SICHERGENUG.DE – KRYPTO-CHECK ORIENTIERT AN BSI TR-02102

Krypto-Prüfbericht (TLS/SSH/PQC)

Dokumentationshilfe zu § 30 Abs. 2 Nr. 8 BSIG – orientiert an BSI TR-02102-2

Technische Untersuchung der Transportverschlüsselung (TLS/SSH), Zertifikatsinfrastruktur, DANE/TLSA-Empfehlungen (BSI TR-03108) sowie der Post-Quanten-Kryptografie-Bereitschaft (ML-KEM / FIPS 203)

Privates Angebot – keine Stelle des BSI oder einer Behörde, keine Zertifizierung.

1. Prüfgegenstand & Stammdaten des Scans

Geprüfte Haupt-Domain	**musterfirma.example**
Scan-Identifikationsnummer	`SG-NIS2-B16CEDE2CC`
Prüfzeitpunkt (UTC) & Scanner-IP	29.10.2026 15:35 UTC | Quell-IP (IPv4): `203.0.113.10` (IPv4-gebundene Messung; reine IPv6-Only-Ziele ohne A-Record erscheinen als geschlossen)
Regulatorischer Kontext & Maßstab	BSI TR-02102-2, BSI TR-02102-4, BSI TR-03108 | Kontext: § 30 Abs. 2 Nr. 8 BSIG (NIS-2), § 38 BSIG, DORA Art. 9
Gesamtergebnis (Ampelstatus)	ROT – KRITISCHER HANDLUNGSBEDARF (ABWEICHUNGEN NACH BSI TR-02102-2)
Erreichter Krypto-Score	**61 / 100 Punkte**
Erfasste Subdomains / Aktive Ports	9 Subdomains erkannt | 8 aktive TLS/SSH-Endpunkte detailliert vermessen

MUSTER

Einordnung für Geschäftsleitung & Aufsichtsgremien

Dieser Bericht dokumentiert den technischen Ist-Zustand der extern gemessenen kryptografischen Außenschnittstellen der Domain **musterfirma.example** zum Stichtag 29.10.2026 15:35 UTC. Zusammen mit dem beigefügten maschinenlesbaren Krypto-Inventar (`cbom.json` nach CycloneDX v1.6) und der Muster-Kryptografie-Richtlinie dient dieses Dokument als technische Dokumentation für Ihre Nachweisführung im Rahmen des Risikomanagements zu § 30 Abs. 2 Nr. 8 BSIG. Privates Angebot – keine Stelle des BSI oder einer Behörde, keine Zertifizierung.

Kurz-Kennzahlen der Untersuchung

61/100	1	0	2	3	2	1/8
KRYPTO-SCORE	ENTSPRECHEND (GRÜN)	WEITGEHEND ENTSPRECHEND (GELB)	TEILWEISE ENTSPRECHEND (ORANGE)	DEUTLICHE ABWEICHUNGEN (DUNKELORANGE)	KRITISCH (ROT)	PQC (ML-KEM) AKTIV

2. Management Summary & Geschäftsleiter-Relevanz (§ 38 BSIG)

Mit dem Inkrafttreten des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (BSIG) sowie des Digital Operational Resilience Act (DORA) unterliegen Geschäftsleiter einer persönlichen Billigungs-, Überwachungs- und Schulungspflicht (§ 38 BSIG). Ein zentraler Prüfpunkt in § 30 Abs. 2 Nr. 8 BSIG ist die wirksame Implementierung von Konzepten und Verfahren für den Einsatz von Kryptografie und Verschlüsselung.

Kernaussage für die Geschäftsleitung (musterfirma.example)

Die automatisierte Prüfung von **musterfirma.example** ergab einen Krypto-Score von **61 von 100 Punkten** (Kritischer Handlungsbedarf (Abweichungen nach BSI TR-02102-2)). Von 8 untersuchten kryptografischen Diensten unterstützt derzeit **1 Endpunkt** hybride Post-Quanten-Schlüsselaustauschverfahren (ML-KEM).

Zusammenfassung der wichtigsten Feststellungen

Prüfbereich	Technischer Befund	Bewertung nach BSI / NIS-2
Transportverschlüsselung (BSI TR-02102-2)	8 aktive TLS/SSH-Dienste identifiziert. Erkannte Server-Stacks: Dovecot, Postfix, SSH-2.0-OpenSSH_8.9p1, Standard Server, envoy, nginx.	SOFORTMASSNAHME
Post-Quantum Readiness (ML-KEM / FIPS 203)	1 von 8 Diensten nutzen hybrides Key-Establishment (X25519MLKEM768 / sntrup761).	MIGRATION NÖTIG
E-Mail-Transport & DNS-Härtung (BSI TR-03108)	SPF: Vorhanden | DMARC: Vorhanden | MX-Gateways: 1	EINGERICHTET
Krypto-Agilität & CBOM-Inventar	CycloneDX v1.6 Krypto-Inventar der extern gemessenen Endpunkte (`cbom.json`) wurde erstellt.	CBOM ERSTELLT

MUSTER

Wirtschaftliches & Haftungsrechtliches Risiko

Fehlende Post-Quanten-Hybridisierung setzt vertrauliche Kommunikationsdaten dem Risiko von „Store Now, Decrypt Later" (SNDL) aus: Angreifer können bereits heute verschlüsselte TLS-Datenströme aufzeichnen, um diese nach Verfügbarkeit kryptografisch relevanter Quantencomputer (CRQC) rückwirkend zu entschlüsseln. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt daher bereits heute den Einsatz hybrider Verfahren aus klassischer ECDH-Kurve und ML-KEM (Kyber).

3. Regulatorisches Anforderungs-Mapping (NIS-2, DORA & BSI)

Die nachfolgende Zuordnung zeigt auf, auf welche gesetzlichen und normativen Anforderungen sich dieser Prüfbericht und das beigefügte Maßnahmenpaket beziehen:

Rechtsnorm / Richtlinie	Anforderung / Empfehlung	Technische Umsetzung im Scan
§ 30 Abs. 2 Nr. 8 BSIG (NIS-2)	Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung als Maßnahme des Risikomanagements.	Muster-Kryptografie-Richtlinie + technische Verifikation der extern gemessenen TLS/SSH-Endpunkte + CycloneDX CBOM.
§ 38 BSIG (Leitungsorgane)	Billigung und Überwachung der Risikomanagementmaßnahmen durch die Geschäftsleitung.	Management-Summary (Kapitel 2) und Dokumentations-/Unterschriftsblatt (Kapitel 15).
BSI TR-02102-2 (TLS)	Empfehlung von TLS 1.3 / TLS 1.2 mit Perfect Forward Secrecy (PFS), AEAD-Chiffren, Mindestschlüssellängen (RSA ≥ 3000 Bit).	Einzelprüfung jedes Ports auf Protokollversion, PFS-Eigenschaft, Schlüssellänge und Signaturalgorithmus.
BSI TR-02102-4 (SSH)	Empfehlung sicherer KEX-Verfahren, Ausschluss von SHA-1-Gruppen, Einsatz moderner Hostkeys (Ed25519 / ECDSA / RSA-SHA2).	Analyse des SSH-2.0-Banners und KEXINIT-Pakets auf Port 22 inkl. `mlkem768x25519-sha256`.
BSI TR-03108 & DANE	Empfehlung sicherer E-Mail-Transportverschlüsselung über STARTTLS/SMTPS sowie DNSSEC-gestützter TLSA-Einträge.	Prüfung der Ports 25, 465, 587, 993 sowie DNS-Abfrage auf `_port._tcp` TLSA Resource Records.
DORA Art. 9 (VO (EU) 2022/2554)	Schutz und Prävention: Schutz von Daten in Übertragung und kryptografische Kontrollen im Finanzsektor.	Einsatz hybrider Post-Quanten-Verfahren (FIPS 203 ML-KEM) und dokumentiertes Krypto-Asset-Register.

MUSTER

Hinweis zum „Stand der Technik" nach § 30 Abs. 1 Satz 2 BSIG

Das Gesetz verlangt die Berücksichtigung des „Stands der Technik" sowie einschlägiger europäischer und internationaler Normen. In Deutschland werden die Technischen Richtlinien der Reihe **BSI TR-02102** regelmäßig als Orientierung für den Stand der Technik bei kryptografischen Verfahren herangezogen.

4. Prüfmethodik & Angriffsoberflächen-Aufklärung

Der Scan erfolgt schonend (keine Exploits, kein Brute-Force, keine Lasttests – nur reguläre TLS-/SSH-Handshakes; beim Komplettpaket ergänzt um eine aktive TCP-Port-Erkennung auf gängigen Dienste-Ports) in drei aufeinander abgestimmten Phasen:

1. **Passive Subdomain-Aufklärung (OSINT & CT-Logs):** Abfrage öffentlicher Certificate-Transparency-Register (`crt.sh`) sowie Auswertung von DNS-Infrastruktureinträgen (`MX` , `TXT/SPF` , `DMARC` , `SRV`).
2. **Risikobasierte Zielpriorisierung:** Höchstbewertung kritischer Infrastrukturendpunkte wie `vpn` , `mail` , `api` , `git` , `ldap` , `portal` , `auth` , `moodle` und `cloud` .
3. **Aktive Multi-Port-Krypto-Inspektion:** Parallele Überprüfung der Standard-Ports 443, 25, 587, 22 sowie aktive Erkennung weiterer verschlüsselter Dienste auf 71 gängigen Ports (u. a. IMAPS, POP3S, LDAPS, alternative SSH-, VPN- und Administrations-Ports) mittels OpenSSL 3.x (inkl. ML-KEM Hybrid-Gruppen `X25519MLKEM768` , `SecP256r1MLKEM768` , `SecP384r1MLKEM1024`) und SSH-KEX-Analyse.

Erkannte DNS- und E-Mail-Sicherheitsattribute für musterfirma.example

MX-Mailgateways	mail.musterfirma.example
SPF-Richtlinie (TXT)	`v=spf1 mx -all`
DMARC-Richtlinie (_dmarc)	`v=DMARC1; p=none; rua=mailto:dmarc@musterfirma.example`
IPv6-Only-Ziele (nur AAAA, kein IPv4 A-Record)	Keine reinen IPv6-Only-Subdomains im aktiven Prüfset erkannt (Hinweis: Aktive Handshake-Probes erfolgen über IPv4 `203.0.113.10` ; reine IPv6-Ziele ohne A-Record erscheinen als geschlossen).
Gefundene Subdomains gesamt	9 Hostnamen im Geltungsbereich

Priorisierte Subdomain-Bewertungsliste (Auszug)

Subdomain / Hostname	Kritikalitäts-Score	Klassifizierung
`musterfirma.example`	63 / 100	Primärer Web-/API-Endpunkt
`vpn.musterfirma.example`	8 / 100	Primärer Web-/API-Endpunkt
`git.musterfirma.example`	38 / 100	Administrativer SSH-Zugang
`www.musterfirma.example`	63 / 100	Primärer Web-/API-Endpunkt
`mail.musterfirma.example`	60 / 100	Mail-Infrastruktur
`api.musterfirma.example`	78 / 100	Primärer Web-/API-Endpunkt
`mail.musterfirma.example`	78 / 100	Mail-Infrastruktur
`portal.musterfirma.example`	100 / 100	Primärer Web-/API-Endpunkt

MUSTER

5. Gesamtübersicht aller geprüften Endpunkte & Ports

Die folgende Tabelle zeigt sämtliche aktiv erreichbaren und kryptografisch vermessenen Endpunkte der Domain **musterfirma.example** inklusive ausgehandelter Protokollversion, Schlüsselaustauschgruppe und Bewertung anhand der BSI TR-02102-2:

Endpunkt (Host:Port)	Dienst	Protokoll	Key Exchange / Gruppe	Zertifikat / Key	PQC (ML-KEM)	Stat
`musterfirma.example:443`	HTTPS	TLSv1.3	`X25519`	RSA (2048 Bit)	Nein (Klassisch)	DU
`vpn.musterfirma.example:443`	HTTPS	TLSv1.2	`RSA`	RSA (2048 Bit)	Nein (Klassisch)	RO
`git.musterfirma.example:22`	SSH	SSH-2.0	`curve25519-sha256`	RSA (3072 Bit)	Nein (Klassisch)	RO
`www.musterfirma.example:443`	HTTPS	TLSv1.3	`X25519`	RSA (2048 Bit)	Nein (Klassisch)	DU
`mail.musterfirma.example:25`	SMTP (STARTTLS)	TLSv1.2	`X25519`	RSA (3072 Bit)	Nein (Klassisch)	DU
`api.musterfirma.example:443`	HTTPS	TLSv1.3	`X25519`	ECDSA (256 Bit)	Nein (Klassisch)	OR
`mail.musterfirma.example:993`	IMAPS	TLSv1.3	`X25519`	RSA (3072 Bit)	Nein (Klassisch)	OR
`portal.musterfirma.example:443`	HTTPS	TLSv1.3	`X25519MLKEM768`	ECDSA (256 Bit)	**Ja (X25519MLKEM768)**	GR

Bewertungslogik nach BSI TR-02102-2

GRÜN: TLS 1.3 bzw. SSH-2.0 mit aktivem Post-Quanten-Hybrid-Schlüsselaustausch (ML-KEM / sntrup761), PFS und empfohlenen Schlüssellängen.
GELB (90–99 Punkte): Kryptografie entspricht den Empfehlungen, es fehlt nur eine ergänzende Härtung, z. B. DANE/TLSA am Mailserver (mit MTA-STS bzw. TLSA ohne DNSSEC teilweise ausgeglichen).
ORANGE (75–89 Punkte): Klassisch sichere Konfiguration (TLS 1.2/1.3 mit PFS), jedoch noch ohne Post-Quanten-Hybridisierung.
DUNKELORANGE (unter 75 Punkte): Mehrere Abweichungen zugleich, z. B. fehlende Post-Quanten-Hybridisierung zusammen mit RSA < 3072 Bit oder nur TLS 1.2.
ROT: Veraltetes Protokoll (TLS 1.0/1.1), fehlende Perfect Forward Secrecy (PFS), unsichere Chiffren oder RSA < 2048 Bit.

MUSTER

6. Technisches Einzelprüfblatt (1/5): musterfirma.example:443

Detaillierte kryptografische Handshake-Messung und Bewertung für den Endpunkt `musterfirma.example` auf Port `443` (HTTPS).

Geprüfter Endpunkt (FQDN : Port)	`musterfirma.example:443` (HTTPS)
Ausgehandeltes Protokoll	**TLSv1.3** (TLS)
Ausgehandelte Cipher-Suite	`TLS_AES_256_GCM_SHA384`
Schlüsselaustausch-Gruppe (KEX)	`X25519`
Post-Quantum Hybrid Status (ML-KEM)	**INAKTIV – NUR KLASSISCHER KEX**
Server-Public-Key / Schlüssellänge	RSA – 2048 Bit
Perfect Forward Secrecy (PFS)	Ja (Ephemerer Schlüsselaustausch aktiv)
DNSSEC / DANE (TLSA-Eintrag)	Nicht hinterlegt
Erkannter Server-Stack / Banner	`nginx`
Einzel-Score	**63 / 100 Punkte** (Deutliche Abweichungen)

Festgestellte Prüfbefunde & Abweichungen nach BSI TR-02102

Regel-Code	Stufe	Feststellung & Normbezug	Konkrete Handlungsempfehlung
`BSI-TR02102-RSA-LT-3072`	GELB	**RSA-Schlüssellänge < 3072 Bit (2048 Bit)** Das Serverzertifikat nutzt RSA mit 2048 Bit. Die BSI TR-02102-2 empfiehlt für RSA eine Schlüssellänge von mindestens 3000 Bit.	Zertifikatserneuerung mit RSA-3072/4096 oder ECDSA P-256/ P-384 einplanen.
`NIS2-PQC-MISSING`	GELB	**Kein Post-Quanten-Schlüsselaustausch (ML-KEM) konfiguriert** Aktueller Schlüsselaustausch (X25519) basiert ausschließlich auf klassischer asymmetrischer Kryptografie (ECC/DH) und bietet keinen Schutz gegen eine spätere Entschlüsselung aufgezeichneter Daten durch Quantencomputer (SNDL).	Aktivierung von hybriden PQC-Key-Exchange-Gruppen (X25519MLKEM768 / SecP256r1MLKEM768 für TLS 1.3 bzw. mlkem768×25519-sha256 für OpenSSH).
`BSI-DANE-TLSA-MISSING`	GELB	**Kein DANE / TLSA-Eintrag für _443._tcp.musterfirma.example** Für diesen TLS-Endpunkt wurde kein DNSSEC-gestützter TLSA Resource Record (DANE) gefunden. Für Mailserver empfiehlt das BSI in der Technischen Richtlinie BSI TR-03108 zusätzlich DANE/TLSA zur Absicherung des E-Mail-Transports.	Veröffentlichung eines DNSSEC-signierten TLSA-Records (z. B. 3 1 1) unter _443._tcp.musterfirma.example.

MUSTER

Hinweis zur Konfigurationshärtung auf musterfirma.example:443

Für diesen Dienst (nginx) finden Sie im Komplettpaket unter `04_Server_Konfigurationen_und_Skripte/` eine passende Referenzkonfiguration mit aktivierter Hybrid-Kurve `X25519MLKEM768:SecP256r1MLKEM768` gemäß Empfehlung der BSI TR-02102-2.

MUSTER

7. Technisches Einzelprüfblatt (2/5): vpn.musterfirma.example:443

Detaillierte kryptografische Handshake-Messung und Bewertung für den Endpunkt `vpn.musterfirma.example` auf Port `443` (HTTPS).

Geprüfter Endpunkt (FQDN : Port)	`vpn.musterfirma.example:443` (HTTPS)
Ausgehandeltes Protokoll	**TLSv1.2** (TLS)
Ausgehandelte Cipher-Suite	`AES256-GCM-SHA384`
Schlüsselaustausch-Gruppe (KEX)	`RSA`
Post-Quantum Hybrid Status (ML-KEM)	INAKTIV – NUR KLASSISCHER KEX
Server-Public-Key / Schlüssellänge	RSA – 2048 Bit
Perfect Forward Secrecy (PFS)	NEIN (Kritische Abweichung von BSI TR-02102-2)
DNSSEC / DANE (TLSA-Eintrag)	Nicht hinterlegt
Erkannter Server-Stack / Banner	`Standard Server`
Einzel-Score	**8 / 100 Punkte** (Kritisch (Abweichung TR-02102))

Festgestellte Prüfbefunde & Abweichungen nach BSI TR-02102

Regel-Code	Stufe	Feststellung & Normbezug	Konkrete Handlungsempfehlung
`BSI-TR02102-TLS12-ONLY`	GELB	**TLS 1.2 statt TLS 1.3 ausgehandelt** TLS 1.2 ist gemäß BSI TR-02102-2 noch zulässig, unterstützt jedoch standardmäßig keine standardisierten hybriden Post-Quanten-Schlüsselaustauschverfahren (ML-KEM).	Aktivierung von TLS 1.3 mit hybriden Gruppen (X25519MLKEM768 / SecP256r1MLKEM768).
`BSI-TR02102-NO-PFS`	ROT	**Fehlende Perfect Forward Secrecy (PFS)** Die ausgehandelte Cipher-Suite (AES256-GCM-SHA384) verwendet keinen ephemeren Schlüsselaustausch. Bei Kompromittierung des privaten Serverschlüssels können sämtliche aufgezeichneten Sitzungen rückwirkend entschlüsselt werden.	Ausschließlich ECDHE- oder DHE-basierte Cipher-Suites gemäß BSI TR-02102-2 Abschnitt 3.3.1 konfigurieren.
`BSI-TR02102-RSA-LT-3072`	GELB	**RSA-Schlüssellänge < 3072 Bit (2048 Bit)** Das Serverzertifikat nutzt RSA mit 2048 Bit. Die BSI TR-02102-2 empfiehlt für RSA eine Schlüssellänge von mindestens 3000 Bit.	Zertifikatserneuerung mit RSA-3072/4096 oder ECDSA P-256/ P-384 einplanen.
`NIS2-PQC-MISSING`	GELB	**Kein Post-Quanten-Schlüsselaustausch (ML-KEM)**	Aktivierung von hybriden PQC-Key-Exchange-Gruppen

MUSTER

Regel-Code	Stufe	Feststellung & Normbezug	Konkrete Handlungsempfehlung
		konfiguriert Aktueller Schlüsselaustausch (RSA) basiert ausschließlich auf klassischer asymmetrischer Kryptografie (ECC/DH) und bietet keinen Schutz gegen eine spätere Entschlüsselung aufgezeichneter Daten durch Quantencomputer (SNDL).	(X25519MLKEM768 / SecP256r1MLKEM768 für TLS 1.3 bzw. mlkem768×25519-sha256 für OpenSSH).
`BSI-DANE-TLSA-MISSING`	GELB	**Kein DANE / TLSA-Eintrag für _443._tcp.vpn.musterfirma.example** Für diesen TLS-Endpunkt wurde kein DNSSEC-gestützter TLSA Resource Record (DANE) gefunden. Für Mailserver empfiehlt das BSI in der Technischen Richtlinie BSI TR-03108 zusätzlich DANE/TLSA zur Absicherung des E-Mail-Transports.	Veröffentlichung eines DNSSEC-signierten TLSA-Records (z. B. 3 1 1) unter _443._tcp.vpn.musterfirma.example.

Hinweis zur Konfigurationshärtung auf vpn.musterfirma.example:443

Für diesen Dienst (Standard Server) finden Sie im Komplettpaket unter `04_Server_Konfigurationen_und_Skripte/` eine passende Referenzkonfiguration mit aktivierter Hybrid-Kurve `X25519MLKEM768:SecP256r1MLKEM768` gemäß Empfehlung der BSI TR-02102-2.

MUS

8. Technisches Einzelprüfblatt (3/5): git.musterfirma.example:22

Detaillierte kryptografische Handshake-Messung und Bewertung für den Endpunkt `git.musterfirma.example` auf Port `22` (SSH).

Geprüfter Endpunkt (FQDN : Port)	`git.musterfirma.example:22` (SSH)
Ausgehandeltes Protokoll	**SSH-2.0** (SSH-2.0)
Ausgehandelte Cipher-Suite	`aes256-gcm@openssh.com`
Schlüsselaustausch-Gruppe (KEX)	`curve25519-sha256`
Post-Quantum Hybrid Status (ML-KEM)	INAKTIV – NUR KLASSISCHER KEX
Server-Public-Key / Schlüssellänge	RSA – 3072 Bit
Perfect Forward Secrecy (PFS)	Ja (Ephemerer Schlüsselaustausch aktiv)
DNSSEC / DANE (TLSA-Eintrag)	Nicht hinterlegt
Erkannter Server-Stack / Banner	`SSH-2.0-OpenSSH_8.9p1`
Einzel-Score	**38 / 100 Punkte** (Kritisch (Abweichung TR-02102))

Festgestellte Prüfbefunde & Abweichungen nach BSI TR-02102

Regel-Code	Stufe	Feststellung & Normbezug	Konkrete Handlungsempfehlung
`BSI-TR02102-4-SSH-SHA1`	ROT	**Schwache SSH-Schlüsselaustauschverfahren aktiv (diffie-hellman-group14-sha1)** Abweichung von den Empfehlungen der BSI TR-02102-4: SHA-1-basierte Diffie-Hellman-Gruppen werden nicht mehr empfohlen.	Beschränkung auf mlkem768×25519-sha256, sntrup761×25519-sha512 und curve25519-sha256.
`NIS2-PQC-MISSING`	GELB	**Kein Post-Quanten-Schlüsselaustausch (ML-KEM) konfiguriert** Aktueller Schlüsselaustausch (curve25519-sha256) basiert ausschließlich auf klassischer asymmetrischer Kryptografie (ECC/DH) und bietet keinen Schutz gegen eine spätere Entschlüsselung aufgezeichneter Daten durch Quantencomputer (SNDL).	Aktivierung von hybriden PQC-Key-Exchange-Gruppen (X25519MLKEM768 / SecP256r1MLKEM768 für TLS 1.3 bzw. mlkem768×25519-sha256 für OpenSSH).

Hinweis zur Konfigurationshärtung auf git.musterfirma.example:22

Für diesen Dienst (SSH-2.0-OpenSSH_8.9p1) finden Sie im Komplettpaket unter `04_Server_Konfigurationen_und_Skripte/` eine passende Referenzkonfiguration mit aktivierter Hybrid-Kurve `X25519MLKEM768:SecP256r1MLKEM768` gemäß Empfehlung der BSI TR-02102-2.

MUSTER

9. Technisches Einzelprüfblatt (4/5): www.musterfirma.example:443

Detaillierte kryptografische Handshake-Messung und Bewertung für den Endpunkt `www.musterfirma.example` auf Port `443` (HTTPS).

Geprüfter Endpunkt (FQDN : Port)	`www.musterfirma.example:443` (HTTPS)
Ausgehandeltes Protokoll	**TLSv1.3** (TLS)
Ausgehandelte Cipher-Suite	`TLS_AES_256_GCM_SHA384`
Schlüsselaustausch-Gruppe (KEX)	`X25519`
Post-Quantum Hybrid Status (ML-KEM)	INAKTIV – NUR KLASSISCHER KEX
Server-Public-Key / Schlüssellänge	RSA – 2048 Bit
Perfect Forward Secrecy (PFS)	Ja (Ephemerer Schlüsselaustausch aktiv)
DNSSEC / DANE (TLSA-Eintrag)	Nicht hinterlegt
Erkannter Server-Stack / Banner	`nginx`
Einzel-Score	**63 / 100 Punkte** (Deutliche Abweichungen)

Festgestellte Prüfbefunde & Abweichungen nach BSI TR-02102

Regel-Code	Stufe	Feststellung & Normbezug	Konkrete Handlungsempfehlung
`BSI-TR02102-RSA-LT-3072`	GELB	**RSA-Schlüssellänge < 3072 Bit (2048 Bit)** Das Serverzertifikat nutzt RSA mit 2048 Bit. Die BSI TR-02102-2 empfiehlt für RSA eine Schlüssellänge von mindestens 3000 Bit.	Zertifikatserneuerung mit RSA-3072/4096 oder ECDSA P-256/ P-384 einplanen.
`NIS2-PQC-MISSING`	GELB	**Kein Post-Quanten-Schlüsselaustausch (ML-KEM) konfiguriert** Aktueller Schlüsselaustausch (X25519) basiert ausschließlich auf klassischer asymmetrischer Kryptografie (ECC/DH) und bietet keinen Schutz gegen eine spätere Entschlüsselung aufgezeichneter Daten durch Quantencomputer (SNDL).	Aktivierung von hybriden PQC-Key-Exchange-Gruppen (X25519MLKEM768 / SecP256r1MLKEM768 für TLS 1.3 bzw. mlkem768×25519-sha256 für OpenSSH).
`BSI-DANE-TLSA-MISSING`	GELB	**Kein DANE / TLSA-Eintrag für _443._tcp.www.musterfirma.example** Für diesen TLS-Endpunkt wurde kein DNSSEC-gestützter TLSA Resource Record (DANE) gefunden. Für Mailserver empfiehlt das BSI in der Technischen Richtlinie BSI TR-03108 zusätzlich DANE/TLSA zur Absicherung des E-Mail-Transports.	Veröffentlichung eines DNSSEC-signierten TLSA-Records (z. B. 3 1 1) unter _443._tcp.www.musterfirma.example.

MUSTER

Hinweis zur Konfigurationshärtung auf www.musterfirma.example:443

Für diesen Dienst (nginx) finden Sie im Komplettpaket unter `04_Server_Konfigurationen_und_Skripte/` eine passende Referenzkonfiguration mit aktivierter Hybrid-Kurve `X25519MLKEM768:SecP256r1MLKEM768` gemäß Empfehlung der BSI TR-02102-2.

MUSTER

10. Technisches Einzelprüfblatt (5/5): mail.musterfirma.example:25

Detaillierte kryptografische Handshake-Messung und Bewertung für den Endpunkt `mail.musterfirma.example` auf Port `25` (SMTP (STARTTLS)).

Geprüfter Endpunkt (FQDN : Port)	`mail.musterfirma.example:25` (SMTP (STARTTLS))
Ausgehandeltes Protokoll	**TLSv1.2** (TLS)
Ausgehandelte Cipher-Suite	`ECDHE-RSA-AES256-GCM-SHA384`
Schlüsselaustausch-Gruppe (KEX)	`X25519`
Post-Quantum Hybrid Status (ML-KEM)	INAKTIV – NUR KLASSISCHER KEX
Server-Public-Key / Schlüssellänge	RSA – 3072 Bit
Perfect Forward Secrecy (PFS)	Ja (Ephemerer Schlüsselaustausch aktiv)
DNSSEC / DANE (TLSA-Eintrag)	Nicht hinterlegt
Erkannter Server-Stack / Banner	`Postfix`
Einzel-Score	**60 / 100 Punkte** (Deutliche Abweichungen)

Festgestellte Prüfbefunde & Abweichungen nach BSI TR-02102

Regel-Code	Stufe	Feststellung & Normbezug	Konkrete Handlungsempfehlung
`BSI-TR02102-TLS12-ONLY`	GELB	**TLS 1.2 statt TLS 1.3 ausgehandelt** TLS 1.2 ist gemäß BSI TR-02102-2 noch zulässig, unterstützt jedoch standardmäßig keine standardisierten hybriden Post-Quanten-Schlüsselaustauschverfahren (ML-KEM).	Aktivierung von TLS 1.3 mit hybriden Gruppen (X25519MLKEM768 / SecP256r1MLKEM768).
`NIS2-PQC-MISSING`	GELB	**Kein Post-Quanten-Schlüsselaustausch (ML-KEM) konfiguriert** Aktueller Schlüsselaustausch (X25519) basiert ausschließlich auf klassischer asymmetrischer Kryptografie (ECC/DH) und bietet keinen Schutz gegen eine spätere Entschlüsselung aufgezeichneter Daten durch Quantencomputer (SNDL).	Aktivierung von hybriden PQC-Key-Exchange-Gruppen (X25519MLKEM768 / SecP256r1MLKEM768 für TLS 1.3 bzw. mlkem768×25519-sha256 für OpenSSH).
`BSI-DANE-TLSA-MISSING`	GELB	**Kein DANE / TLSA-Eintrag für _25._tcp.mail.musterfirma.example** Für diesen TLS-Endpunkt wurde kein DNSSEC-gestützter TLSA Resource Record (DANE) gefunden. Für Mailserver empfiehlt das BSI in der Technischen Richtlinie BSI TR-03108	Veröffentlichung eines DNSSEC-signierten TLSA-Records (z. B. 3 1 1) unter _25._tcp.mail.musterfirma.example.

MUSTER

Regel-Code	Stufe	Feststellung & Normbezug	Konkrete Handlungsempfehlung
		zusätzlich DANE/TLSA zur Absicherung des E-Mail-Transports.	

Hinweis zur Konfigurationshärtung auf mail.musterfirma.example:25

Für diesen Dienst (Postfix) finden Sie im Komplettpaket unter `04_Server_Konfigurationen_und_Skripte/` eine passende Referenzkonfiguration mit aktivierter Hybrid-Kurve `X25519MLKEM768:SecP256r1MLKEM768` gemäß Empfehlung der BSI TR-02102-2.

MUSTER

11. Post-Quanten-Kryptografie (ML-KEM) & SNDL-Risikoanalyse

Klassische asymmetrische Verfahren wie RSA, Diffie-Hellman und elliptische Kurven (ECDH/ECDSA) beruhen auf dem Faktorisierungsproblem bzw. dem diskreten Logarithmusproblem. Ein hinreichend leistungsfähiger Quantencomputer löst beide Probleme mittels des **Shor-Algorithmus** in polynomieller Zeit.

Das akute „Store Now, Decrypt Later" (SNDL) Bedrohungsszenario

Auch wenn kryptografisch relevante Quantencomputer (CRQC) erst in wenigen Jahren breit verfügbar sind, besteht das Sicherheitsrisiko **bereits heute**: Es ist damit zu rechnen, dass staatliche und kriminelle Akteure verschlüsselten TLS- und VPN-Datenverkehr auf Vorrat mitschneiden, um ihn später zu entschlüsseln. Betroffen sind sämtliche Geschäftsgeheimnisse, personenbezogene Daten, Gesundheitsdaten und Finanztransaktionen mit mehrjähriger Schutzbedarfsdauer.

Verfahrensklasse	Klassischer Algorithmus	Bedrohung durch Quantencomputer	BSI / NIST Post-Quanten-Lösung
Schlüsselaustausch (TLS 1.3)	ECDH (X25519, P-256, P-384), DH	Vollständiger Bruch durch Shor-Algorithmus (SNDL-verwundbar)	**Hybrides ML-KEM (FIPS 203):** `X25519MLKEM768`, `SecP256r1MLKEM768`
Schlüsselaustausch (SSH-2.0)	curve25519-sha256, DH-Group14/16	Vollständiger Bruch durch Shor-Algorithmus	`mlkem768x25519-sha256` oder `sntrup761x25519-sha512`
Symmetrische Verschlüsselung	AES-128-GCM, AES-256-GCM, ChaCha20	Grover-Algorithmus halbiert effektive Schlüssellänge	**AES-256-GCM** und **ChaCha20-Poly1305** gelten nach heutigem Stand als widerstandsfähig gegen bekannte Quantenangriffe (≥ 128 Bit Quanten-Sicherheit)

Warum das BSI hybride Verfahren empfiehlt

Beim hybriden Schlüsselaustausch (z. B. `X25519MLKEM768`) werden die gemeinsamen Sitzungsschlüssel sowohl aus einem bewährten klassischen Verfahren (`X25519`) als auch aus dem gitterbasierten Post-Quanten-Verfahren `ML-KEM-768` (ehemals CRYSTALS-Kyber) abgeleitet. Die Verbindung bleibt nach heutigem Kenntnisstand selbst dann geschützt, wenn eines der beiden Verfahren künftig geschwächt werden sollte.

MUSTER

12. E-Mail-Sicherheit, DNSSEC & DANE / TLSA nach BSI TR-03108

Neben HTTPS-Webdiensten stellt die E-Mail-Kommunikation (SMTP Ports 25, 465, 587 sowie IMAPS Port 993) einen der kritischsten Angriffsvektoren für Man-in-the-Middle- und Downgrade-Angriffe dar. Die Technische Richtlinie **BSI TR-03108** empfiehlt hierfür den kombinierten Einsatz von TLS, DNSSEC und DANE (DNS-based Authentication of Named Entities).

Empfohlener DANE / TLSA-Eintrag für musterfirma.example

Durch Veröffentlichung eines DNSSEC-signierten `TLSA` Resource Records (RFC 6698 / RFC 7671) legen Sie verbindlich fest, welchem Zertifikat bzw. Public-Key ein anliefernder Mailserver bei Verbindungen zu Ihrer Domain vertrauen muss:

```
; Beispiel für DANE-EE (3) SPKI (1) SHA-256 (1) auf Port 25 und 443:
_25._tcp.mail.musterfirma.example.  3600 IN TLSA 3 1 1 (
    e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 )
_443._tcp.musterfirma.example.      3600 IN TLSA 3 1 1 (
    e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 )
```

Befundmatrix E-Mail & DNS für musterfirma.example

Prüfkriterium	Ist-Zustand bei musterfirma.example	BSI-Empfehlung
MX-Server Einträge	mail.musterfirma.example	Redundante MX-Gateways mit erzwungenem STARTTLS (TLS 1.3 + ML-KEM).
SPF (Sender Policy Framework)	v=spf1 mx -all	Restriktiver SPF-Eintrag mit `-all` oder `~all` Abschluss.
DMARC-Policy	v=DMARC1; p=none; rua=mailto:dmarc@musterfirma.example	Mindestens `p=quarantine` bzw. `p=reject` mit RUA-Reporting.

MUSTER

13. Cryptographic Bill of Materials (CycloneDX v1.6 CBOM)

Ein zentrales Element moderner Krypto-Governance nach NIS-2 und DORA ist ein maschinenlesbares Verzeichnis der extern gemessenen kryptografischen Algorithmen, Protokolle, Schlüssellängen und Zertifikate (**CBOM**). In Ihrem Download-Paket befindet sich die Datei `cbom.json` nach dem internationalen OWASP-Standard **CycloneDX v1.6**.

Auszug aus dem generierten CycloneDX v1.6 Krypto-Inventar


```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:892de36e-5366-5426-a36e-d4c81b9a6cb0",
  "version": 1,
  "metadata": {
    "timestamp": "2026-10-29T15:35:43.569956Z",
    "tools": {
      "components": [
        {
          "type": "application",
          "bom-ref": "tool:sichergenug-pqc-scanner",
          "vendor": "sichergenug.de",
          "name": "Krypto-Check orientiert an BSI TR-02102",
          "version": "1.0.0"
        }
      ]
    },
    "component": {
      "type": "application",
      "bom-ref": "pkg:generic/musterfirma.example@2026",
      "name": "musterfirma.example",
      "version": "2026",
      "description": "CBOM der extern gemessenen TLS/SSH-Endpunkte zu § 30 BSIG & BSI TR-02102-2 für
musterfirma.example"
    },
    "properties": [
      {
  // ... [Vollständiges Inventar in cbom.json im Archiv]
```


Integration in Ihr ISMS / GRC- und SIEM-System

Die Datei `cbom.json` kann direkt in Dependency-Track, ServiceNow GRC, DefectDojo oder Ihre CI/CD-Compliance-Pipelines importiert werden, um die Dokumentation Ihres Krypto-Inventars (extern erreichbare Endpunkte) zu § 30 Abs. 2 Nr. 8 BSIG zu unterstützen.

14. Priorisierter 30-60-90-Tage Maßnahmen- & Migrationsplan

Um sowohl die kurzfristige Umsetzung der BSI-Empfehlungen als auch die mittelfristige Post-Quanten-Härtung für **musterfirma.example** strukturiert umzusetzen, empfehlen wir folgenden Stufenplan:

Zeitraum	Maßnahmenpaket	Technische & Organisatorische Umsetzungsschritte
Tag 1 – 30 (Quick Wins & Governance)	Kryptografie-Richtlinie & Abschaltung von Altlasten	1. Anpassung, Zeichnung und Inkraftsetzung der beigefügten Muster-Kryptografie-Richtlinie durch die Geschäftsleitung (§ 38 BSIG). 2. Deaktivierung sämtlicher TLS 1.0/1.1-Protokolle und Non-PFS-Cipher-Suites. 3. Ablage des `cbom.json` im ISMS-Dokumentationsordner.
Tag 31 – 60 (PQC-Rollout Edge & SSH)	Aktivierung hybrider ML-KEM Schlüsselaustauschgruppen	1. Anpassung und Einspielen der Server-Konfiguration (Nginx, Apache, Caddy, HAProxy) mit `X25519MLKEM768:SecP256r1MLKEM768` durch Ihr IT-Fachpersonal; Beispielkonfigurationen sind im Komplettpaket enthalten. 2. Härtung aller SSH-Zugänge (Port 22) auf `mlkem768x25519-sha256` bzw. `sntrup761x25519-sha512`. 3. Erneuerung von RSA-2048-Zertifikaten auf ECDSA P-256/P-384 oder RSA-3072/4096.
Tag 61 – 90 (DANE & Dauerbetrieb)	DNSSEC/DANE-Härtung & erneuter Scan	1. Aktivierung von DNSSEC und Veröffentlichung von `TLSA` Resource Records für Mail- und Web-Endpunkte. 2. Durchführung eines Verifikations-Scans auf `sichergenug.de` zur Bestätigung des Zielstatus GRÜN.

MUSTER

15. Kenntnisnahme & Freigabe der Maßnahmen (§ 38 BSIG)

Mit diesem Dokumentationsblatt bestätigt die Organisation die Kenntnisnahme der technischen Prüfergebnisse für **musterfirma.example** sowie die Einleitung der im Maßnahmenplan (Kapitel 14) definierten Schritte für Ihre Nachweisführung zu § 30 Abs. 2 Nr. 8 BSIG und BSI TR-02102-2.

Geprüfte Organisation / Domain	**musterfirma.example**
Scan-Referenz & Zeitstempel	`SG-NIS2-B16CEDE2CC` (29.10.2026 15:35 UTC)
SHA-256 Prüfsumme des CBOM-Inventars	`b16cede2cc81c2745e1556ef7280062a27927bbff50878425b09790d1a82ccf7`
Beigefügte Dokumente im Archiv	1. Dieser Prüfbericht 2. `cbom_musterfirma_example.json` (CycloneDX v1.6 Cryptographic Bill of Materials der extern gemessenen Endpunkte) 3. Server-Konfigurationspakete & Muster-Kryptografie-Richtlinie (im Komplettpaket)

Dokumentation der Kenntnisnahme & Maßnahmengenehmigung

Informationssicherheitsbeauftragter (ISB / CISO) _____ Ort, Datum, Name & Unterschrift	**Geschäftsleitung / Vorstand (gem. § 38 BSIG)** _____ Ort, Datum, Name & Unterschrift
Verantwortlicher IT-Betrieb / Systemarchitektur _____ Ort, Datum, Name & Unterschrift	**Datenschutz / Compliance (optional)** _____ Ort, Datum, Name & Unterschrift

Erstellt durch: sichergenug.de – automatisierter Krypto-Check, orientiert an BSI TR-02102 (`https://sichergenug.de`). **Privates Angebot – keine Stelle des BSI oder einer Behörde, keine Zertifizierung.** Dieser Prüfbericht wurde automatisiert auf Basis realer Handshake- und DNS-Messdaten der extern erreichbaren Endpunkte erstellt.

Hinweise zur Verwendung, Leistungsabgrenzung und Haftung

Sämtliche Ergebnisse und Unterlagen von sichergenug.de – je nach Leistung Kurzcheck, Prüfbericht, Management-Zusammenfassung, Krypto-Inventar, Richtlinien- und Fragebogenvorlagen, Konfigurationsbeispiele, Prüfskript und Checklisten – werden automatisiert auf Grundlage einer externen Stichtagsmessung der öffentlich erreichbaren Endpunkte erstellt. Sie dienen als fachliche Arbeitsgrundlage und Dokumentationshilfe. Sie ersetzen weder eine Rechtsberatung noch eine Zertifizierung, ein Audit oder eine Prüfung durch eine Behörde oder Prüfstelle.

Die im Komplettpaket enthaltenen Konfigurationsdateien und das Prüfskript sind Beispiele dafür, wie die betroffenen Dienste nach den Empfehlungen der BSI TR-02102 eingerichtet werden können. Sie sind keine einsatzfertigen Konfigurationen für Ihre Systeme, da dem Anbieter Softwareversionen, Module, bestehende Einstellungen, Abhängigkeiten und die eingesetzten Clients Ihrer Umgebung nicht bekannt sind. Auswahl, Anpassung, Prüfung und Implementierung sowie der anschließende Betrieb – einschließlich Datensicherung, Test in einer geeigneten Umgebung und Rückfallplanung – liegen in der Verantwortung des Kunden und seines qualifizierten IT-Fachpersonals (§ 2 Abs. 4 AGB).

Die Richtlinien- und Fragebogenvorlagen sind unverbindliche Muster. Sie sind vor Freigabe oder Versand an die Organisation, ihre Prozesse und die für sie geltenden rechtlichen Anforderungen anzupassen. Für Inhalt und Umsetzung der freigegebenen Fassung ist die jeweilige Organisation verantwortlich.

Die Haftung des Anbieters und die gesetzlichen Mängelrechte richten sich nach § 6 der Allgemeinen Geschäftsbedingungen. Danach haftet der Anbieter insbesondere unbeschränkt für Vorsatz und grobe Fahrlässigkeit, für die Verletzung von Leben, Körper oder Gesundheit sowie nach dem Produkthaftungsgesetz und bei leicht fahrlässiger Verletzung wesentlicher Vertragspflichten begrenzt auf den vertragstypischen, vorhersehbaren Schaden.

Genannte Produkt- und Firmennamen (wie SAP, Microsoft Word und Excel, LibreOffice, Google Docs und Google Tabellen sowie Apple Pages und Numbers) sind Marken oder eingetragene Marken ihrer jeweiligen Inhaber. Ihre Nennung dient ausschließlich dem Hinweis auf kompatible Dateiformate und Importmöglichkeiten; eine wirtschaftliche Verbindung zu den Markeninhabern oder eine Zertifizierung durch diese besteht nicht.

MUSTER