TOMORIS
MORE THAN IT

FREE DOWNLOAD

CHECKLIST · TOMORIS TOOLBOX

TLS and Certificates: Checklist for Servers and Websites

Protocols, keys, validity down to 47 days, ACME, inventory, HSTS and CAA according to BSI TR-02102-2, the CA/Browser Forum and the IETF, with configuration and test commands

UPDATED	LENGTH	ONLINE
Oct 25, 2026	PDF, 12 pages	tomoris.com/en/downloads/tls-zertifikate-checkliste

AT A GLANCE

200 days
maximum validity of public certificates since Mar 15, 2026

47 days
maximum validity from Mar 15, 2029 (CA/Browser Forum)

TLS 1.3
Preferred; BSI allows TLS 1.2 only until end of 2031

10 days
maximum validity of domain validation from Mar 15, 2029

WHO IT IS FOR

- Administrators of web, mail and VPN servers, reverse proxies and load balancers
- Web agencies and hosting providers that run websites and certificates for customers
- Website owners and IT management who need to keep track of certificates, service providers and deadlines

Redistribution in unchanged form permitted

WHAT THIS COVERS

Since March 15, 2026, public TLS certificates have been valid for at most 200 days; from March 2029, only 47 days, and domain validation will then be valid for only 10 days. Anyone who renews certificates by hand will have an operational problem. This checklist covers protocols, cipher suites and keys according to BSI TR-02102-2 (version 2026-01) and TLSRef, automation with ACME, inventory and expiry monitoring, HSTS, CAA, internal services and revocation checking after the end of OCSP at Let's Encrypt. It also includes sample configurations for nginx and Apache and test commands with OpenSSL.

This checklist is a TOMORIS recommendation based on the sources listed, as of October 25, 2026. For certification authorities, the Baseline Requirements as currently in force are binding; for essential and important entities, the NISG 2026; BSI TR-02102-2 is a recommendation. It does not replace legal advice. Default values and names may change. Test changes in a test environment first; overly strict settings can lock out older clients.

CONTENTS

01 What this is about and what is required 3
02 Validity periods: the phased plan to 2029 3
03 Protocols, cipher suites and keys 4
04 Automating with ACME 6
05 Inventory and expiry monitoring 7
06 Enforcing HTTPS: redirect, HSTS and CAA 7
07 Sample configuration and test commands 8
08 Internal services and revocation checking 10
09 Checklist to tick off 11
10 Sources 12

01

What this is about and what is required

Why certificates are getting shorter lifetimes, what the NISG 2026 (Austrian Network and Information Systems Security Act 2026) requires and what is only a recommendation.

TLS encrypts connections to websites, mail and VPN servers and devices; the certificate proves that the server belongs to the name. Besides the validity periods (section 02), the BSI (German Federal Office for Information Security) recommendation changes in 2026: TR-02102-2, version 2026-01 of January 27, 2026, recommends TLS 1.2 only until the end of 2031, because no quantum-safe key agreement methods are expected to be standardized for it (Section 3.2).

What is required and what is recommended

REQUIREMENT	FOR WHOM	BASIS
Cryptography policy: protocols, algorithms, keys and certificates, according to the state of the art	essential and important entities, since Oct 1, 2026	§ 32 para. 4 lit. h NISG 2026; § 2 NISV 2026 (Austrian NIS Regulation 2026) with Annex point 9 IR (EU) 2024/2690
Validity, domain validation, CAA, revocation	public certification authorities, affects all users	Baseline Requirements 2.3.1 of Oct 4, 2026
Do not use TLS 1.0 and 1.1, prefer TLS 1.3	operators of TLS services (IETF recommendation, not legally binding)	RFC 8996; RFC 9325 Section 3.1.1, amended by RFC 9852 and RFC 10015 (July 2026)
Versions, cipher suites, key lengths	recommendation, not binding in Austria	BSI TR-02102-2, version 2026-01
all other points	all operators	TOMORIS recommendation

> The Baseline Requirements bind certification authorities once browser and software vendors enforce them (Section 1.1). § 32 NISG 2026 does not prescribe a specific method but requires appropriate, proportionate measures according to the state of the art (paras. 1 and 2).

02

Validity periods: the phased plan to 2029

Maximum validity and domain validation decrease in three steps; the first has applied since March 15, 2026.

Phased plan under Ballot SC-081v3 (Baseline Requirements 2.3.1, Sections 6.3.2 and 4.2.1)

CERTIFICATE ISSUED	MAXIMUM VALIDITY	MAXIMUM DOMAIN VALIDATION REUSE
before Mar 15, 2026	398 days	398 days
from Mar 15, 2026 (applies now)	200 days	200 days

from Mar 15, 2027	100 days	100 days
from Mar 15, 2029	47 days	10 days

CAs should stay one day below each limit (199, 99, 46 days), because a day has 86,400 seconds and even fractions beyond that count as another day (Section 6.3.2). Since March 15, 2026, validated organization information for OV certificates may be reused for at most 398 instead of 825 days (4.2.1); for EV, the EV Guidelines (3.2.2.14.3) have already set a maximum of 398 days since 2021. SC-081v3 was adopted on April 11, 2025, without any votes against.

- At 47 days, every name needs at least eight certificates a year, and at 10 days domain validation is practically due again every time. Let's Encrypt advises against manual renewal; validation must also run automatically (section 04).
- In case of a compromised key and some other reasons, such as unreliable domain validation, the CA must revoke within 24 hours, in other cases within 5 days (Section 4.9.1.1). So a replacement must be possible at short notice at any time.

> Let's Encrypt is shortening sooner (announcement of December 2, 2025): tlsserver profile with 45 days since May 13, 2026; classic default profile with 64 days and 10 days of domain validation reuse from February 10, 2027 (confirmed on October 7, 2026), and with 45 days and 7 hours from February 16, 2028; shortlived profile with about 6 days.

03

Protocols, cipher suites and keys

Prefer TLS 1.3, TLS 1.2 only with forward secrecy, turn off anything older, choose keys correctly.

TLS versions according to BSI TR-02102-2 (Table 2), RFC 8996, RFC 9325 and RFC 9852

VERSION	RECOMMENDATION	REFERENCE
TLS 1.3	use preferentially; BSI: until 2032, possibly longer (stated as 2032+)	TR-02102-2 Section 3.2; RFC 9325 Section 3.1.1; RFC 9852: new protocols must require TLS 1.3
TLS 1.2	keep enabled for older clients; BSI: only until the end of 2031	TR-02102-2 Section 3.2; RFC 9325 Section 3.1.1 required it, RFC 9852 (July 2026) makes it optional
TLS 1.0, 1.1	turn off	RFC 8996: "MUST NOT be used"; not recommended by the BSI
SSL 2.0, 3.0	turn off	RFC 9325 Section 3.1.1; TR-02102-2 Section 3.2

TLS 1.3 `TLS_AES_128_GCM_SHA256`	AEAD algorithms only, every key exchange via public keys with forward secrecy (RFC 9846, Section 1.3; replaces RFC 8446 since July 2026). BSI: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_AES_128_CCM_SHA256 (Table 13). TLSRef adds TLS_CHACHA20_POLY1305_SHA256, which TR-02102-2 does not list; the BSI does not necessarily consider anything not listed to be insecure (Chapter 1). Neither send nor accept 0-RTT data (Section 3.4.1).
TLS 1.2 `ECDHE+AESGCM:ECDHE+CHACHA20`	Only ECDHE with AES-GCM or ChaCha20-Poly1305, the six suites of TLSRef Intermediate. Since RFC 10015 (July 2026, amends RFC 9325 Section 4.1), TLS_RSA_*, TLS_DH_* and TLS_DHE_* must no longer be negotiated in TLS 1.2 (MUST NOT), and static ECDH is discouraged. BSI: CBC only with Encrypt-then-MAC, DHE until 2029 (the IETF is stricter here), Extended Master Secret yes (3.3.1, 3.3.4). Compression off (RFC 9325 Section 3.3), heartbeat off (BSI 3.3.4.6).
Groups	TLSRef 6.0: X25519MLKEM768 (hybrid, quantum-safe, from OpenSSL 3.5), X25519, P-256, P-384. BSI: secp256r1, secp384r1, secp521r1, Brainpool, ffdhe3072/4096 (Table 10), not X25519; classical alone only until the end of 2031. Since RFC 10024 (August 2026), according to the BSI, SecP256r1MLKEM768 and SecP384r1MLKEM1024 may be used in compliance with the TR (recommendation announced for the next TR version), as well as X25519MLKEM768.

Keys and signatures of public certificates

TOPIC	MINIMUM	RECOMMENDATION
ECDSA	only P-256, P-384 or P-521 (Baseline Requirements 6.1.5)	P-256 (TLSRef) or P-384; BSI: at least 250 bits. The Brainpool curves preferred by the BSI are not permitted for public certificates.
RSA	2048 bits (6.1.5; RFC 9325)	BSI: at least 3000 bits (Table 14), for example 3072 bits; TLSRef Intermediate: 2048 bits
Signature	no SHA-1; long excluded for server certificates, the last exceptions for CA certificates and CRLs ended on Sep 15, 2026 (Baseline Requirements 1.2.2, 7.1.3.2.1)	SHA-256 or stronger; the BSI recommends RSA with PKCS #1 v1.5 only until 2025, RSA-PSS and ECDSA beyond that (Tables 7 and 12)

TLSRef is the successor to the Mozilla SSL Configuration Generator (ssl-config.mozilla.org redirects; according to Mozilla, a community working group outside Mozilla maintains the project). Intermediate allows the sha256WithRSAEncryption signature (PKCS #1 v1.5); if you follow TR-02102-2 closely, check the chain and choose ECDSA with a CA that has an ECDSA intermediate certificate.

04

Automating with ACME

Request, domain validation and renewal without manual work, with monitoring.

ACME (RFC 8555) is the IETF standard for request, domain validation and renewal without manual work; whether your CA offers it is stated in its documentation. The most common ACME validation methods (others such as dns-account-01, Baseline Requirements 3.2.2.4.21, are being added):

http-01 `/.well-known/acme-challenge/`	The CA fetches a file over HTTP on TCP port 80 (RFC 8555, Section 8.3); port 80 must stay open. Not for wildcards (Baseline Requirements 3.2.2.4).
dns-01 `_acme-challenge TXT`	TXT record (RFC 8555, Section 8.4), also for wildcards and systems not reachable from the internet. Requires write access to the DNS zone; TOMORIS recommends limiting it tightly.
tls-alpn-01	Validation via a dedicated TLS handshake with ALPN (Baseline Requirements 3.2.2.4.20, based on RFC 8737), if port 80 is to stay closed. Not for wildcards.
Persistent record `_validation-persist TXT`	New (Baseline Requirements 3.2.2.4.22, Ballot SC-088v3): names the CA and account and stays the same across renewals; a validation based on it is valid for at most 10 days. Let's Encrypt has announced DNS-PERSIST-01 for this.

- Schedule renewal: ideally using ACME Renewal Information (ARI, RFC 9773), so that the CA suggests a time window, for example earlier ahead of a mass revocation. Without ARI, Let's Encrypt considers renewal after about two thirds of the validity period suitable; a fixed 60 days is not enough at 45 days.
- Deploy and reload: the service must load the new certificate, including on load balancers, firewalls or appliances. After the first automatic renewal, check with the commands from section 07.
- Get alerted to failures: Let's Encrypt recommends monitoring that raises an alert if renewal does not happen as expected. TOMORIS recommends checking from the outside what the service actually delivers.

> Confirmation by phone or email is being phased out: the Baseline Requirements exclude domain validation by phone from March 15, 2027 (3.2.2.4.16, 3.2.2.4.17) and by email to contacts such as admin@ from March 15, 2028 (3.2.2.4.4, 3.2.2.4.13, 3.2.2.4.14; Ballot SC-090).

05

Inventory and expiry monitoring

Record every certificate with expiry date and owner and monitor it from the outside.

For entities under the NISG 2026, Implementing Regulation (EU) 2024/2690 (via § 2 NISV 2026, Austrian NIS Regulation 2026) requires a key management policy covering, where appropriate, among other things the issuance and obtaining of public key certificates, key changes, revocation and activation periods (Annex point 9.2(c), items ii, v, vii and xii). An inventory is the simplest basis for this and benefits every business.

Template: certificate inventory (one row per name and service)

SERVICE AND NAME	ISSUER	EXPIRES	RENEWAL	OWNER
Website: [www.domain]	_____	_____	_____	_____
Mail: SMTP, IMAP, webmail	_____	_____	_____	_____
VPN, firewall, proxy	_____	_____	_____	_____
Printers, NAS, devices	_____	_____	_____	_____
Internal applications	_____	_____	_____	_____

- [ ] All names recorded, including subdomains, remote access and certificates at hosting or service providers; under Renewal, enter “ACME” or the manual procedure with a date.
- [ ] Unknown certificates searched for: Certificate Transparency (RFC 6962) logs issued certificates publicly; a search for your domains shows certificates outside the inventory.
- [ ] External monitoring per service and port; TOMORIS recommends a warning at one third of remaining validity and an alert at seven days, sent to a group rather than one person.

06

Enforcing HTTPS: redirect, HSTS and CAA

Redirect HTTP permanently, introduce HSTS in stages, use CAA to define the issuers.

Three building blocks ensure that visitors connect only over encrypted connections and only the intended certification authority may issue certificates: redirect, HSTS and CAA.

- Redirect: port 80 permanently redirects to the same address with https, for example with status 301 (RFC 6797, Section 7.2) or 308 as in TLSRef; the Apache template excludes /.well-known/acme-challenge/.
- HSTS: Strict-Transport-Security with max-age (required) and optionally includeSubDomains, sent only over HTTPS (RFC 6797, Sections 6.1 and 7.2); RFC 9325 recommends it for web servers (Section 3.2).

- Introduce in stages: hstspreload.org suggests 5 minutes, 1 week and 1 month, checking all subdomains beforehand, including internal ones. After that, TOMORIS recommends one year (31536000 seconds); TLSRef sets two years. hstspreload.org now advises against the preload list.

> With HSTS, every certificate error becomes a hard block: the browser must abort, for example with an expired certificate, and should not offer to proceed (RFC 6797, Sections 8.4 and 12.1). HSTS therefore requires expiry monitoring.

CAA records (RFC 8659) specify which certification authorities may issue for a domain; they also apply to subdomains without their own record (Section 3). Public CAs must check them, since March 15, 2026, with DNSSEC validation where set up, and from March 15, 2027, they must evaluate accounturi and validationmethods (RFC 8657; Baseline Requirements 4.2.2.1 and 4.2.2.2). The name of your CA is given in its Certification Practice Statement.

CAA records (example, adjust values)

```
; only this certification authority may issue, no 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"

; stricter (RFC 8657): INSTEAD OF the first issue line, not in addition, since CAA is additive
; (RFC 8659, 4.2); accounturi=<account URL> additionally binds to an ACME account
example.at. IN CAA 0 issue "ca.example.net; validationmethods=dns-01"
```

07

Sample configuration and test commands

nginx and Apache based on TLSRef Intermediate, Windows Server and test commands with OpenSSL.

nginx: Intermediate profile with HSTS and redirect

```
# based on TLSRef Configurator (guidelines 6.0), Intermediate profile (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_schluessel;
        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;

    # redirect HTTP permanently to HTTPS
    server {
        listen 80 default_server;
```

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

Apache httpd 2.4: the same settings

```
# based on TLSRef Configurator (guidelines 6.0), Apache 2.4.60; requires 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 and SSLCertificateKeyFile as usual
    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
```

> The cipher list is in OpenSSL shorthand (+ means “and”) and results in the same six suites as in the Configurator, verifiable with `openssl ciphers -v`. X25519MLKEM768 only from OpenSSL 3.5. The certificate file also contains the intermediate certificates. Strictly following TR-02102-2: without ChaCha20 and pure X25519, put SecP256r1MLKEM768 or SecP384r1MLKEM1024 first (from OpenSSL 3.5), with ECDSA.

Windows servers with IIS use Schannel. According to Microsoft Learn, TLS 1.0 and 1.1 are still enabled by default even on Windows Server 2025; TLS 1.3 is available from Windows Server 2022. Turn them off with the DWORD value `Enabled` = 0 in the subkeys `TLS 1.0\Server` and `TLS 1.1\Server` under `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`; a restart of the service may be required afterwards. Microsoft advises using Group Policy rather than direct registry changes where possible.

Testing with OpenSSL 3.x: protocols

```
# connection: protocol, cipher suite, group, certificate
openssl s_client -connect www.example.at:443 -servername www.example.at -brief </dev/null

# counter-check, must fail (expected: "alert protocol version"). OpenSSL 3.x blocks
# TLS 1.0/1.1 already from security level 1 (default 2), so level 0 only here
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
```

Testing with OpenSSL 3.x: certificate, chain, mail server

```
# issuer, names, expiry; exit code not 0 if it expires within 14 days
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

# chain sent by the server (unverified, in the order sent)
openssl s_client -connect www.example.at:443 -servername www.example.at -showcerts </dev/null

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

08

Internal services and revocation checking

Do not forget mail, VPN and devices; what has changed with OCSP and CRLs.

- Mail: if there is a dedicated TLS port and STARTTLS, RFC 9325 prefers the TLS port; with STARTTLS only, a strict policy without plaintext fallback (Section 3.2); between mail servers, RFC 9325 mentions MTA-STS.
- VPN: in closed systems, mutual authentication is usually necessary according to the BSI (TR-02102-2, Section 3.5). Printers, NAS, hypervisors, switches: check the web interface, update the firmware, turn off TLS 1.0 and 1.1 where possible.
- Internal names such as server.firma.local: public CAs do not issue certificates for them (Baseline Requirements 4.2.2). Use your own PKI or public names; the Baseline Requirements do not apply to your own PKI (1.1).

Revocation checking: what has applied since 2025

Certificate revocation list (CRL)	Mandatory for public CAs: publish via HTTP, for end-entity certificates at least every 7 days (with OCSP URL) or 4 days (without), and update within 24 hours after a revocation (Baseline Requirements 4.9.7).
OCSP	The OCSP URL in the certificate is now only permitted, not required (7.1.2.7.7). Let's Encrypt removed it on May 7, 2025, rejected Must-Staple and shut down OCSP on August 6, 2025, mainly for privacy reasons; CRLs remain. Without an OCSP URL, stapling no longer applies (deselected by default in the TLSRef Configurator). Let's Encrypt advises testing VPN and other software for this.
Short-lived certificates	Validity of up to 7 days (since March 15, 2026): the CA does not have to be able to revoke them, and a CRL URL is optional (Baseline Requirements 4.9.1.1, 7.1.2.11.2).

09

Checklist to tick off

All points in one list to tick off.

- [ ] TLS 1.3 enabled and preferred, TLS 1.2 only with ECDHE and AEAD; TLS 1.0, 1.1, SSL 2.0 and 3.0 off on all services and cross-checked with `openssl s_client`.
- [ ] No suites with RSA key transport, DH or DHE (TLS_RSA_*, TLS_DH_*, TLS_DHE_*, RFC 10015), no static ECDH, no RC4, 3DES or NULL; 0-RTT, compression and heartbeat off.
- [ ] Keys ECDSA P-256 or P-384, or RSA with at least 3000 bits (BSI), minimum 2048 bits; signature SHA-256 or stronger; private key stored securely (BSI, Section 4.1).
- [ ] Complete chain delivered (`-showcerts`); subjectAltName covers all names in use.
- [ ] Every public certificate including domain validation via ACME, renewal according to ARI or at two thirds of the validity period, followed by a reload; migrate exceptions by March 15, 2027.
- [ ] Inventory with expiry, renewal method and owner, including at hosting providers; CT logs checked.
- [ ] HTTP redirects permanently to HTTPS; HSTS for at least one year, includeSubDomains only once all subdomains support HTTPS.
- [ ] CAA records for all domains with the certification authorities in use and an iodef address.
- [ ] Mail, VPN, printers, NAS and other devices checked and in the inventory; internal names via your own PKI; software works without OCSP.
- [ ] Checked annually against TR-02102-2 and TLSRef; hybrid key agreement planned by the end of 2031.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

SSL/TLS check (German)
tomoris.com/tools/ssl-tls-check

Security header check (German)
tomoris.com/tools/security-header-check

DNS security check (German)
tomoris.com/tools/dns-security-check

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact

contact@tomoris.com

10

Sources

All statements are supported by sources. Legislation applies in its current version.

1 **BSI TR-02102-2: Use of TLS, version 2026-01**
PDF of January 27, 2026: chap. 1, 3.2 to 3.6, 4.1; note on TLS 1.3 (RFC 10024) on the page
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standa...

2 **CA/Browser Forum: TLS Baseline Requirements 2.3.1**
of October 4, 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/requir...

3 **CA/Browser Forum: EV Guidelines 2.0.4**
August 13, 2026; 3.2.2.14.3 (398 days since SC042, 2021)
cabforum.org/working-groups/server/extended-validation/guidelin...

4 **CA/Browser Forum: Ballot SC-081v3**
Phased plan, vote of April 11, 2025
cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-re...

5 **RFC 9846: TLS 1.3 (replaces RFC 8446)**
July 2026; Sections 1.2 and 1.3
www.rfc-editor.org/rfc/rfc9846.html

6 **RFC 8996: Deprecating TLS 1.0 and TLS 1.1**
Sections 4 and 5
www.rfc-editor.org/rfc/rfc8996.html

7 **RFC 9325 (BCP 195): Secure Use of TLS**
Sections 3.1.1, 3.2, 3.3, 4.1 and 4.5
www.rfc-editor.org/rfc/rfc9325.html

8 **RFC 9852 and RFC 10015 (July 2026): amendments to RFC 9325**
9852: 4, 5; 10015: 2 to 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**
Sections 8.3 and 8.4
www.rfc-editor.org/rfc/rfc8555.html

11 **RFC 8737: ACME TLS-ALPN-01**
Section 3
www.rfc-editor.org/rfc/rfc8737.html

12 **RFC 9773: ACME Renewal Information (ARI)**
Section 1
www.rfc-editor.org/rfc/rfc9773.html

13 **RFC 6797: HSTS**
Sections 6.1, 7.2, 8.4 and 12.1
www.rfc-editor.org/rfc/rfc6797.html

14 **RFC 8659 and RFC 8657: CAA**
8659: 3, 4.1 to 4.4; 8657: 4, Appendix A (www.rfc-editor.org/rfc/rfc8657.html)
www.rfc-editor.org/rfc/rfc8659.html

15 **RFC 6962: Certificate Transparency**
experimental, formally replaced by RFC 9162; summary
www.rfc-editor.org/rfc/rfc6962.html

16 **TLSRef Configurator (formerly Mozilla) and guidelines 6.0**
nginx and Apache templates (build 6bcb595); docs.tlsref.org/server-side-tls.html; move: github.com/mozilla/ssl-config-generator
configurator.tlsref.org

17 **Let's Encrypt: End of OCSP**
August 6, 2025; timeline in the post of December 5, 2024
letsencrypt.org/2025/08/06/ocsp-service-has-reached-end-of-life

18 **Let's Encrypt: Validity down to 45 days**
December 2, 2025; timeline, profiles, ARI, monitoring; confirmed in letsencrypt.org/2026/10/07/64-day-certs
letsencrypt.org/2025/12/02/from-90-to-45

19 **OpenSSL 3.5: Documentation**
s_client, x509, ciphers, SSL_CTX_set_security_level
docs.openssl.org/3.5

20 **Microsoft Learn: Protocols in TLS/SSL (Schannel SSP) and TLS registry settings**
Versions per Windows release; registry: learn.microsoft.com/de-de/windows-server/security/tls/tls-registry-settings
learn.microsoft.com/de-de/windows/win32/secauthn/protocols-in-t...

21 **hstspreload.org: Deploying HSTS, preload**
accessed October 25, 2026
hstspreload.org

22 **NISG 2026, BGBl. I No. 94/2025 (RIS)**
§ 32 and § 51 para. 2; version of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

23 **NISV 2026, BGBl. II No. 290/2026 (RIS)**
§ 2
www.ris.bka.gv.at/eli/bgbl/II/2026/290

24 **IR (EU) 2024/2690, Annex point 9**
Cryptography; applicable under § 2 NISV 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu