Bundesamt
für Sicherheit in der
Informationstechnik

TLS nach TR-03116-4
Checkliste für Diensteanbieter

Stand 2020

Datum: 10. Januar 2020

1 Einleitung

Ziel dieser Checkliste ist es, Diensteanbieter bei der Konfiguration von TLS gemäß den Vorgaben und Empfehlungen der Technischen Richtlinie BSI TR-03116-4 zu unterstützen. Der Fokus liegt hierbei auf der Konfiguration von TLS 1.2 sowie der Verwendung korrekter TLS-Versionen und Cipher Suites gemäß TR-03116-4.

Für eine erfolgreiche Prüfung müssen grundsätzlich alle Kriterien der Abschnitte 2.1-2.5 mit „Ja“ beantwortet werden. Die Erfüllung der Kriterien aus Abschnitt 2.6 wird von TR-03116-4 empfohlen. Für die Interoperabilität mit TR-konformen TLS-Clients sind hierbei insbesondere die mit '*' gekennzeichneten Punkte von besonderer Relevanz. Diese Checkliste dient lediglich zur Unterstützung, eine vollständige Konformität zur TR-03116-4 kann durch die erfolgreiche Abarbeitung nicht garantiert werden.

Hilfe bei der Konfiguration können auch entsprechende Prüfwerkzeuge (z.B. ssllabs.com oder entsprechende Prüfwerkzeuge anderer Hersteller) bieten.

2 Checkliste

2.1 Server Schlüssel

Nr.	***Zu prüfende Anforderungen***	***Erfüllt***	
		Ja	***Nein***
2.1.1*	Der Schlüssel im Server-Zertifikat entspricht den kryptographischen Mindestanforderungen: • RSA-Schlüssel: ◦ Mindestens 2048 Bitlänge • ECDSA-Schlüssel: ◦ Es wird eine der folgenden Kurven verwendet: ▪ brainpoolP256r1 ▪ brainpoolP384r1 ▪ brainpoolP512r1		

Nr.	*Zu prüfende Anforderungen*	*Erfüllt*	
		Ja	*Nein*
	▪ secp224r1 ▪ secp256r1 ▪ secp384r1 ▪ secp521r1 *Prüfanweisung (ssllabs): Prüfung aller Einträge „Key“ in „Server Key“ und „Additional Certificates“.*		
2.1.2*	Der Signatur-Algorithmus des Server-Zertifikats entspricht den Anforderungen: • Signaturalgorithmus: ◦ RSA ◦ ECDSA • Hashfunktion: ◦ SHA-224 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512 *Prüfanweisung (ssllabs): Prüfung aller Einträge „Signature Algorithm“ in „Server Key“ und „Additional Certificates“.*		
2.1.3	Das Server-Zertifikat enthält keine Wildcards. *Prüfanweisung (ssllabs): Prüfung, dass die URLs in „Subject“ und „Common Name“ und „Alternative Names“ kein „*“ enthalten.*		
2.1.4*	Das Server-Zertifikat enthält Information zur Rückrufprüfung, d.h. einen „CLRDistributionPoint“ oder eine „AuthorityInfoAccess“ (Bei der Verwendung eines qualifizierten Webseitenzertifikats bzw. Extended Validation-Zertifikats automatisch erfüllt) *Prüfanweisung (ssllabs): Prüfung, dass das Feld „Revocation Information“ „CRL“ und/oder „OCSP“ enthält.*		
2.1.5*	Das Server-Zertifikat ist nicht gesperrt. *Prüfanweisung (ssllabs): Prüfung, dass das Feld „Revocation Status“ die Information „not revoked“ enthält.*		
2.1.6	Das Server-Zertifikat enthält eine „KeyUsage“-Extension. Folgende Bits sind gesetzt: • „digitalSignature“: JA • „keyCertSign“: NEIN (bei Verwendung eines qualifizierten Webseitenzertifikats bzw. Extended Validation-Zertifikats automatisch erfüllt) • „cRLSign“: NEIN (Bei Verwendung eines qualifizierten Webseitenzertifikats bzw. Extended Validation-Zertifikats automatisch erfüllt) *Prüfanweisung: Prüfung des o.g. Sachverhaltes direkt im Zertifikat.*		
2.1.7	Das Server-Zertifikat enthält eine „Extended Key Usage“-Extension mit dem Eintrag „id-kp-serverAuth“. (Bei Verwendung eines qualifizierten Webseitenzertifikats bzw. Extended Validation-Zertifikats automatisch erfüllt.)		

Nr.	*Zu prüfende Anforderungen*	*Erfüllt*	
		Ja	*Nein*
	Prüfanweisung: Prüfung des o.g. Sachverhaltes direkt im Zertifikat.		
2.1.8*	Das Server-Zertifikat enthält alle (Sub-)Domain Namen, für die das Zertifikat genutzt wird. *Prüfanweisung (ssllabs): Prüfung, dass jeder (Sub-)Domain-Name für den das Zertifikat genutzt und im Rahmen von TLS ausgeliefert wird, im Feld „Alternatitve Names" enthalten ist.*		

2.2 Zertifikatskette

Nr.	*Zu prüfende Anforderungen*	*Erfüllt*	
		Ja	*Nein*
2.2.1*	Alle Schlüssel der CA-Zertifikate der gesamten Zertifikatskette entsprechen den Anforderungen: • RSA-Schlüssel: ◦ Mindestens 2048 Bitlänge • ECDSA-Schlüssel: ◦ Es wird eine der folgenden Kurven verwendet: ▪ brainpoolPP256r1 ▪ brainpoolP384r1 ▪ brainpoolP512r1 ▪ secp224r1 ▪ secp256r1 ▪ secp384r1 ▪ secp521r1 *Prüfanweisung (ssllabs): Prüfung, dass die Schlüssel in „Certification Paths“ den o.g. Anforderungen entsprechen.*		
2.2.2*	Die Signaturalgorithmen aller untergeordneten CA-Zertifikate der Kette (d.h. CA-Zertifikate außer dem Root-Zertifikat) entsprechen den Anforderungen: • Signaturalgorithmus ◦ RSA ◦ ECDSA • Hashfunktion: ◦ SHA-224 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512 *Prüfanweisung (ssllabs): Prüfung, dass alle Signaturalgorithmen in „Certification Paths“) den o.g. Anforderungen entsprechen.*		
2.2.3	Alle CA-Zertifikate der Zertifikatskette enthalten keine Wildcards im „Subject“ oder „SubjectAltName“. *Prüfanweisung: Prüfung des o.g. Sachverhaltes direkt in den CA-Zertifikaten der Kette.*		
2.2.4*	Alle untergeordneten CA-Zertifikate der Zertifikatskette (d.h. CA-Zertifikate außer dem Root-Zertifikat) enthalten Information zur Rückrufprüfung („CRLDistributionPoint“ oder „AuthorityInfoAccess“). (Bei Verwendung von qualifizierten Webseitenzertifikaten bzw. Extended Validation-Zertifikaten automatisch erfüllt.) *Prüfanweisung: Prüfung des o.g. Sachverhaltes direkt allen untergeordneten CA-Zertifikaten der Kette.*		
2.2.5	Alle CA-Zertifikate enthalten eine als kritisch markierte „Basic Constraints“-Extension. (Bei Verwendung von qualifizierten Webseitenzertifikaten bzw. Exten-		

Nr.	*Zu prüfende Anforderungen*	*Erfüllt*	
		Ja	*Nein*
	ded Validation-Zertifikaten automatisch erfüllt.) *Prüfanweisung: Prüfung des o.g. Sachverhaltes direkt in den CA-Zertifikaten der Kette.*		
2.2.6	Alle CA-Zertifikate enthalten eine als kritisch markierte „Key Usage“-Extension mit den gesetzten Bits „keyCertSign“ und „cRLSign“. (Bei Verwendung von qualifizierten Webseitenzertifikaten bzw. Extended Validation-Zertifikaten automatisch erfüllt.) *Prüfanweisung: Prüfung des o.g. Sachverhaltes direkt in den CA-Zertifikaten der Kette.*		

2.3 TLS-Version und Cipher Suites

Nr.	*Zu prüfende Anforderungen*	*Erfüllt*	
		Ja	*Nein*
2.3.1	Die verpflichtend zu unterstützenden TLS-Versionen werden unterstützt: • TLS 1.2: JA *Prüfanweisung (ssllabs): Prüfung, dass die verpflichtend zu unterstützenden TLS-Versionen im Eintrag „Protocols“ enthalten sind.*		
2.3.2*	Es werden nur erlaubte TLS-Versionen unterstützt: • TLS 1.3: JA • TLS 1.2: JA • TLS 1.1: NEIN • TLS 1.0: NEIN • SSL 3: NEIN • SSL 2: NEIN *Prüfanweisung (ssllabs): Prüfung, dass nur erlaubte TLS-Versionen im Eintrag „Protocols“ enthalten sind.*		
2.3.3*	Die verpflichtend zu unterstützenden Cipher Suites für TLS 1.2 werden unterstützt. *Prüfanweisung (ssllabs): Prüfung, dass die verpflichtend zu unterstützenden Cipher Suites aus Kapitel 3 (s.u.) im Feld „Cipher Suites“ für TLS 1.2 gelistet sind.*		
2.3.4	Es werden nur erlaubte Cipher Suites für TLS 1.2 unterstützt. *Prüfanweisung (ssllabs): Prüfung, dass das Feld „Cipher Suites“ für TLS1.2 keine Cipher Suites enthält, die nicht in Kapitel 3 gelistet sind.*		
2.3.5	Die Priorisierung der Cipher Suites für TLS 1.2 ist korrekt, d.h. Cipher Suites mit größerem Prioritätswert gemäß den Tabellen aus Kapitel 3 werden mit höherer Priorität eingesetzt . *Prüfanweisung (ssllabs): Prüfung, dass die Cipher Suites in Feld „Cipher Suites“ in „Server-preferred Order“ gelistet sind und dass die Reihenfolge den Prioritäten aus Kapitel 3 entspricht.*		
2.3.6	Es werden nur erlaubte Cipher Suites für TLS 1.3 unterstützt. *Prüfanweisung (ssllabs): Prüfung, dass das Feld „Cipher Suites“ für TLS1.3 keine Cipher Suites enthält, die nicht in Kapitel 3 gelistet sind.*		
2.3.7	Es werden keine Cipher Suites für SSL2, SSL3, TLS 1.0 oder TLS 1.1 unterstützt. *Prüfanweisung (ssllabs): Prüfung, dass das Feld „Cipher Suites“ für SSL2, SSL3, TLS 1.0 oder TLS 1.1 keinerlei Cipher Suites gelistet sind.*		

2.4 Algorithmen und Parameter des Handshakes

Nr.	*Zu prüfende Anforderungen*	*Erfüllt*	
		Ja	*Nein*
2.4.1*	Die verwendeten ephemeren Parameter während des TLS-Handshakes bieten ausreichende Sicherheit: • ECDHE-Cipher Suites: ▪ brainpoolP256r1 ▪ brainpoolP384r1 ▪ brainpoolP512r1 ▪ secp224r1 ▪ secp256r1 ▪ secp384r1 ▪ secp521r1 • DHE-Cipher Suites: ▪ Mindestens 2048 Bit *Prüfanweisung (ssllabs): Prüfung, dass die angezeigten Parameter zu DHE- bzw. ECDHE-Cipher Suites in Feld „Cipher Suites“ den o.g. Anforderungen entsprechen.*		
2.4.2*	Für die Erstellung und Verifikation von Signaturen während des TLS-Handshakes werden folgende Algorithmen verwendet: • Signaturalgorithmus: ◦ RSA ◦ ECDSA • Hashfunktion: ◦ SHA-224 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512 *Prüfanweisung: Prüfung der Konfigurationseinstellungen der TLS-Bibliothek.*		

2.5 Vorgaben zu weiteren Protokoll-Details

Nr.	***Zu prüfende Anforderungen***	***Erfüllt***	
		Ja	***Nein***
2.5.1	Client-initiierte Session Renegotiation wird nicht unterstützt. *Prüfanweisung (ssllabs):Prüfung, dass „Secure Client-initiated Renegotiation“ und „Insecure Client-initiated Renegotiation” auf „No“ stehen.*		
2.5.2	TLS-Kompression wird nicht unterstützt. *Prüfanweisung (ssllabs): Prüfung, dass der Eintrag „SSL/TLS compression“ auf „No“ steht.*		
2.5.3	Die Heartbeat-Extension wird nicht unterstützt. *Prüfanweisung (ssllabs): Prüfung, dass der Eintrag „Heartbeat“ auf „No“ steht.*		
2.5.4	Die „truncated_hmac“-Extension wird nicht unterstützt.		

2.6 Weitere Empfehlungen (nicht verpflichtend)

Nr.	***Zu prüfende Anforderungen***	***Erfüllt***	
		Ja	***Nein***
2.6.1	Es werden nur Cipher Suites mit „Perfect Forward Secrecy“ unterstützt. (Nur Cipher Suites die mit „TLS_ECDHE“ oder „TLS_DHE“ beginnen) (EMPFOHLEN)		
2.6.2	Die „Encrypt-then-MAC“-Extension wird unterstützt (EMPFOHLEN).		
2.6.3	OCSP-Stapling wird unterstützt (EMPFOHLEN). *Prüfanweisung (ssllabs): Prüfung, dass der Eintrag „OCSP stapling“ auf „Yes“ steht.*		
2.6.4	Die „Extended-Master-Secret-Extension“ wird unterstützt (EMPFOHLEN).		
2.6.5	Das Server-Zertifikat ist ein qualifiziertes Webseiten-Zertifikat gemäß eIDAS-VO oder ein Extended-Validation-Zertifikat (EMPFOHLEN). *Prüfanweisung (ssllabs): Prüfung, dass der Eintrag „Extended Validation“ „Yes“ enthält.*		

3 Cipher Suites

3.1 Cipher Suites für TLS 1.2

Cipher Suites	*Unterstützung*	*Priorität*[1]
Server mit EC-Public Key		
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	MUSS	3
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	MUSS	3
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	EMPFOHLEN	3
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	EMPFOHLEN	3
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	OPTIONAL	1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	OPTIONAL	1
Server mit RSA-Public Key		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	MUSS	3
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	MUSS	3
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	EMPFOHLEN	3
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	EMPFOHLEN	3
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	OPTIONAL	2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	OPTIONAL	2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	OPTIONAL	2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	OPTIONAL	2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	OPTIONAL	2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	OPTIONAL	1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	OPTIONAL	1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	OPTIONAL	1
Weitere Hinweise[2]		

1 Ein größerer Prioritätswert impliziert eine höhere Priorität.

2 Sofern mit TLS keine personenbezogenen Daten verarbeitet werden, ist prinzipiell auch möglich zusätzlich Cipher Suites der Form TLS_ECDH_ECDSA*, TLS_DH_DSS_*, TLS_DH_RSA_* oder TLS_DH_RSA* zu unterstützen. Dies wird aber nicht empfohlen. Im Falle der Unterstützung sind diese Cipher Suites mit geringster Priorität zu verwenden, da sie keine Perfect Forward Secrecy bieten. Zudem sollten hierfür separate Schlüsselpaare und Zertifikate verwendet werden.

3.2 Cipher Suites für TLS 1.3

Cipher Suites	*Unterstützung*	*Priorität*[3]
TLS_AES_128_GCM_SHA256	EMPFOHLEN	1
TLS_AES_256_GCM_SHA384	EMPFOHLEN	1
TLS_AES_128_CCM_SHA256	EMPFOHLEN	1

3 Ein größerer Prioritätswert impliziert eine höhere Priorität.