OCSP**
6.8.2025; Zeitplan im Beitrag vom 5.12.2024
letsencrypt.org/2025/08/06/ocsp-service-has-reached-end-of-life
- 18 **Let's Encrypt: Laufzeiten bis 45 Tage**
2.12.2025; Zeitplan, Profile, ARI, Überwachung; bestätigt in
letsencrypt.org/2026/10/07/64-day-certs
letsencrypt.org/2025/12/02/from-90-to-45
- 19 **OpenSSL 3.5: Dokumentation**
s_client, x509, ciphers, SSL_CTX_set_security_level
docs.openssl.org/3.5
- 20 **Microsoft Learn: Protokolle in TLS/SSL (Schannel) und TLS-Registrierungseinstellungen**
Versionen je Windows; Registry:
learn.microsoft.com/de-de/windows-server/security/tls/tls-registry-settings
learn.microsoft.com/de-de/windows/win32/secauthn/protocols-in-tls
- 21 **hstspreload.org: HSTS einführen, Preload**
gelesen am 25.10.2026
hstspreload.org
- 22 **NISG 2026, BGBl. I Nr. 94/2025 (RIS)**
§ 32 und § 51 Abs. 2; Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=2025094
- 23 **NISV 2026, BGBl. II Nr. 290/2026 (RIS)**
§ 2
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 24 **DVO (EU) 2024/2690, Anhang Nr. 9**
Kryptografie; anwendbar nach § 2 NISV 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu