Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Klarstellungen und Anwendungshinweise zu BSI TR-03153-TS und BSI-CC-PP-0105-V2-2020

17. November 2020

1 Einleitung

Dieses Dokument ergänzt [TR-03153-TS] sowie die [Erg. TR-03153-TS] um Prüfanweisungen basierend auf den Klarstellungen und Anwendungshinweisen zu BSI TR-03153 und BSI-CC-PP-0105-V2-2020 [KuA TR-03153 CC-PP-0105]. Das Grundlagendokument für die Konformitätsprüfung ist weiterhin die Testspezifikation [TR-03153-TS], ergänzt um die Hinweise aus [Erg. TR-03153-TS] und das vorliegende Dokument.

1.1 Schlüsselworte

Anforderungen als Ausdruck normativer Festlegungen werden durch die in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS / MÜSSEN, DARF NICHT / DÜRFEN NICHT, VERPFLICHTEND, SOLLTE / SOLLTEN, EMPFOHLEN, SOLLTE NICHT / SOLLTEN NICHT, KANN / KÖNNEN / DARF / DÜRFEN, und OPTIONAL gekennzeichnet. Die verwendeten Schlüsselworte sind auf Basis der folgenden Übersetzungstabelle gemäß [RFC-2119] zu interpretieren:

Deutsch	Englisch
MUSS / MÜSSEN	MUST
DARF NICHT / DÜRFEN NICHT	MUST NOT
VERPFLICHTEND	REQUIRED
SOLLTE / SOLLTEN	SHOULD
SOLLTE NICHT / SOLLTEN NICHT	SHOULD NOT
EMPFOHLEN	RECOMMENDED

2 Ergänzende Prüfungen

In diesem Abschnitt werden ergänzende Prüfungen spezifiziert. Diese sollen den korrekten Betrieb der TSE sowie eine einheitliche Struktur der durch die TSE erzeugten Log-Nachrichten gewährleisten.

Alle Prüfungen MÜSSEN im Rahmen einer Konformitätsprüfung nach [TR-03153-TS] durchgeführt werden, es sei denn, im Folgenden werden anderweitige Angaben gemacht.

2.1 Architektur des Sicherheitsmoduls

Diese Gruppe enthält ergänzende Prüfungen, welche die Architektur des Sicherheitsmoduls bewerten. Hierbei MUSS die Prüfstelle testen, ob die vorliegende TSE den Klarstellungen und Anwendungshinweisen aus [KuA TR-03153 CC-PP-0105] genügt.

2.1.1 Ergänzende Angaben zum ICS

Der Hersteller MUSS ergänzend zum Implementation Conformance Statement (ICS) eine Dokumentation bereitstellen, in der die logische Architektur des Sicherheitsmoduls in Bezug auf die Anforderungen aus [KuA TR-03153 CC-PP-0105] beschrieben wird.

Hieraus MUSS insbesondere Folgendes hervorgehen:

- Werden mehrere SMAERS-Einheiten auf einer SMAERS zusammengefasst?
- Umfasst die Architektur mehrere SMAERS?
- Werden mehrere CSP-Einheiten auf einem CSP betrieben? Liegt ein Cluster-Betrieb vor?

- Umfasst die Architektur mehrere CSP?
- Wie sind SMAERS(-Einheiten) und CSP(-Einheiten) miteinander verbunden? Gibt es Fernverbindungen?
- Wie sprechen die Aufzeichnungssysteme die TSE an?

Kann die TSE in verschiedenen Konfigurationen betrieben werden, so MUSS die Dokumentation für jede mögliche Konfiguration mit dem Prüfbericht vorgelegt werden.

2.1.2 Prüfung zu der genutzten Architektur des Sicherheitsmoduls

Die folgenden zusätzlichen Prüfungen MÜSSEN von der Prüfstelle durchgeführt werden:

Testfall-ID	Beschreibung
SM_ARCH_01	Prüfung, ob die Technische Sicherheitseinrichtung genau einen eindeutigen Signaturschlüssel besitzt, welcher im Sicherheitsmodul gespeichert ist.
SM_ARCH_02	Prüfung, ob jede Technische Sicherheitseinrichtung genau ein Sicherheitsmodul enthält.
SM_ARCH_03	Prüfung, ob das Sicherheitsmodul jeder Technischen Sicherheitseinrichtung aus einer Sicherheitsmodulanwendung und einem Krypto-Kern besteht.
SM_ARCH_04	Prüfung, ob die Sicherheitsmodulanwendung des Sicherheitsmoduls einer Technischen Sicherheitseinrichtung aus genau einer SMAERS-Einheit besteht, welche über genau einen eindeutigen Transaktionszähler verfügt.
SM_ARCH_05	Prüfung, ob der Krypto-Kern des Sicherheitsmoduls einer Technischen Sicherheitseinrichtung aus genau einer CSP-Einheit besteht, welche über genau einen Signatur-Schlüssel (inkl. zugehörigem Signaturzähler) verfügt.
SM_ARCH_06	Prüfung, ob die SMAERS-Einheit einer Technischen Sicherheitseinrichtung immer eineindeutig der CSP-Einheit der jeweiligen Technischen Sicherheitseinrichtung zugeordnet ist und umgekehrt. Insbesondere ist jedem Signaturschlüssel einer CSP-Einheit eines CSPs genau ein Transaktionszähler einer SMAERS-Einheit eines SMAERS zugeordnet und umgekehrt.
SM_ARCH_07	Prüfung, ob jedes Aufzeichnungssystem genau einem Signaturschlüssel genau einer CSP-Einheit und genau einem Transaktionszähler genau einer SMAERS-Einheit zugeordnet wird.
SM_ARCH_08	Prüfung, ob ein Aufzeichnungssystem bei Betrieb von mehreren TSEn auf SMAERS und CSP immer nur genau einer TSE zugeordnet wird.
SM_ARCH_09	Prüfung, ob zeitnah aufgezeichnet werden kann, wenn die TSE mit der im ICS angegebenen Anzahl von maximalen Clients und Transaktionen parallel angesprochen wird. Hierbei muss jeder Client mindestens alle MAX_UPDATE_DELAY-Sekunden die Transaktion aktualisieren.

2.2 Ergänzende Testfälle zu Log-Nachrichten

Im Rahmen von [KuA TR-03153 CC-PP-0105] wurden zusätzliche Log-Nachrichten des Typs System-Log definiert. Diese MÜSSEN auch im Rahmen der Konformitätsprüfung geprüft werden.

2.2.1 Ergänzende ICS-Angaben

Der Hersteller MUSS alle Log-Nachrichten, die über die in der [TR-03151] definierten Log-Nachrichten hinausgehen, auflisten und die Auflistung der Prüfstelle zur Verfügung stellen. Die Auflistung umfasst das genaue Format und ist Teil der Herstellerdokumentation. Bei der Angabe des Formates muss sich an die

Struktur der Log-Beschreibung aus [TR-03151] gehalten werden. Die Prüfstelle MUSS diese Auflistung auf Konformität zu [KuA TR-03153 CC-PP-0105] prüfen und MUSS der Zertifizierungsstelle im Prüfbericht darüber berichten.

2.2.2 Prüfung der ergänzenden Log-Nachrichten

Die folgenden zusätzlichen Prüfungen MÜSSEN von der Prüfstelle durchgeführt werden:

Testfall-ID	Beschreibung
EXP_LOG_18	Formale und praktische Prüfung, ob die TSE ausschließlich solche Log-Nachrichten produziert, die in der [TR-03151] und den [KuA TR-03153 CC-PP-0105] definiert sind. Die Prüfung erfolgt sowohl anhand der Herstellerangaben als auch durch Durchsicht aller während der Durchführung der Gesamtheit der Tests auftretenden Log-Nachrichten[1].
EXP_LOG_19	Prüfung, ob die TSE alle[2] von [TR-03151] und [KuA TR-03153 CC-PP-0105] als verpflichtend eingestuften Log-Nachrichten erstellt.

Die folgenden ergänzenden Prüfungen MÜSSEN von der Prüfstelle durchgeführt werden. Der jeweilige Template-Testfall ist für alle[3] in der darauf folgenden Tabelle aufgelisteten Events / Befehlsaufrufe durchzuführen. Nur bei Lognachrichten, welche laut [KuA TR-03153 CC-PP-0105] bzw. [TR-03151], durch optionale Funktionalitäten erzeugt werden, sind auch die passenden Template-Testfälle OPTIONAL. Ein Beispiel hierfür ist deleteStoredData.

Testfall-ID	Beschreibung
EXP_LOG_20_Template	Prüfung, ob eine Log-Nachricht für das abzusichernde Ereignis (Event) bzw. den Befehlsaufruf erstellt wurde.

Auf Testfall EXP_LOG_20_Template anzuwendende Verfeinerungen:

Testfall-ID	Event / aufgerufener Befehl
EXP_LOG_20_A	initialize
EXP_LOG_20_B	updateTime
EXP_LOG_20_C	disableSecureElement
EXP_LOG_20_D	authenticateUser
EXP_LOG_20_E	logOut
EXP_LOG_20_F	unblockUser
EXP_LOG_20_G	authenticateSmaersAdmin

[1] Stellt die Prüfstelle während der Durchführung der Testfälle fest, dass andere, nicht in den genannten Dokumenten definierte, Log-Nachrichten erstellt werden, so MUSS dies im Prüfbericht festgehalten werden.

[2] Gemäß Kapitel 3 [KuA TR-03153 CC-PP-0105] sind nach älteren Versionen der Schutzprofile zertifizierte Sicherheitsmodule von der Verpflichtung, bestimmte System-Logs zu erzeugen, ausgenommen. Genaueres ist den Anwendungshinweisen selbst zu entnehmen.

[3] Gemäß Kapitel 3 [KuA TR-03153 CC-PP-0105] sind nach älteren Versionen der Schutzprofile zertifizierte Sicherheitsmodule von der Verpflichtung, bestimmte System-Logs zu erzeugen, ausgenommen. Genaueres ist den Anwendungshinweisen selbst zu entnehmen.

Testfall-ID	Event / aufgerufener Befehl
EXP_LOG_20_H	updateDevice
EXP_LOG_20_I	updateDeviceCompleted
EXP_LOG_20_J	startAudit
EXP_LOG_20_K	configureLogging
EXP_LOG_20_L	enterSecureState
EXP_LOG_20_M	exitSecureState
EXP_LOG_20_N	selfTest
EXP_LOG_20_O	deleteStoredData
EXP_LOG_20_P	lockTransactionLogging
EXP_LOG_20_Q	unlockTransactionLogging
EXP_LOG_20_R	registerClient
EXP_LOG_20_S	deregisterClient

Testfall-ID	Beschreibung
EXP_LOG_21_Template	Prüfung, ob die Struktur der Log-Nachricht den Vorgaben in den Klarstellungen und Anwendungshinweisen sowie der TR-03151 entspricht. Es dürfen nur die vorgegebenen Elemente in den Log-Nachrichten enthalten sein.

Auf Testfall EXP_LOG_21_Template anzuwendende Verfeinerungen:

Testfall-ID	Event / aufgerufener Befehl
EXP_LOG_21_A	initialize
EXP_LOG_21_B	updateTime
EXP_LOG_21_C	disableSecureElement
EXP_LOG_21_D	authenticateUser
EXP_LOG_21_E	logOut
EXP_LOG_21_F	unblockUser
EXP_LOG_21_G	authenticateSmaersAdmin
EXP_LOG_21_H	updateDevice
EXP_LOG_21_I	updateDeviceCompleted
EXP_LOG_21_J	startAudit
EXP_LOG_21_K	configureLogging
EXP_LOG_21_L	enterSecureState
EXP_LOG_21_M	exitSecureState
EXP_LOG_21_N	selfTest
EXP_LOG_21_O	deleteStoredData
EXP_LOG_21_P	lockTransactionLogging

Testfall-ID	Event / aufgerufener Befehl
EXP_LOG_21_Q	unlockTransactionLogging
EXP_LOG_21_R	registerClient
EXP_LOG_21_S	deregisterClient

Testfall-ID	Beschreibung
EXP_LOG_22_Template	Prüfung, ob die Inhalte der Log-Nachricht den Vorgaben in den Klarstellungen und Anwendungshinweisen sowie der TR-03151 entsprechen.

Auf Testfall EXP_LOG_22_Template anzuwendende Verfeinerungen:

Testfall-ID	Event / aufgerufener Befehl
EXP_LOG_22_A	initialize
EXP_LOG_22_B	updateTime
EXP_LOG_22_C	disableSecureElement
EXP_LOG_22_D	authenticateUser
EXP_LOG_22_E	logOut
EXP_LOG_22_F	unblockUser
EXP_LOG_22_G	authenticateSmaersAdmin
EXP_LOG_22_H	updateDevice
EXP_LOG_22_I	updateDeviceCompleted
EXP_LOG_22_J	startAudit
EXP_LOG_22_K	configureLogging
EXP_LOG_22_L	enterSecureState
EXP_LOG_22_M	exitSecureState
EXP_LOG_22_N	selfTest
EXP_LOG_22_O	deleteStoredData
EXP_LOG_22_P	lockTransactionLogging
EXP_LOG_22_Q	unlockTransactionLogging
EXP_LOG_22_R	registerClient
EXP_LOG_22_S	deregisterClient

2.2.3 Ergänzung zu Prüfungen für Sicherheitsmodule in einer Client-Server-Architektur

Falls der Hersteller erklärt, dass die CSP-Einheit der Technischen Sicherheitseinrichtung einen von mehreren TSEn gleichzeitig nutzbaren CSP, bzw. einen CSP im Cluster-Betrieb, nutzt, so MUSS geprüft werden, ob bei Auftritt eines Audit-Events der CSP-Einheit beziehungsweise des CSPs für jede angeschlossene TSE eine zugehörige Audit-Log-Nachricht erstellt wird:

Testfall-ID	Beschreibung
EXP_LOG_23	Prüfung, ob bei Auftritt eines Audit-Events der CSP-Einheit beziehungsweise des CSPs für jede[4] angeschlossene TSE unverzüglich eine zugehörige Audit-Log-Nachricht erstellt wird und diese mit den jeweiligen privaten Schlüsseln der Technischen Sicherheitseinrichtungen signiert und durch diese gespeichert werden.

Die folgenden Prüffälle MÜSSEN durchgeführt werden, wenn SMAERS und CSP in einer Client-Server-Architektur angeordnet sind:

Testfall-ID	Beschreibung
EXP_LOG_24	Prüfung, ob bei einer Unterbrechung der oder Fehler in der Verbindung zwischen den CSP-Einheit und SMAERS-Einheit keine Log-Nachrichtenteile verloren gehen können.
EXP_LOG_25	Prüfung, ob durch Fehler bei der Übertragung keine Lücken in der Sequenz der Transaktions- und Signaturzählerstände entstehen können.

2.2.4 Prüfung von additionalExternalData und additionalInternalData

Die folgenden Testfälle prüfen das korrekte Verhalten des Sicherheitsmoduls bezüglich der in Transaction- und (teilweise) System-Logs enthaltenen Felder additionalExternalData und additionalInternalData. Sie MÜSSEN durchgeführt werden:

Testfall-ID	Beschreibung
EXP_LOG_26	Prüfung, ob bei Erstellung aller Transaction-Log-Varianten das Feld additionalInternalData nicht belegt wird.
EXP_LOG_27	Prüfung, ob bei Erstellung aller Transaction-Log-Varianten das Feld additionalExternalData nicht belegt wird, wenn keine zusätzlichen Daten (additionalData / additionalExternalData oder andere) vom Aufzeichnungssystem an die TSE übergeben wurden.
EXP_LOG_28	Prüfung, ob die TSE alle Transaction-Log-Varianten korrekt erstellt, wenn das Aufzeichnungssystem, den Vorgaben zuwider, zusätzliche Daten für das Feld additionalExternalData übergibt.
EXP_LOG_29	Prüfung, ob bei Erstellung aller System-Logs das Feld additionalInternalData nicht belegt wird.

2.2.5 Ergänzung zu Prüfungen zur Zeitführung im Sicherheitsmodul

Falls der Hersteller in der Erläuterung seiner Architektur erklärt, dass seine TSE einen zentral betriebenen CSP nutzt, MUSS, gemäß den Klarstellungen und Anwendungshinweisen [KuA TR-03153 CC-PP-0105] und der [TR-03153-TS] sichergestellt werden, dass beim Stellen der Zeit ein System-Log des Typs updateTime erstellt wird:

[4] Vereinfachung der Tests: Die Tests KÖNNEN mit einer exemplarischen Anzahl von TSEn durchgeführt werden, welche vermuten lässt, dass sich die Verteilung der Nachrichten für die Gesamtanzahl der unterstützten TSEn analog verhält.

Testfall-ID	Beschreibung
SM_TME_12	Prüfung, ob als Reaktion auf jedes Stellen der Zeitführung einer CSP-Einheit bzw. des CSPs unmittelbar korrekte System-Log-Nachrichten des Typs updateTime nach TR-03151 erstellt werden und diese mit den jeweiligen privaten Schlüsseln der Technischen Sicherheitseinrichtungen signiert und durch diese gespeichert werden.
SM_TME_13	Prüfung, ob beim Aufruf der Funktion updateTime über die SE-API die Exception „ErrorFunctionNotSupported“ zurückgegeben wird, wenn eine Zeitstellung über die SE-API nicht von der TSE unterstützt wird.

2.2.6 Ergänzung zu Prüfungen zur Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung

Der folgenden Testfälle prüfen, ob eine Deaktivierung der TSE im Sinne der [TR-03153] und [TR-03151] erfolgt. Die Testfälle MÜSSEN durchgeführt werden.

Testfall-ID	Beschreibung
II_DSE_08	Prüfung, ob bei Stoppen der Audit-Funktionalität in der Sicherheitsmodulanwendung eine permanente Deaktivierung des Sicherheitsmoduls erfolgt. Prüfung, ob diese permanente Deaktivierung durch ein System-Log des Typs disableSecureElement quittiert wird.
II_DSE_09	Prüfung, ob bei Deaktivierung des Sicherheitsmoduls durch die Funktionalität von disableSecureElement die Audit-Funktionalität im Sicherheitsmodul gestoppt wird.

2.2.7 Ergänzung zu Prüfungen zur Herstellerdokumentation

Der folgenden Testfälle prüfen die Geeignetheit der Herstellerdokumentation zur Sicherstellung der unmittelbaren Aufzeichnung durch die TSE. Die Testfälle MÜSSEN durchgeführt werden:

Testfall-ID	Beschreibung
DOC_PAR_01	Prüfung, ob der Hersteller den Anwender / Nutzer (Steuerpflichtigen) in einer Herstellerdokumentation zum Produkt darüber informiert, inwieweit die Nutzung mehrerer Aufzeichnungssysteme oder Eingabegeräte mit der TSE zulässig ist und welche Verzögerungen und Probleme bei den Betrieb der TSE mit mehreren Aufzeichnungssystemen zu erwarten sind.
DOC_DLY_01	Prüfung, ob der Hersteller den Anwender / Nutzer (Steuerpflichtigen) in einer Herstellerdokumentation über die Durchführungszeiten und mögliche Verzögerungen bei der Absicherung paralleler Transaktionen aufklärt, insbesondere in Bezug auf die Dauer der Signaturerstellung in Abhängigkeit gleichzeitig zu bearbeitender Absicherungen.

3 Literaturverzeichnis

Verweis	Quelle
[Erg. TR-03153-TS]	BSI: Ergänzung der Technischen Richtlinie TR-03153: Testspezifikation (TS), 02.12.2019
[KuA TR-03153 CC-PP-0105]	BSI: Klarstellungen und Anwendungshinweise zu BSI TR-03153 und BSI-CC-PP-0105-V2-2020
[RFC-2119]	Bradner, S: Key words for use in RFCs to indicate requirement levels
[TR-03151]	BSI: Technical Guideline BSI TR-03151 Secure Element API (SE API), Version 1.0.1, 20.12.2018
[TR-03153]	BSI: Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1, 20.12.2018
[TR-03153-TS]	BSI: TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme Testspezifikation (TS), Version 1.0.1, 05.02.2019