



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

BSI TR-03153-1-TS

Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Teil 1: Anforderungen an die Technische Sicherheitseinrichtung
Testspezifikation (TS)

Version 1.1.1
2024-08-30



Änderungshistorie

Version	Datum	Beschreibung
1.0.1	5. Februar 2019	Initiale Version
1.1.0	19. Dezember 2023	Spezifikation entsprechend TR-03153-1 Version 1.1.0
1.1.1	30. August 2024	Entfernung der Wahlmöglichkeit des Profils configureLogging im ICS. Barrierefreiheitsverbesserungen.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: registrierkassen@bsi.bund.de
Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2024

Inhaltsverzeichnis

<u>1</u>	<u>EINLEITUNG.....</u>	<u>10</u>
1.1	MOTIVATION UND ZIELE	10
1.2	INHALT UND ABGRENZUNG	10
<u>2</u>	<u>GENERELLE ANFORDERUNGEN AN DIE DURCHFÜHRUNG VON PRÜFUNGEN UND DEN PRÜFBERICHT</u>	<u>11</u>
<u>3</u>	<u>WEITERE ANFORDERUNGEN AN DIE DURCHFÜHRUNG VON PRÜFUNGEN VON TECHNISCHEN SICHERHEITSEINRICHTUNGEN</u>	<u>12</u>
3.1	AUFBAU UND ABLAUF DER PRAKTISCHEN TESTDURCHFÜHRUNG BEI EINER TSE	12
3.2	BEISPIEL EINER TESTDURCHFÜHRUNG	13
<u>4</u>	<u>PROFILE</u>	<u>16</u>
4.1	SPEICHERMEDIUM-PROFILE	16
4.2	SICHERHEITSMODUL-PROFILE	16
4.3	SCHNITTSTELLEN-PROFILE	17
4.4	ALLGEMEINE PROFILE	19
<u>5</u>	<u>IMPLEMENTATION CONFORMANCE STATEMENT.....</u>	<u>21</u>
5.1	HERSTELLERERKLÄRUNG	21
5.2	VERSICHERUNG ZU GEMACHTEN ANGABEN	32
5.3	ZUSTIMMUNG ZUR VERÖFFENTLICHUNG DER BESCHRÄNKUNGEN	32
<u>6</u>	<u>MODULE.....</u>	<u>33</u>
6.1	MODUL STORAGE – SPEICHERMEDIUM (STO)	33
6.1.1	FUNKTIONALE PRÜFUNGEN VON SPEICHERMEDIEN (STO_FUN)	33
6.1.2	PRÜFUNGEN DER SPEICHERKAPAZITÄT VON SPEICHERMEDIEN (STO_CAP)	35
6.1.3	PRÜFUNGEN DER ZUVERLÄSSIGKEIT VON SPEICHERMEDIEN (STO_REL)	35
6.1.4	PRÜFUNGEN FÜR FERNVERBUNDENE SPEICHERMEDIEN (STO_REM)	35
6.2	MODUL SECURITY MODULE – SICHERHEITSMODUL (SM)	35
6.2.1	PRÜFUNG ZU DER GENUTZTEN ARCHITEKTUR DES SICHERHEITSMODULS (SM_ARCH)	35
6.2.2	PRÜFUNGEN ZUR KONKATENATION UND SIGNATURERSTELLUNG (SM_CON)	37
6.2.3	PRÜFUNGEN ZUR ZEITFÜHRUNG IM SICHERHEITSMODUL (SM_TME)	39

6.2.4	PRÜFUNGEN ZUM SIGNATURZÄHLER IM SICHERHEITSMODUL (SM_SIG)	42
6.2.5	PRÜFUNGEN ZUR TRANSAKTIONSNUMMER IM SICHERHEITSMODUL (SM_TRA)	43
6.2.6	PRÜFUNGEN ZUR KRYPTOGRAPHIEANWENDUNG IM SICHERHEITSMODUL (SM_KRY)	44
6.2.7	PRÜFUNGEN DER PUBLIC-KEY-INFRASTRUKTUR VON SICHERHEITSMODULEN (SM_PKI)	45
6.2.8	PRÜFUNGEN FÜR FERNVERBUNDENE SICHERHEITSMODULE (SM_REM)	45
6.2.9	PRÜFUNGEN FÜR DIE SICHERHEITSMODULANWENDUNG (SM_LOG)	46
6.2.10	DEAKTIVIERUNG DES SICHERHEITSMODULS (SM_AUD)	47
6.3	MODUL INTEGRATION INTERFACE – EINBINDUNGSSCHNITTSTELLE	47
6.3.1	BASISPRÜFUNGEN DER EINBINDUNGSSCHNITTSTELLE (II)	47
6.3.1.1	Authentifizierung von Nutzern der Technischen Sicherheitseinrichtung (II_AUT)	47
6.3.1.2	Abmeldung von Nutzern der Technischen Sicherheitseinrichtung (II_LGO)	60
6.3.1.3	Entsperren von Nutzern (II_UBP)	61
6.3.1.4	Initialisierung der Technischen Sicherheitseinrichtung (II_INI)	62
6.3.1.5	Setzen von Beschreibungen in der TSE (II_SDE)	62
6.3.1.6	Abfrage der TSE Beschreibung (II_GDE)	62
6.3.1.7	Auslösen eines Selbsttests (II_STE)	63
6.3.1.8	Geräte-Update (II_UDD)	64
6.3.1.9	Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung (II_DSE)	65
6.3.1.10	Abfrage zur Gesamtkapazität des Speichermediums (II_GTM)	65
6.3.1.11	Abfrage zur aktuell verwendeten Speicherkapazität (II_GUM)	66
6.3.1.12	Abfrage zur freien Speicherkapazität (II_GFM)	66
6.3.1.13	Abfrage zum Gesundheitszustand aller Komponenten der TSE (II_GDH)	66
6.3.1.14	Abfrage der TSE Version (II_GCV)	67
6.3.1.15	Abfrage zum Datum des voraussichtlichen Nutzungsendes (II_GEU)	68
6.3.1.16	Aktualisierung der Uhrzeit (II_UDT)	68
6.3.1.17	Abfrage der unterstützten Variante zur Aktualisierung der Zeit (II_TSV)	69
6.3.1.18	Abfrage der aktuellen eingestellten Zeit (II_GCT)	70
6.3.1.19	Konfiguration der Protokollierung von Ereignissen (II_CLG)	70
6.3.1.20	Export des TAR-Containers (II_EXP)	70
6.3.1.21	Zertifikatsexport (II_EXC)	72
6.3.1.22	Löschen von gespeicherten Daten im Speichermedium (II_DLM)	72
6.3.1.23	Export von Seriennummern (II_ESN)	73
6.3.1.24	Prüfungen zum aktuellen Stand der Signaturzähler (II_CSC)	73
6.3.1.25	Wiederherstellung durch ein Backup (II_RFB)	74
6.3.1.26	Lesen der letzten Log-Nachricht (II_GLL)	75
6.3.1.27	Registrieren von Aufzeichnungssystemen (II_REC)	76
6.3.1.28	Deregistrieren von Aufzeichnungssystemen (II_DRC)	77
6.3.1.29	Starten einer Transaktion (II_STA)	78
6.3.1.30	Aktualisierung einer Transaktion (II_UPD)	79
6.3.1.31	Beenden einer Transaktion (II_FIN)	81
6.3.1.32	Export von Transaktions-Log-Nachrichten (II_EXF)	83
6.3.1.33	Abfrage der unterstützten Varianten für die Aktualisierung von Transaktionen (II_UTV)	95
6.3.1.34	Abfrage der aktuellen Anzahl von Aufzeichnungssystemen der Technischen Sicherheitseinrichtung (II_CNC)	95
6.3.1.35	Abfrage der maximalen Anzahl von simultanen Aufzeichnungssystemen der Technischen Sicherheitseinrichtung (II_MNC)	97

6.3.1.36	Abfrage zu registrierten Aufzeichnungssystemen (II_GRC)	98
6.3.1.37	Abfrage der aktuellen Anzahl von parallel geöffneten Transaktionen (II_CNT)	99
6.3.1.38	Abfrage der maximalen Anzahl von parallelen Transaktionen (II_MNT)	100
6.3.1.39	Abfrage zum Stadium einer Transaktion (II_GTS)	100
6.3.1.40	Abfrage der Transaktionsnummern aller nicht beendeten Transaktionen (II_GOT)	101
6.3.1.41	Abfrage zum aktuellen Transaktionszählers (II_CTC)	102
6.3.1.42	Ausgabe der letzten Transaktions-Log-Nachricht (II_GLT)	103
6.3.1.43	Sperren von Log-Nachrichten von Transaktionen (II_LTL)	104
6.3.1.44	Entsperren von Log-Nachrichten von Transaktionen (II_UTL)	105
6.3.1.45	Verwendung der Technischen Sicherheitseinrichtung durch mehrere Aufzeichnungssysteme (II_MCU)	105
6.3.1.46	Allgemeine Fehlermeldungen (II_ERR)	106
6.3.1.47	Unterstützung von herstellerspezifische Funktionalitäten der Einbindungsschnittstelle (II_ADD)	124
6.3.2	PRÜFUNGEN DER STANDARDSCHNITTSTELLEN GEMÄß BSI TR-03151-2 (SDI)	124
6.3.2.1	Verwendete Varianten der Einbindungsschnittstelle (SDI_IMP)	124
6.3.2.2	Funktionsnamen der Standardschnittstelle (SDI_FUN)	124
6.3.2.3	Fehlermeldungen der Standardschnittstelle (SDI_ERR)	128
6.3.2.4	Parameter der Standardschnittstelle (SDI_PAR)	128
6.3.3	PRÜFUNGEN FÜR HERSTELLERSPEZIFISCHE FUNKTIONALITÄTEN DER EINBINDUNGSSCHNITTSTELLE (ADD)	130
6.3.3.1	Beschreibung der Funktionalitäten (ADD_DOC)	130
6.3.3.2	Unterscheidbarkeit herstellerspezifische Funktionalitäten zur Standardschnittstelle (ADD_DIF)	131
6.3.3.3	Abwandlungen von Standardfunktionen (ADD_ABW)	131
6.4	PRÜFUNGEN DER EXPORTDATEN GEMÄß BSI TR-03153-1 (EXP)	131
6.4.1	TAR-FORMAT (EXP_TAR)	131
6.4.2	DATEI INFO.CSV (EXP_INF)	132
6.4.3	LOG-NACHRICHTEN (EXP_LOG)	132
6.5	ERGÄNZUNG ZU PRÜFUNGEN ZUR HERSTELLERDOKUMENTATION (DOC)	138
7	TESTFÄLLE	141
7.1	NOTATION VON TESTFÄLLEN	141
7.1.1	VERWENDUNG VON VARIABLEN	142
7.2	XML SCHEMA	142
LITERATURVERZEICHNIS		144
ANHANG		145
A.1	XML SCHEMA FÜR DIE XML-TESTFÄLLE DER BSI TR-03153-1-TS	145
A.2	XML BEISPIELE	147
A.3	DARSTELLUNG VON XML-TESTFÄLLEN IN EINEM WEBBROWSER	151

ABKÜRZUNGSVERZEICHNIS 152

Abbildungsverzeichnis

Abbildung 1: Testdurchführung für eine TSE mit Einbindungsschnittstelle nach [BSI TR-03153-1].....	13
Abbildung 2: Erste Phase in Bezug auf das Testen der Funktion startTransaction	14
Abbildung 3: Zweite Phase in Bezug auf das Testen der Funktion startTransaction.....	15
Abbildung 4: Darstellung eines XML-Testfalls in einem Webbrowser.....	151

Tabellenverzeichnis

Tabelle 1: Profil für das Speichermedium der Technischen Sicherheitseinrichtung.....	16
Tabelle 2: Profile für das Sicherheitsmodul.....	17
Tabelle 3: Profile der Einbindungsschnittstelle gemäß [BSI TR-03153-1].....	18
Tabelle 4: Profil für herstellereigene Funktionalitäten der Einbindungsschnittstelle	18
Tabelle 5: Profile für optionale Funktionen.....	19
Tabelle 6: Profile zu allgemeinen Eigenschaften einer TSE.....	20
Tabelle 7: ICS - Profile der Eigenschaften der Technischen Sicherheitseinrichtung	24
Tabelle 8: ICS - Profile der verfügbaren Funktionen der Technischen Sicherheitseinrichtung	26
Tabelle 9: Angaben zu verwendeten Kryptofunktionen für die Absicherungsschritte der TSE	27
Tabelle 10: Angaben zu verwendeten Kryptofunktionen der PKI.....	27
Tabelle 11: Zusätzliche Angaben zu den Komponenten der Technischen Sicherheitseinrichtung	28
Tabelle 12: Zusätzliche Angaben zum verwendeten Zeitformat.....	28
Tabelle 13: Zusätzliche Angaben zu der Anzahl von gleichzeitigen Aufzeichnungssystemen der TSE.....	28
Tabelle 14: Zusätzliche Angaben zu der maximalen Anzahl von parallel geöffneten Transaktionen.....	28
Tabelle 15: Zusätzliche Angaben zu der maximalen Anzahl von parallel genutzten Technische Sicherheitseinrichtungen.....	29
Tabelle 16: Weitere Angaben zur TSE.....	32
Tabelle 17: Testfälle zur Funktionalität des Speichermediums	35
Tabelle 18: Prüfungen der Speicherkapazität von Speichermedien.....	35
Tabelle 19: Prüfungen der Zuverlässigkeit von Speichermedien.....	35
Tabelle 20: Prüfungen für fernverbundene Speichermedien	35
Tabelle 21: Prüfung zu der genutzten Architektur des Sicherheitsmoduls.....	37
Tabelle 22: Testfälle zur Konkatenation und Signaturerstellung.....	39
Tabelle 23: Testfälle zur Zeitführung im Sicherheitsmodul	42
Tabelle 24: Auf Testfälle SM_TME_08_Template, SM_SIG_08_Template anzuwendende Verfeinerungen.....	42
Tabelle 25: Testfälle für Signaturzähler	43
Tabelle 26: Testfälle zur Transaktionsnummer im Sicherheitsmodul	44
Tabelle 27: Testfälle der Kryptographieanwendung des Sicherheitsmoduls	45
Tabelle 28: Testfälle der Public-Key-Infrastruktur von Sicherheitsmodulen.....	45
Tabelle 29: Testfälle für fernverbundene Sicherheitsmodule.....	46
Tabelle 30: Testfälle für die Sicherheitsmodulanwendung.....	46
Tabelle 31: Testfälle zur Deaktivierung des Sicherheitsmoduls	47
Tabelle 32: Testfälle für die Einbindungsschnittstelle – Authentifizierung von Nutzern	51

Tabelle 33: Auf Testfälle II_AUT_01_Template, II_AUT_03_Template, II_AUT_04_Template, II_AUT_05_Template, II_LGO_01_Template, II_LGO_02_Template, II_UBP_01_Template und II_UBP_02_Template anzuwendende Verfeinerungen	51
Tabelle 34: Auf Testfall II_AUT_06_Template anzuwendende Verfeinerungen	52
Tabelle 35: Auf Testfall II_AUT_07_Template anzuwendende Verfeinerungen	52
Tabelle 36: Auf Testfall II_AUT_08_Template anzuwendende Verfeinerungen	53
Tabelle 37: Auf Testfall II_AUT_09_Template anzuwendende Verfeinerungen	54
Tabelle 38: Auf Testfälle II_AUT_10_Template und II_AUT_12_Template anzuwendende Verfeinerungen	56
Tabelle 39: Auf Testfall II_AUT_11_Template anzuwendende Verfeinerungen	56
Tabelle 40: Auf Testfall II_AUT_13_Template anzuwendende Verfeinerungen	56
Tabelle 41: Auf Testfall II_AUT_14_Template anzuwendende Verfeinerungen	58
Tabelle 42: Auf Testfall II_AUT_15_Template anzuwendende Verfeinerungen	58
Tabelle 43: Auf Testfall II_AUT_16_Template anzuwendende Verfeinerungen	59
Tabelle 44: Auf Testfall II_AUT_17_Template anzuwendende Verfeinerungen	59
Tabelle 45: Auf Testfall II_AUT_18_Template anzuwendende Verfeinerungen	60
Tabelle 46: Testfälle für die Einbindungsschnittstelle – Abmelden von Nutzern.....	60
Tabelle 47: Testfälle für die Einbindungsschnittstelle – Entsperren der PIN eines autorisierten Nutzers	61
Tabelle 48: Testfälle für die Einbindungsschnittstelle – Initialisierung der Technischen Sicherheitseinrichtung	62
Tabelle 49: Testfälle für die Einbindungsschnittstelle – Setzen von Beschreibungen in der TSE	62
Tabelle 50: Testfälle für die Einbindungsschnittstelle – Abfrage der Beschreibung der TSE	63
Tabelle 51: Testfälle für die Einbindungsschnittstelle – Auslösen eines Selbsttests	63
Tabelle 52: Testfälle für die Einbindungsschnittstelle – Geräte-Update	65
Tabelle 53: Testfälle für die Einbindungsschnittstelle – Außerbetriebnahme des Sicherheitsmoduls.....	65
Tabelle 54: Testfälle für die Einbindungsschnittstelle – Abfrage der Gesamtkapazität des Speichermediums	66
Tabelle 55: Testfälle für die Einbindungsschnittstelle – Abfrage der aktuell verwendeten Speicherkapazität.....	66
Tabelle 56: Testfälle für die Einbindungsschnittstelle – Abfrage der freien Speicherkapazität	66
Tabelle 57: Testfälle für die Einbindungsschnittstelle – Abfrage zum Gesundheitszustand aller Komponenten der TSE	67
Tabelle 58: Testfälle für die Einbindungsschnittstelle – Abfrage der TSE Version.....	67
Tabelle 59: Testfälle für die Einbindungsschnittstelle – Abfrage zum Datum des voraussichtlichen Nutzungsendes.....	68
Tabelle 60: Testfälle für die Einbindungsschnittstelle - Aktualisierung der Zeit im Sicherheitsmodul.....	69
Tabelle 61: Testfälle für die Einbindungsschnittstelle – Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen	69
Tabelle 62: Testfälle für die Einbindungsschnittstelle – Abfrage der aktuellen eingestellten Zeit	70
Tabelle 63: Testfälle zu Protokolldateien für die Konfiguration von Ereignissen	70
Tabelle 64: Testfälle für die Einbindungsschnittstelle – Export aller Log-Nachrichten, zur Verifikation benötigten Zertifikate und Zusatzdateien.....	71
Tabelle 65: Testfälle für die Einbindungsschnittstelle - Ausgabe der Zertifikate der Zertifikatskette	72
Tabelle 66: Testfälle für die Einbindungsschnittstelle – Löschen der Log-Nachrichten	72
Tabelle 67: Testfälle für die Einbindungsschnittstelle – Ausgabe der Seriennummern	73
Tabelle 68: Testfälle für die Einbindungsschnittstelle – Ausgabe des aktuellen Stands des Signaturzählers	74
Tabelle 69: Testfälle für die Einbindungsschnittstelle – Wiedereinspielung von Backups von Log-Nachrichten	75
Tabelle 70: Testfälle für die Einbindungsschnittstelle – Ausgabe der zuletzt erzeugten Log-Nachricht.....	75
Tabelle 71: Testfälle für die Einbindungsschnittstelle – Registrieren von Aufzeichnungssystemen	76

Tabelle 72: Testfälle für die Einbindungsschnittstelle – Deregistrierung von Aufzeichnungssystemen.....	77
Tabelle 73: Testfälle für die Einbindungsschnittstelle – Starten einer Transaktion	78
Tabelle 74: Testfälle für die Einbindungsschnittstelle – Aktualisieren einer Transaktion	80
Tabelle 75: Testfälle für die Einbindungsschnittstelle – Beenden einer Transaktion	83
Tabelle 76: Testfälle für die Einbindungsschnittstelle – gefilterter Export von Transaktions-Log-Nachrichten	94
Tabelle 77: Testfälle für die Einbindungsschnittstelle – Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können	95
Tabelle 78: Testfälle für die Einbindungsschnittstelle – Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind	97
Tabelle 79: Testfälle für die Einbindungsschnittstelle – Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können.....	97
Tabelle 80: Testfälle für die Einbindungsschnittstelle – Abfrage zu registrierten Aufzeichnungssystemen	98
Tabelle 81: Testfälle für die Einbindungsschnittstelle – Ausgabe der Anzahl von offenen Transaktionen....	100
Tabelle 82: Testfälle für die Einbindungsschnittstelle – Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig verwaltet werden können.....	100
Tabelle 83: Testfälle für die Einbindungsschnittstelle – Ausgabe des Stadiums in welchem sich eine Transaktion befindet.....	101
Tabelle 84: Testfälle für die Einbindungsschnittstelle – Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.....	102
Tabelle 85: Testfälle für die Einbindungsschnittstelle – Ausgabe des aktuellen Stands des Transaktionszählers	102
Tabelle 86: Testfälle für die Einbindungsschnittstelle – Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht	104
Tabelle 87: Testfälle für die Einbindungsschnittstelle – Unterbindung der Aufzeichnung von Transaktionen	104
Tabelle 88: Testfälle zum Entsperrern von Log-Nachrichten von Transaktionen	105
Tabelle 89: Testfälle für die Einbindungsschnittstelle – Verwendung der Technischen Sicherheitseinrichtung durch mehrere Aufzeichnungssysteme	106
Tabelle 90: Testfälle für Allgemeine Fehlermeldungen von Funktionen	110
Tabelle 91: Auf Testfall II_ERR_01_Template anzuwendende Verfeinerungen.....	112
Tabelle 92: Auf Testfälle II_ERR_02_Template und II_ERR_03_Template anzuwendende Verfeinerungen..	113
Tabelle 93: Auf Testfall II_ERR_04_Template anzuwendende Verfeinerungen.....	113
Tabelle 94: Auf Testfall II_ERR_05_Template anzuwendende Verfeinerungen.....	115
Tabelle 95: Auf Testfall II_ERR_06_Template anzuwendende Verfeinerungen.....	115
Tabelle 96: Auf Testfall II_ERR_07_Template anzuwendende Verfeinerungen.....	117
Tabelle 97: Auf Testfälle II_ERR_08_Template, II_ERR_09_Template, II_ERR_11_Template, II_ERR_12_Template und II_ERR_13_Template anzuwendende Verfeinerungen.....	118
Tabelle 98: Auf Testfall II_ERR_10_Template anzuwendende Verfeinerungen.....	119
Tabelle 99: Auf Testfall II_ERR_14_Template anzuwendende Verfeinerungen.....	121
Tabelle 100: Auf Testfall II_ERR_15_Template anzuwendende Verfeinerungen	122
Tabelle 101: Auf Testfall II_ERR_16_Template anzuwendende Verfeinerungen	123
Tabelle 102 Auf Testfall II_ERR_17_Template anzuwendende Verfeinerungen.....	124
Tabelle 103: Testfälle für die Einbindungsschnittstelle – Unterstützung von herstellereigenspezifische Funktionalitäten der Einbindungsschnittstelle	124
Tabelle 104: Testfälle zu verwendeten Variante der Einbindungsschnittstelle.....	124
Tabelle 105: Prüfungen der Beschreibung der herstellereigenspezifische Funktionalitäten der Einbindungsschnittstelle	124

Tabelle 106: Auf Testfälle SDI_FUN_01_Template und SDI_ERR_01_Template anzuwendende Verfeinerungen	127
Tabelle 107: Prüfungen der Parameter der Standardschnittstelle.....	128
Tabelle 108: Prüfungen der Parameter der Standardschnittstelle.....	128
Tabelle 109: Auf Testfall SDI_PAR_01_Template anzuwendende Verfeinerungen.....	130
Tabelle 110: Prüfungen der Beschreibung der herstellereigene Funktionalitäten der Einbindungsschnittstelle	130
Tabelle 111: Prüfungen der Unterscheidbarkeit herstellereigene Funktionalitäten zur Einbindungsschnittstelle gemäß BSI TR-03151-1.....	131
Tabelle 112: Prüfungen der herstellereigene Funktionalitäten die Abwandlungen von Standardfunktionen sind.....	131
Tabelle 113: Prüfungen der Exportschnittstelle gemäß BSI TR-03153-1 – TAR-Format.....	131
Tabelle 114: Prüfungen der Exportschnittstelle gemäß BSI TR-03153-1 – Initialisierungsdaten.....	132
Tabelle 115: Prüfungen der Exportschnittstelle gemäß BSI TR-03153-1 – Log-Nachrichten.....	136
Tabelle 116: Auf Testfälle EXP_LOG_01_Template, EXP_LOG_02_Template, EXP_LOG_03_Template, EXP_LOG_04_Template und und EXP_LOG_26_Template anzuwendende Verfeinerungen.....	138
Tabelle 117: Prüfungen zur Herstellerdokumentation.....	140
Tabelle 118: Definition der Informationen für einen Testfall	142
Tabelle 119: Definition der Informationen für einen Testschritt.....	143

1 Einleitung

1.1 Motivation und Ziele

Die Technische Richtlinie [BSI TR-03153-1] definiert Anforderungen an Technische Sicherheitseinrichtungen für elektronische Aufzeichnungssysteme.

Diese Anforderungen müssen von Herstellern einer Technischen Sicherheitseinrichtung in den Produkten umgesetzt werden. Die vorliegende Testspezifikation zur [BSI TR-03153-1] definiert Anforderungen an Konformitätsprüfungen einer Technischen Sicherheitseinrichtung.

Anhand des Prüfungsergebnisses kann eine Aussage getroffen werden, ob das Verhalten und die Funktionalität einer Technischen Sicherheitseinrichtung konform zur [BSI TR-03153-1] sind.

Diese Prüfvorschriften ermöglichen eine einheitliche und konsistente Prüfung unterschiedlicher Implementierungen der Technischen Sicherheitseinrichtung durch verschiedene Prüfstellen mit vergleichbaren Prüfergebnissen.

Hinweis:

Es gelten weiterhin alle Anforderungen der Technischen Richtlinie [BSI TR-03153-1], welche von Herstellern erfüllt werden müssen, auch dann, falls es keinen zu der Anforderung gehörenden Testfall gibt.

1.2 Inhalt und Abgrenzung

Das vorliegende Dokument enthält verbindliche Anforderungen an die Prüfung von **Technischen Sicherheitseinrichtungen (TSE) für Aufzeichnungssysteme** gemäß [BSI TR-03153-1].

Anhand einer Konformitätsprüfung soll festgestellt werden, ob die bereitgestellte Funktionalität einer Technischen Sicherheitseinrichtung konform zu den entsprechenden Anforderungen in der Technischen Richtlinie [BSI TR-03153-1] und deren nachgelagerten Richtlinien und Anforderungen ist.

Diese Technische Richtlinie definiert in der Hauptsache Anforderungen für die folgenden Prüfungen:

- Prüfung der Funktionalität für die Sicherung von Anwendungsdaten und den vom Sicherheitsmodul erzeugten Protokolldaten.
- Prüfung der Exportfunktion für abgesicherte Daten.
- Prüfung der Einbindungsschnittstelle.
- Prüfung der Vollständigkeit der Funktionalität von herstellereigenen Einbindungsschnittstellen.

Bedingt durch weitere verbindliche Anforderungen der [BSI TR-03153-1] sind im Rahmen einer Zertifizierung/Konformitätsprüfung von Technischen Sicherheitseinrichtungen ergänzende formelle Prüfungen notwendig. Die hierzu zu erstellenden Herstellererklärungen werden auf Vollständigkeit und Plausibilität geprüft.

Folgenden Prüfaspekte werden von dieser Technischen Richtlinie beispielsweise nicht betrachtet:

- Prüfung der elektronischen Aufzeichnungssysteme (Registrierkassen, Taxameter, etc.),
- Prüfung der durch die Common Criteria-Zertifizierung abgedeckten Sicherheitseigenschaften der Technischen Sicherheitseinrichtung.

2 Generelle Anforderungen an die Durchführung von Prüfungen und den Prüfbericht

Anforderungen an die Prüfung und den Prüfbericht werden im Rahmen des Produktzertifizierungsprogramm für Technische Sicherheitseinrichtungen gemäß BSI TR-03153 sowie im Produktzertifizierungssystem festgelegt. Das Produktzertifizierungssystem sowie das zu TR-03153 gehörende Produktzertifizierungsprogramm werden auf der Webseite des BSI unter folgenden Link veröffentlicht:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-TR/Allgemeine-Informationen/allgemeine-informationen_node.html

3 Weitere Anforderungen an die Durchführung von Prüfungen von Technischen Sicherheitseinrichtungen

Die Einbindungsschnittelle dient zur Anbindung der Technischen Sicherheitseinrichtung an das elektronische Aufzeichnungssystem. Über die Einbindungsschnittstelle wird ein Großteil der Tests der Technischen Sicherheitseinrichtung durchgeführt. Die Validierung der Aufzeichnungen und Funktionalitäten findet größtenteils unter Verwendung von exportierten (abgesicherten) Daten an der Exportschnittstelle statt.

Die Einbindungsschnittstellen müssen den in der Technischen Richtlinie [BSI TR-03151-1] genannten Anforderungen genügen. Genaueres regelt die Technischen Richtlinie [BSI TR-03153-1].

Alle Implementierungen der Einbindungsschnittstellen, unabhängig davon ob sie herstellerspezifisch sind oder den Vorgaben der Technischen Richtlinie [BSI TR-03151-2] folgen, müssen vom Hersteller für die Prüfung bereitgestellt und erfolgreich überprüft werden. Genaueres regelt die Technischen Richtlinie [BSI TR-03153-1].

Eine manuelle Ablaufsteuerung an den Schnittstellen und eine Parameterveränderung müssen möglich sein. Zusätzlich muss der Hersteller die notwendigen Mittel für das Aufrufen der einzelnen Funktionalitäten der Einbindungsschnittstelle und das Empfangen der zurückgegebenen Werte zur Verfügung stellen.

3.1 Aufbau und Ablauf der praktischen Testdurchführung bei einer TSE

Die Abbildung 1 zeigt den allgemeinen Aufbau der Testdurchführung.

Hierbei repräsentiert die Abbildung 1 den allgemeinen Aufbau für eine Technische Sicherheitseinrichtung, die eine Einbindungsschnittstelle gemäß [BSI TR-03153-1] bereitstellt.

Im Rahmen dieser Technischen Richtlinie erfolgen konkreten Angaben zum Aufbau der Testdurchführung. Je nach Implementierung können Komponenten der TSE lokal oder fernverbunden implementiert sein.

Der Ablauf der praktischen Testdurchführung erfolgt meistens durch einen Aufruf von Funktionen über die Einbindungsschnittstelle sowie der Auswertung von Rückgabewerten und Ausgaben über die Exportschnittstelle.

Die Funktionsaufrufe begründen sich aus den Anforderungen der in diesem Dokument beschriebenen Testfälle. Hierzu notwendige Prüfschritte und weitere Details zu erwarteten Ergebnissen sind in den XML Beschreibungen der Testfälle (s. Kapitel 7.2) zu finden.

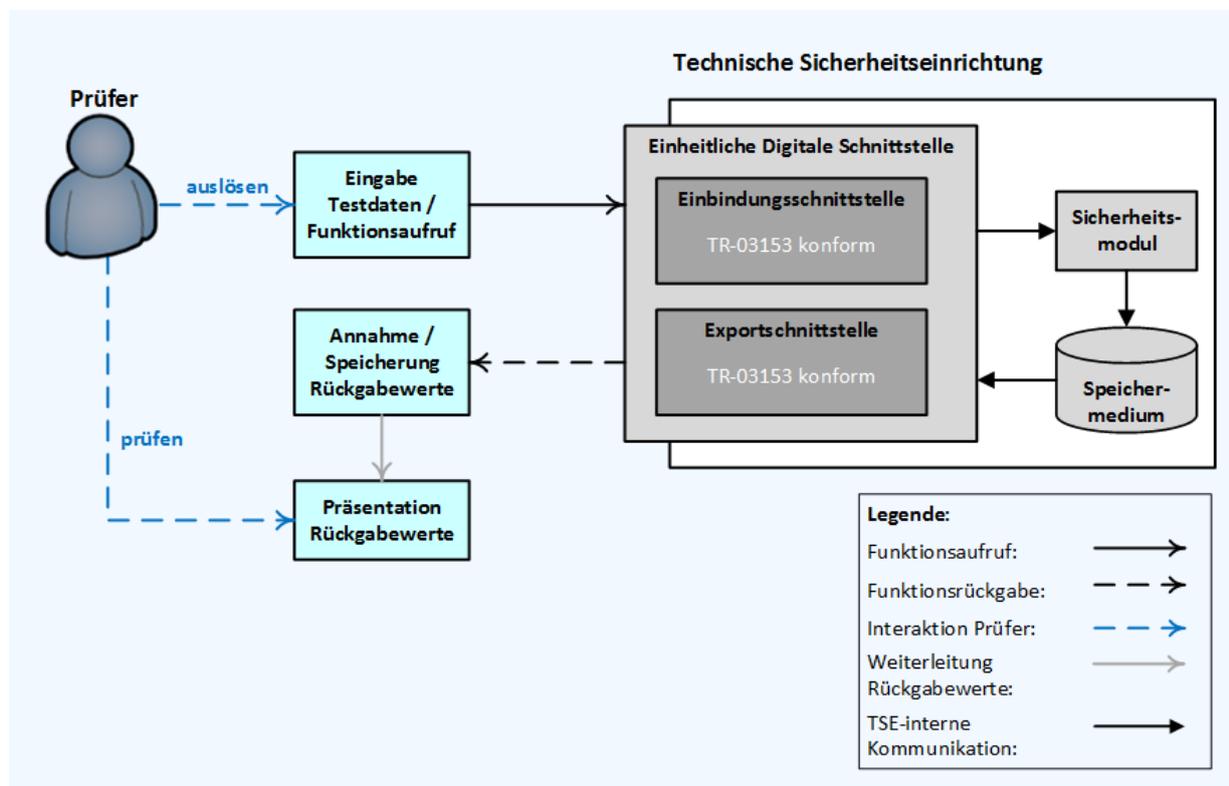


Abbildung 1: Testdurchführung für eine TSE mit Einbindungsschnittstelle nach [BSI TR-03153-1]

3.2 Beispiel einer Testdurchführung

Im Folgenden wird die allgemeine Ausführung von Konformitätstests für die erforderliche Einbindungsschnittstelle nach [BSI TR-03151-2] anhand eines Tests in Bezug auf die Funktionalität zum Starten einer Transaktion skizziert. Die entsprechende Funktionalität wird hierbei in Form der Funktion `startTransaction` bereitgestellt.

Die Abbildung 2 stellt beispielhaft die erste Phase des Tests für die Funktion `startTransaction` dar. Der Prüfer löst den Aufruf der Funktion `startTransaction` aus. Hierbei werden der Funktion die Seriennummer des Aufzeichnungssystems, die Daten des Vorgangs und die Art des Vorgangs über die entsprechenden Eingabeparameter der Funktion übergeben. Innerhalb der Technischen Sicherheitseinrichtung erfolgt nun die Absicherung der übergebenen Daten und der entsprechenden Protokolldaten, wobei die abgesicherten Daten im Speichermedium der Technischen Sicherheitseinrichtung gespeichert werden. Anschließend gibt die Funktion `startTransaction` die folgenden Werte als Rückgabeparameter zurück:

- Transaktionsnummer,
- Zeitpunkt der Protokollierung,
- Seriennummer der Technischen Sicherheitseinrichtung,
- Signaturzähler,
- Prüfwert (Signatur).

Anschließend kann der Prüfer die Korrektheit dieser Rückgabeparameter überprüfen.

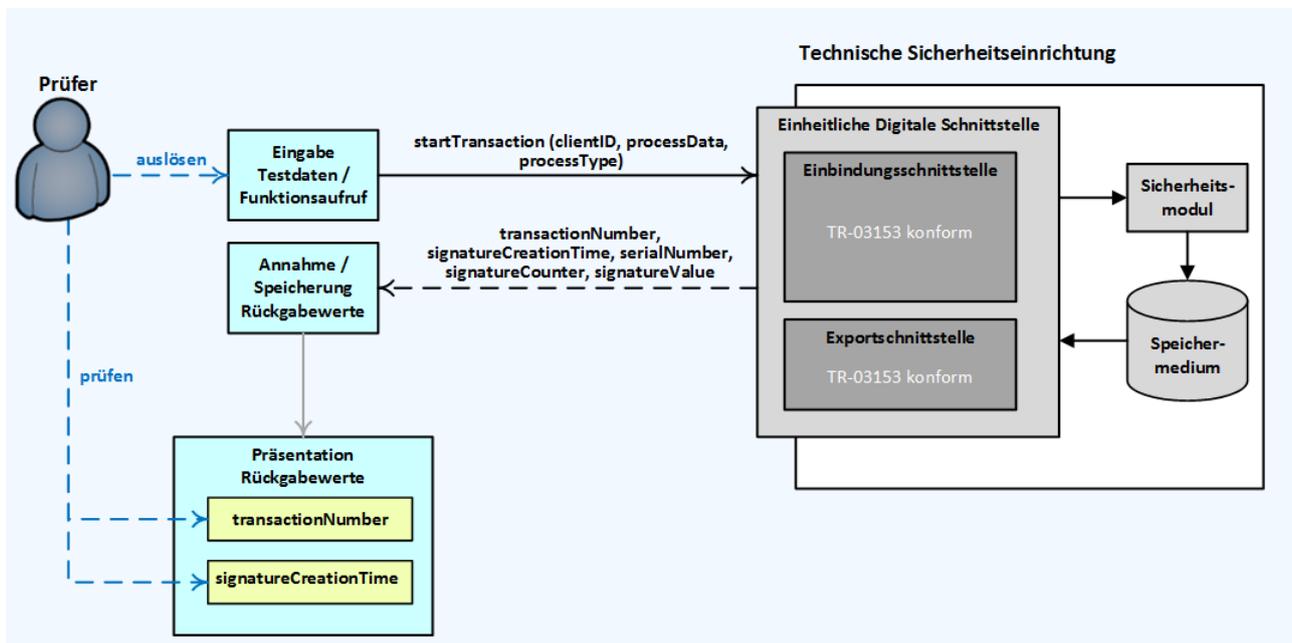


Abbildung 2: Erste Phase in Bezug auf das Testen der Funktion startTransaction

Die Abbildung 3 zeigt die zweite Phase des Tests, in der überprüft werden soll, ob die entsprechenden abgesicherten Daten im Rahmen der Ausführung der Funktion startTransaction korrekt gespeichert wurden. Hierzu löst der Prüfer den Aufruf der Funktion exportLogMessages der Einbindungsschnittstelle gemäß [BSI TR-03153-1] aus, um die entsprechenden abgesicherten Daten in Form einer Log-Nachricht über die Exportschnittstelle zu exportieren. Eine Ausprägung der Export-Funktion, exportFilteredTransactionLogs, ermöglicht den gezielten Export der Log-Nachrichten für einen bestimmten Vorgang anhand der betreffenden Transaktionsnummer. Die exportierten Daten werden von der Exportschnittstelle in dem vorgegebenen Format exportiert. Anschließend kann eine Prüfung erfolgen, ob

1. eine entsprechende Log-Nachricht exportiert wurde.
2. die folgenden Daten korrekt in der entsprechenden Log-Nachricht abgebildet werden:
 - Anwendungsdaten (Seriennummer des Aufzeichnungssystems, die Daten des Vorgangs und der Typ des Vorgangs), die beim Aufruf der Funktion startTransaction in Phase 1 des Tests (siehe Abbildung 2) übergeben wurden.
 - Protokolldaten (Transaktionsnummer, Zeitpunkt der Absicherung, Seriennummer der Technischen Sicherheitseinrichtung, Signaturzähler, Prüfwert), die im Rahmen der Ausführung der Funktion

startTransaction vom Sicherheitsmodul erzeugt und als Rückgabeparameter von startTransaction zurückgegeben wurden (siehe Abbildung 2).

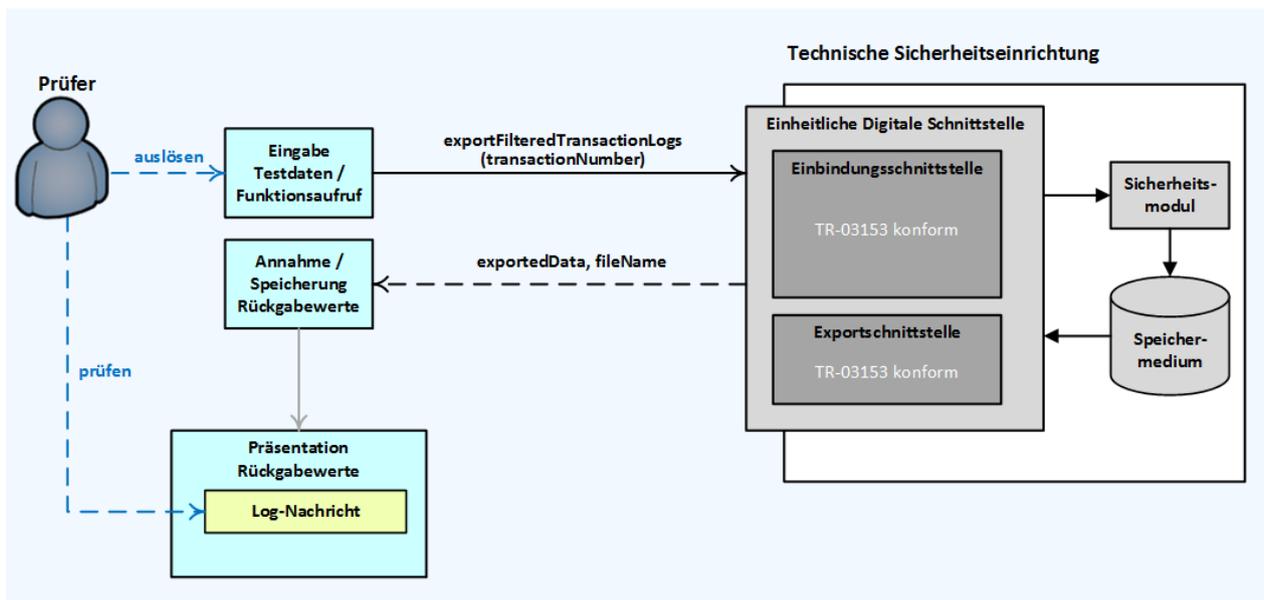


Abbildung 3: Zweite Phase in Bezug auf das Testen der Funktion startTransaction

4 Profile

Die Technische Sicherheitseinrichtung besteht aus den folgenden Komponenten:

- Speichermedium,
- Sicherheitsmodul,
- Exportschnittstelle,
- Einbindungsschnittstelle.

Die folgenden Profile dienen zur Auswahl von Testfällen bei unterschiedlichen Ausprägungen der Komponenten der Technischen Sicherheitseinrichtungen. Beispiel: Eine Technische Sicherheitseinrichtung kann über fernverbundene Komponenten des Sicherheitsmoduls verfügen. Somit gilt für diese TSE das Profil SM_REMOTE. Damit sind alle Tests mit dem Profil SM_REMOTE auszuwählen und zu bestehen.

Eine Kombination von mehreren Profilen führt zur Auswahl der Schnittmenge der beiden Profile.

Beispiel: Einem Testfall sind die Profile SM_MULTI und SM_NOAGG zugeordnet. Somit ist der Test nur zu bestehen, wenn es sich um ein Sicherheitsmodul handelt, welches mehrere parallele Transaktionen verwalten kann und keine Aggregation von Aktualisierungen vornimmt.

4.1 Speichermedium-Profile

Profil ID	Beschreibung
STORAGE_BASIC	Tests und formelle Prüfungen, die von allen Speichermedien von Technischen Sicherheitseinrichtungen erfüllt werden müssen.
STORAGE_REMOTE	Formelle Prüfungen, die sich ausschließlich auf fernverbundene Speichermedien beziehen.

Tabelle 1: Profil für das Speichermedium der Technischen Sicherheitseinrichtung

4.2 Sicherheitsmodul-Profile

Profil ID	Beschreibung
SM_BASIC	Tests und formelle Prüfungen, die von allen Sicherheitsmodulen von Technischen Sicherheitseinrichtungen erfüllt werden müssen.
SM_NOAGG	Tests für Sicherheitsmodule welche Aktualisierungen (Updates) immer direkt signieren und nicht aggregieren.
SM_AGG	Tests für Sicherheitsmodule, welche Aktualisierungen (Updates) aggregieren und zusammengefasst absichern (signieren) können.

Profil ID	Beschreibung
SM_INDEF	Tests für TSEn, welche Log-Nachrichten für aggregierte Aktualisierungen erzeugen kann, in denen indefinite length encoding verwendet wird.
SM_NO_INDEF	Tests für TSEn, welche keine Log-Nachrichten erzeugen kann, in denen indefinite length encoding verwendet wird.
SM_MULTI	Tests für Sicherheitsmodule, welche mehrere Transaktionen parallel verwalten können. ¹
SM_REMOTE	Tests für fernverbundene Sicherheitsmodule.
SM_REMOTE_COMPONENTS	Tests für Sicherheitsmodule mit fernverbundenen Komponenten.
CSP_ENTITY	Tests für TSEn deren CSP-Einheiten zu einem sicherheits-einrichtungübergreifenden CSP zusammengefasst werden.
CSP_CLUSTER	Tests für TSEn deren Krypto-Kern als Cluster betrieben wird.
CSP_LIGHT	Tests für TSEn die einen CSP-Light als Krypto-Kern verwenden.
SMAADMIN_AVAILABLE	Test, wenn ein Administrator an der Sicherheitsmodulanwendung angemeldet werden kann.

Tabelle 2: Profile für das Sicherheitsmodul

4.3 Schnittstellen-Profile

Profil ID	Beschreibung
II	Tests für alle Einbindungsschnittstellen. Die Tests umfassen alle Funktionen und Eigenschaften der Einbindungsschnittstelle gemäß [BSI TR-03153-1] und [BSI TR-03151-1].
SDI	Tests für Implementierungen der Einbindungsschnittstelle nach [BSI TR-03151-2].
AUDIT_MODIFY	Tests, wenn die Einstellungen der Audit-Funktionalität der Sicherheitsmodulanwendung nach der initialen Einstellung verändert werden können.

¹ Die maximale Anzahl der parallelen Transaktionen ist auf dem ICS zu nennen.

Profil ID	Beschreibung
MULTI_CLIENT	Tests für Technische Sicherheitseinrichtungen, die eine gleichzeitige Protokollierung von Transaktionen durch mehrere Aufzeichnungssysteme ermöglichen.
NO_MULTI_CLIENT	Tests für Technische Sicherheitseinrichtungen, die nur eine Protokollierung von Transaktionen durch ein Aufzeichnungssystem ermöglichen.
LIMITED_CLIENTS_TRACKED	Tests, wenn die TSE eine begrenzte Anzahl an Aufzeichnungssystemen unterstützt und die aktuelle Anzahl der Aufzeichnungssysteme nachgehalten wird.
UNLIMITED_CLIENTS_NOT_TRACKED	Tests, wenn die TSE eine unbegrenzte Anzahl an Aufzeichnungssystemen unterstützt aber die aktuelle Anzahl der Aufzeichnungssysteme nicht nachgehalten wird.

Tabelle 3: Profile der Einbindungsschnittstelle gemäß [BSI TR-03153-1]

Profil ID	Beschreibung
ADDITIONAL_FUNCTIONALITIES	Tests, wenn die Einbindungsschnittstelle Funktionalitäten bereitstellt, die nicht in der [BSI TR-03153-1] beschrieben sind.
NO_ADDITIONAL_FUNCTIONALITIES	Tests, wenn die Einbindungsschnittstelle keine Funktionalitäten bereitstellt, die nicht in der [BSI TR-03153-1] beschrieben sind.

Tabelle 4: Profil für herstellerspezifische Funktionalitäten der Einbindungsschnittstelle

Name der optionalen Funktion	Profil ID wenn die Funktion unterstützt wird	Profil ID wenn die Funktion nicht unterstützt wird
updateDevice	II_UPDATEDEVICE	II_NO_UPDATEDEVICE
getTotalMemory	II_TOTALMEMORY	II_NO_TOTALMEMORY
getUsedMemory	II_USEDMEMORY	II_NO_USEDMEMORY
getFreeMemory	II_FREEMEMORY	II_NO_FREEMEMORY
getDeviceHealth	II_DEVICEHEALTH	II_NO_DEVICEHEALTH
getComponentVersions	II_GETVERSIONS	II_NO_GETVERSIONS
getEndOfUsageDate	II_ENDOFUSAGEDATE	II_NO_ENDOFUSAGEDATE
updateTime	II_UPDATETIME	II_NO_UPDATETIME

Name der optionalen Funktion	Profil ID wenn die Funktion unterstützt wird	Profil ID wenn die Funktion nicht unterstützt wird
getCurrentSeTime	II_CURRENTTIME	II_NO_CURRENTTIME
configureLogging	II_CONFIGLOGGING	II_NO_CONFIGLOGGING
deleteLogMessages	II_DELETELOGS	II_NO_DELETELOGS
restoreLogsFromBackup	II_RESTOREBACKUP	II_NO_RESTOREBACKUP
exportFilteredTransactionLogs	II_EXPORTFILTERED	II_NO_EXPORTFILTERED
getCurrentNumberOfClients	II_CURNOClients	II_NO_CURNOClients
getMaxNumberOfClients	II_MAXNOClients	II_NO_MAXNOClients
getRegisteredClients	II_REGISTEREDClients	II_NO_REGISTEREDClients
getCurrentNumberOfTransactions	II_CURNOTRANSACTIONS	II_NO_CURNOTRANSACTIONS
getMaxNumberOfTransactions	II_MAXNOTRANSACTIONS	II_NO_MAXNOTRANSACTIONS
getTransactionState	II_TRANSACTIONSTATE	II_NO_TRANSACTIONSTATE
getOpenTransactions	II_OPENTRANSACTIONS	II_NO_OPENTRANSACTIONS
getLastTransactionLogMessage	II_LASTTRANSLOG	II_NO_LASTTRANSLOG
lockTransactionLogging	II_LOCKTRANSLOGGING	II_NO_LOCKTRANSLOGGING
unlockTransactionLogging	II_UNLOCKTRANSLOGGING	II_NO_UNLOCKTRANSLOGGING

Tabelle 5: Profile für optionale Funktionen

4.4 Allgemeine Profile

Profil ID	Beschreibung
TIME_SYNC	Tests für Technische Sicherheitseinrichtungen, die über einen Mechanismus, zum eigenständigen Stellen der Zeit des Sicherheitsmoduls (ohne Übergabe eines Zeitwerts), verfügen.
NO_TIME_SYNC	Tests für Technische Sicherheitseinrichtungen, die über keinen Mechanismus, zum eigenständigen Stellen der Zeit des Sicherheitsmoduls (ohne Übergabe eines Zeitwerts), verfügen.
CENTRAL_TIME	Tests, wenn die Zeit zentral im fernverbundenen Sicherheitsmodul eingestellt wird.
NO_CENTRAL_TIME	Tests, wenn die Zeit nicht zentral im fernverbundenen Sicherheitsmodul eingestellt wird.

Profil ID	Beschreibung
DESCRIPTION_SET	Tests, wenn bei der Produktion eine Beschreibung eingebracht wurde.
DESCRIPTION_NOT_SET	Tests, wenn bei der Produktion keine Beschreibung eingebracht wurde.
RECERT	Tests, wenn eine neue Version einer bereits zertifizierten TSE geprüft wird und die Beibehaltung der bereits verwendeten Signaturschlüssel geplant ist .
INTERIM_PKI_RULING	Test, wenn die TSE bereits nach Version 1.0.1 der [BSI TR-03153 1.0.1] zertifiziert wurde, wobei das PKI-Konzept mit dem BSI abgestimmt wurde und eine PKI verwendet wird, die über eine Zertifizierung nach Teil 1 der [BSI TR-03145] verfügt.
NO_INTERIM_PKI_RULING	Test, wenn die TSE nicht bereits nach Version 1.0.1 der [BSI TR-03153 1.0.1] zertifiziert wurde, wobei das PKI-Konzept mit dem BSI abgestimmt wurde und keine PKI verwendet wird, die über eine Zertifizierung nach Teil 1 der [BSI TR-03145] verfügt.
DIRECTORY_SERVICES	Tests, wenn ein Verzeichnisdienst implementiert ist, über den die Zertifikate der TSE abgerufen werden können.
UPDATE_EXTERNAL	Tests, wenn die TSE durch ein externes Programm aktualisiert werden kann.
UPDATE_EXTERNAL_LOGGED	Tests, wenn eine Log-Nachricht für den Start einer Aktualisierung erstellt wird, wenn die Aktualisierung nicht über die Einbindungsschnittstelle ausgelöst wurde.
UPDATE_EXTERNAL_NOT_LOGGED	Tests, wenn keine Log-Nachricht für den Start einer Aktualisierung erstellt wird, wenn die Aktualisierung nicht über die Einbindungsschnittstelle ausgelöst wurde.
EXPORTTOOL	Tests, wenn für den Export der abgesicherten Daten, in Form des TAR-Containers, ohne Hilfe des Aufzeichnungssystems, zusätzliche Hilfstools benötigt werden.
NO_EXPORTTOOL	Tests, wenn für den Export der abgesicherten Daten, in Form des TAR-Containers, ohne Hilfe des Aufzeichnungssystems, keine zusätzlichen Hilfstools benötigt werden.
PUK_BLOCKABLE	Tests, wenn als Gegenmaßnahmen gegen Angriffe in Bezug auf das Erraten der PUK dieser zeitweise gesperrt wird.

Tabelle 6: Profile zu allgemeinen Eigenschaften einer TSE

5 Implementation Conformance Statement

Ein Implementation Conformance Statement (ICS) enthält die für die Durchführung der Konformitätsprüfung benötigten Informationen zur Technischen Sicherheitseinrichtung.

In diesem ICS gibt der Antragsteller an, zu welchen Teilen der Testspezifikation der Technischen Richtlinie die betreffende Technische Sicherheitseinrichtung konform sein soll. Darunter fällt auch die Angabe der unterstützten Kryptographie und die Auswahl von den in Kapitel 3 definierten Profilen.

5.1 Herstellererklärung

In der folgenden Auflistung gibt der Antragsteller für die Zertifizierung an, welche Eigenschaften die zu prüfende Technische Sicherheitseinrichtung hat.

Gegenstand	Daraus folgende Profile
<input checked="" type="checkbox"/> Die TSE verfügt über ein Speichermedium.	STORAGE_BASIC
<input type="checkbox"/> Die TSE hat ein fernverbundenes Speichermedium.	STORAGE_REMOTE
<input checked="" type="checkbox"/> Die TSE verfügt über ein Sicherheitsmodul.	SM_BASIC
<input type="checkbox"/> Die TSE hat ein fernverbundenes Sicherheitsmodul	SM_REMOTE
<input type="checkbox"/> Die TSE hat ein Sicherheitsmodul mit fernverbundenen Komponenten.	SM_REMOTE_COMPONENTS
<input type="checkbox"/> CSP-Einheiten der TSE werden mit anderen logischen Einheiten zu einem sicherheitseinrichtungsübergreifenden CSP zusammengefasst.	CSP_ENTITY
<input type="checkbox"/> Die TSE enthält einen Krypto-Kern der als Cluster betrieben wird.	CSP_CLUSTER
<input type="checkbox"/> Die TSE verwendet einen CSP-Light als Krypto-Kern.	CSP_LIGHT
<input type="checkbox"/> Es ist ein Verzeichnisdienst implementiert, über den die Zertifikate der TSE abgerufen werden können.	DIRECTORY_SERVICES
<input type="checkbox"/> Die TSE signiert Aktualisierungen (Updates) direkt und aggregiert diese nicht.	SM_NOAGG
UND/ODER	
<input type="checkbox"/> aggregiert Aktualisierungen (Updates) und sichert diese zusammengefasst ab (signiert).	SM_AGG

Gegenstand		Daraus folgende Profile
<input type="checkbox"/>	Die TSE kann Log-Nachrichten für aggregierte Aktualisierungen erzeugen, in denen indefinite length encoding verwendet wird. ODER	SM_INDEF
<input type="checkbox"/>	Die TSE kann keine Log-Nachrichten erzeugen in denen indefinite length encoding verwendet wird.	SM_NO_INDEF
<input type="checkbox"/>	Die TSE kann mehrere Transaktionen parallel verwalten.	SM_MULTI
<input type="checkbox"/>	Es kann ein Administrator an der Sicherheitsmodulanwendung angemeldet werden.	SMAADMIN_AVAILABLE
<input checked="" type="checkbox"/>	Alle Schnittstellen der TSE implementieren alle verpflichtenden Funktionen und Eigenschaften gemäß [BSI TR-03153-1] und [BSI TR-03151-1] UND	II
<input checked="" type="checkbox"/>	die TSE implementiert mindestens eine Schnittstelle gemäß [BSI TR-03151-2] UND	SDI
<input type="checkbox"/>	die Schnittstellen implementieren neben den Funktionen der Einheitlichen Digitalen Schnittstelle gemäß der [BSI TR-03153-1] keine weitere Funktionen ODER	NO_ADDITIONAL_FUNCTIONALITIES
<input type="checkbox"/>	die Schnittstellen implementieren neben den Funktionen der Einheitlichen Digitalen Schnittstelle gemäß der [BSI TR-03153-1] weitere Funktionen.	ADDITIONAL_FUNCTIONALITIES
<input type="checkbox"/>	Die TSE verfügt über einen Mechanismus, zum eigenständigen Stellen der Zeit des Sicherheitsmoduls. ODER	TIME_SYNC
<input type="checkbox"/>	verfügt über keinen Mechanismus, zum eigenständigen Stellen der Zeit des Sicherheitsmoduls.	NO_TIME_SYNC

Gegenstand		Daraus folgende Profile
<input type="checkbox"/>	Die TSE wurde bereits nach [BSI TR-03153 1.0.1] zertifiziert, wobei das PKI-Konzept mit dem BSI abgestimmt wurde und eine PKI verwendet wurde, die über eine Zertifizierung nach Teil 1 der [BSI TR-03145] verfügt.	INTERIM_PKI_RULING
	ODER	
<input type="checkbox"/>	wurde nicht nach [BSI TR-03153 1.0.1] zertifiziert oder verwendet eine PKI die nicht über eine Zertifizierung nach Teil 1 der [BSI TR-03145] verfügt.	NO_INTERIM_PKI_RULING
<input type="checkbox"/>	Die TSE kann über eine andere Schnittstelle als die Einheitliche Digitale Schnittstelle gemäß der [BSI TR-03153-1] aktualisiert werden.	UPDATE_EXTERNAL
<input type="checkbox"/>	Bei einer Aktualisierung wird die Log-Nachricht zum Start des Updates erzeugt.	UPDATE_EXTERNAL_LOGGED
<input type="checkbox"/>	Bei einer Aktualisierung wird die Log-Nachricht zum Start des Updates nicht erzeugt.	UPDATE_EXTERNAL_NOT_LOGGED
<input type="checkbox"/>	Für den Export der abgesicherten Daten, in Form des TAR-Containers, ohne Hilfe des Aufzeichnungssystems, werden zusätzliche Hilfstools benötigt	EXPORTTOOL
	ODER	
<input type="checkbox"/>	für den Export der abgesicherten Daten, in Form des TAR-Containers, ohne Hilfe des Aufzeichnungssystems, werden keine zusätzlichen Hilfstools benötigt.	NO_EXPORTTOOL
<input type="checkbox"/>	Als Gegenmaßnahmen gegen Angriffe in Bezug auf das Erraten der PUK wird dieser zeitweise gesperrt.	PUK_BLOCKABLE

Tabelle 7: ICS - Profile der Eigenschaften der Technischen Sicherheitseinrichtung

	Gegenstand	Daraus folgende Profile
<input type="checkbox"/>	Die TSE unterstützt die Funktion updateDevice ODER	II_UPDATEDEVICE
<input type="checkbox"/>	unterstützt die Funktion updateDevice nicht.	II_NO_UPDATEDEVICE
<input type="checkbox"/>	Die TSE unterstützt die Funktion getTotalMemory ODER	II_TOTALMEMORY

	Gegenstand	Daraus folgende Profile
<input type="checkbox"/>	unterstützt die Funktion getTotalMemory nicht.	II_NO_TOTALMEMORY
<input type="checkbox"/>	Die TSE unterstützt die Funktion getUsedMemory ODER	II_USEDMEMORY
<input type="checkbox"/>	unterstützt die Funktion getUsedMemory nicht.	II_NO_USEDMEMORY
<input type="checkbox"/>	Die TSE unterstützt die Funktion getFreeMemory ODER	II_FREEMEMORY
<input type="checkbox"/>	unterstützt die Funktion getFreeMemory nicht.	II_NO_FREEMEMORY
<input type="checkbox"/>	Die TSE unterstützt die Funktion getDeviceHealth ODER	II_DEVICEHEALTH
<input type="checkbox"/>	unterstützt die Funktion getDeviceHealth nicht.	II_NO_DEVICEHEALTH
<input type="checkbox"/>	Die TSE unterstützt die Funktion GetComponentVersions ODER	II_GETVERSIONS
<input type="checkbox"/>	unterstützt die Funktion GetComponentVersions nicht.	II_NO_GETVERSIONS
<input type="checkbox"/>	Die TSE unterstützt die Funktion getEndOfUsageDate ODER	II_ENDOFUSAGEDATE
<input type="checkbox"/>	unterstützt die Funktion getEndOfUsageDate nicht.	II_NO_ENDOFUSAGEDATE
<input type="checkbox"/>	Die TSE unterstützt die Funktion updateTime ODER	II_UPDATETIME
<input type="checkbox"/>	unterstützt die Funktion updateTime nicht.	II_NO_UPDATETIME
<input type="checkbox"/>	Die TSE unterstützt die Funktion getCurrentSeTime ODER	II_CURRENTTIME
<input type="checkbox"/>	unterstützt die Funktion getCurrentSeTime nicht.	II_NO_CURRENTTIME
<input type="checkbox"/>	Die TSE unterstützt die Funktion configureLogging ODER	II_CONFIGLOGGING
<input type="checkbox"/>	unterstützt die Funktion configureLogging nicht.	II_NO_CONFIGLOGGING
<input type="checkbox"/>	Die TSE unterstützt die Funktion deleteLogMessages ODER	II_DELETELOGS
<input type="checkbox"/>	unterstützt die Funktion deleteLogMessages nicht.	II_NO_DELETELOGS
<input type="checkbox"/>	Die TSE unterstützt die Funktion restoreLogsFromBackup ODER	II_RESTOREBACKUP
<input type="checkbox"/>	unterstützt die Funktion restoreLogsFromBackup nicht.	II_NO_RESTOREBACKUP
<input type="checkbox"/>	Die TSE unterstützt die Funktion exportFilteredTransactionLogs ODER	II_EXPORTFILTERED
<input type="checkbox"/>	unterstützt die Funktion exportFilteredTransactionLogs nicht.	II_NO_EXPORTFILTERED
<input type="checkbox"/>	Die TSE unterstützt die Funktion getCurrentNumberOfClients ODER	II_CURNOClients
<input type="checkbox"/>	unterstützt die Funktion getCurrentNumberOfClients nicht.	II_NO_CURNOClients
<input type="checkbox"/>	Die TSE unterstützt die Funktion getMaxNumberOfClients ODER	II_MAXNOClients
<input type="checkbox"/>	unterstützt die Funktion getMaxNumberOfClients nicht.	II_NO_MAXNOClients

	Gegenstand	Daraus folgende Profile
<input type="checkbox"/>	Die TSE unterstützt die Funktion getRegisteredClients ODER	II_REGISTEREDCLIENTS
<input type="checkbox"/>	unterstützt die Funktion getRegisteredClients nicht.	II_NO_REGISTEREDCLIENTS
<input type="checkbox"/>	Die TSE unterstützt die Funktion getCurrentNumberOfTransactions ODER	II_CURNOTRANSACTIONS
<input type="checkbox"/>	unterstützt die Funktion getCurrentNumberOfTransactions nicht.	II_NO_CURNOTRANSAC-TIONS
<input type="checkbox"/>	Die TSE unterstützt die Funktion getMaxNumberOfTransactions ODER	II_MAXNOTRANSACTIONS
<input type="checkbox"/>	unterstützt die Funktion getMaxNumberOfTransactions nicht.	II_NO_MAXNOTRANSAC-TIONS
<input type="checkbox"/>	Die TSE unterstützt die Funktion getTransactionState ODER	II_TRANSACTIONSTATE
<input type="checkbox"/>	unterstützt die Funktion getTransactionState nicht.	II_NO_TRANSACTIONSTATE
<input type="checkbox"/>	Die TSE unterstützt die Funktion getOpenTransactions ODER	II_OPENTRANSACTIONS
<input type="checkbox"/>	unterstützt die Funktion getOpenTransactions nicht.	II_NO_OPENTRANSAC-TIONS
<input type="checkbox"/>	Die TSE unterstützt die Funktion getLastTransactionLogMessage ODER	II_LASTTRANSLOG
<input type="checkbox"/>	unterstützt die Funktion getLastTransactionLogMessage nicht.	II_NO_LASTTRANSLOG
<input type="checkbox"/>	Die TSE unterstützt die Funktion lockTransactionLogging ODER	II_LOCKTRANSLOGGING
<input type="checkbox"/>	unterstützt die Funktion lockTransactionLogging nicht.	II_NO_LOCKTRANSLOG-GING
<input type="checkbox"/>	Die TSE unterstützt die Funktion unlockTransactionLogging ODER	II_UNLOCKTRANSLOGGING
<input type="checkbox"/>	unterstützt die Funktion unlockTransactionLogging nicht.	II_NO_UNLOCKTRANSLOG-GING

Tabelle 8: ICS - Profile der verfügbaren Funktionen der Technischen Sicherheitseinrichtung

In Tabelle 9 macht der Antragssteller Angaben zu kryptographischen Algorithmen, die vom Sicherheitsmodul der Technischen Sicherheitseinrichtung bei Absicherungsschritten verwendet werden.

Verwendete Kryptofunktionen	Angaben des Antragstellers
Signaturverfahren	
Signaturformat	
Hashfunktion	

Verwendete Kryptofunktionen	Angaben des Antragstellers
Länge des Hashwertes	
EC-Domain-Parameter	
Klasse des Zufallszahlengenerators	

Tabelle 9: Angaben zu verwendeten Kryptofunktionen für die Absicherungsschritte der TSE

In Tabelle 10 macht der Antragssteller Angaben zu verwendeten kryptographischen Algorithmen, der eingesetzten Public-Key-Infrastruktur (PKI) zur Erzeugung der Signatur von Zertifikaten

Verwendete Kryptofunktionen	Angaben des Antragstellers
Signaturverfahren	
Signaturformate	
Hashfunktionen	
Länge der Hashwerte	
EC-Domain-Parameter	

Tabelle 10: Angaben zu verwendeten Kryptofunktionen der PKI

Zusätzliche Angaben:

Gegenstand	Angaben des Antragstellers
Größe des für das Speichern von Log-Nachrichten nutzbaren Speichers	
Anzahl der Transaktions-Log-Nachrichten, die erwartet gespeichert werden können.	
Methode zur Schätzung der Anzahl der Transaktions-Log-Nachrichten, die erwartet gespeichert werden können.	Details in gesonderter Dokumentation. Namen und Version (und ggf. Kapitel) der Dokumentation:
Maximale Anzahl an Lösch-/Schreibzyklen des für Transaktionen nutzbaren Speichers	
Maximale Größe des Transaktionszählers	
Maximale Anzahl an Lösch-/Schreibzyklen des Transaktionszählers	
Maximale Größe des Signaturzählers	

Gegenstand	Angaben des Antragstellers
Maximale Anzahl an Lösch-/Schreibzyklen des Signaturzählers	

Tabelle 11: Zusätzliche Angaben zu den Komponenten der Technischen Sicherheitseinrichtung

Gegenstand	Angaben des Antragstellers
Welches Zeitformat wird in Lognachrichten verwendet (genau eins)?	<input type="checkbox"/> UTC Time <input type="checkbox"/> Generalized Time <input type="checkbox"/> Unix Time
Welches Zeitformat kann als Input für die Funktion updateTime verwendet werden, falls diese implementiert ist und die TSE über keinen Mechanismus zum eigenständigen Stellen der Zeit des Sicherheitsmoduls verfügt (mindestens 1)?	<input type="checkbox"/> UTC Time <input type="checkbox"/> Generalized Time <input type="checkbox"/> Unix Time
Welcher ist der früheste von der Zeitführung der TSE verarbeitbare Zeitpunkt?	
Welcher ist der späteste von der Zeitführung der TSE verarbeitbare Zeitpunkt?	

Tabelle 12: Zusätzliche Angaben zum verwendeten Zeitformat

Gegenstand	Angaben des Antragstellers
Maximale Anzahl von Aufzeichnungssystemen, die die TSE gleichzeitig zur Absicherung von Transaktionen nutzen können.	

Tabelle 13: Zusätzliche Angaben zu der Anzahl von gleichzeitigen Aufzeichnungssystemen der TSE

Gegenstand	Angaben des Antragstellers
Maximale Anzahl der parallel geöffneten Transaktionen, die das Sicherheitsmodul verwalten kann.	

Tabelle 14: Zusätzliche Angaben zu der maximalen Anzahl von parallel geöffneten Transaktionen

Gegenstand	Angaben des Antragstellers
Maximale Anzahl der Technische Sicherheitseinrichtungen, die mit einem Krypto-Kern verbunden sein können, ohne dass mit Performanceeinbußen gerechnet werden muss.	

Tabelle 15: Zusätzliche Angaben zu der maximalen Anzahl von parallel genutzten Technische Sicherheitseinrichtungen

In der nachfolgenden Tabelle macht der Antragssteller weitere Angaben zur TSE. Dort wird auch angezeigt, ob detaillierte Angaben in einer gesonderten Dokumentation zu erfolgen haben.

Gegenstand	Angaben des Antragstellers
Benennen Sie Hersteller, Modell, Version und Zertifizierungs-ID(s) der gesamten TSE	
Benennen Sie Hersteller, Modell und Version des Speichermediums	
Benennen Sie Hersteller, Modell und Version der Einbindungsschnittstelle	
Benennen Sie Hersteller, Modell, Version und Zertifizierungs-ID(s) des Krypto-Kerns (CSP)	
Benennen Sie Hersteller, Modell, Version und Zertifizierungs-ID(s) der Sicherheitsmodulanwendung (SMAERS)	

Gegenstand	Angaben des Antragstellers
Beschreiben Sie welche Längen für Inputs bei den Funktionen authenticateUser, unblockPin, setDescription, updateDevice, restoreLogsFromBackup, registerClient, deregisterClient, startTransaction, updateTransaction, finishTransaction, exportFilteredTransactionLogs unterstützt werden. Listen Sie hier Namen und Version (und ggf. Kapitel) dieser Übersicht.	Details in gesonderter Dokumentation. Namen und Version (und ggf. Kapitel) der Dokumentation:
Beschreiben Sie, wie der Fehler ErrorParameterSyntax für jede Funktion provoziert werden kann. Sollte der Fehler nicht provoziert werden können, erläutern Sie warum dies nicht möglich ist. Listen Sie hier Namen und Version (und ggf. Kapitel) dieser Beschreibung.	Details in gesonderter Dokumentation. Namen und Version (und ggf. Kapitel) der Dokumentation:
Reichen Sie eine Übersicht ein welche Funktion welche Fehlermeldungen in welchen Situationen werfen kann. Listen Sie hier Namen und Version (und ggf. Kapitel) dieser Übersicht.	Details in gesonderter Dokumentation Namen und Version (und ggf. Kapitel) der Dokumentation:
Verwendet die TSE neben dem Verfahren zur Berechnung von Prüfwerten, weitere kryptographische Verfahren?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Bei der Verwendung weiterer kryptographischer Verfahren TSE neben der Berechnung von Prüfwerten werden die allgemeinen Empfehlungen der [BSI TR-02102] eingehalten?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Können in den exportierten TAR-Containern noch andere als von der BSI TR-03153-1 definierte Dateien enthalten sein?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein
Die TSE unterstützt die folgenden Funktionen:	Details in gesonderter Dokumentation. Namen und Version (und ggf. Kapitel) der Dokumentation:
Die TSE verfügt über die folgenden Nutzer:	<input type="checkbox"/> unauthenticated <input type="checkbox"/> logger <input type="checkbox"/> admin <input type="checkbox"/> timeadmin

Gegenstand	Angaben des Antragstellers
Die TSE verfügt über mindestens einen weiteren Nutzer - wenn ja, welche?:	<input type="checkbox"/> Nein <input type="checkbox"/> Ja Details in gesonderter Dokumentation. Namen und Version (und ggf. Kapitel) der Dokumentation:
Wie lauten die Passwörter/PINs für die verschiedenen Rollen?	Details in gesonderter Dokumentation. Namen und Version (und ggf. Kapitel) der Dokumentation:
In welcher Komponente wird der PIN Fehlbedienungszähler geführt?	
Auf welchen Wert wird der PIN Fehlbedienungszähler gesetzt, wenn eine Authentifizierung erfolgreich war?	
In welcher Komponente werden für die verschiedenen Nutzer PIN und PUK gespeichert?	
Welche Gegenmaßnahmen gegen Angriffe in Bezug auf das Erraten der PUK sind implementiert?	Details in gesonderter Dokumentation. Namen und Version (und ggf. Kapitel) der Dokumentation:
Unter welchen Bedingungen wird eine Transaktion als verwaist angesehen?	Details in gesonderter Dokumentation Namen und Version (und ggf. Kapitel) der Dokumentation:
Beschreiben Sie, in welchen Fällen die TSE indefinite length encoding und welchen nicht verwendet und wie diese Zustände durch die Prüfstelle provoziert werden können.	Details in gesonderter Dokumentation Namen und Version (und ggf. Kapitel) der Dokumentation:

Gegenstand	Angaben des Antragstellers
restoreLogsFromBackup: Woran werden Logs anderer TSEn erkannt?	Details in gesonderter Dokumentation Namen und Version (und ggf. Kapitel) der Dokumentation:
Beschreiben Sie, welche Audit Logs von der TSE erzeugt werden. Diese Übersicht muss die genaue Spezifikation (ASN.1-Definition) der Logs enthalten.	Details in gesonderter Dokumentation Namen und Version (und ggf. Kapitel) der Dokumentation:
Beschreiben Sie, wie sichergestellt wird, dass die TSE nach einer Aktualisierung von einzelnen Komponenten nur in zertifizierter Form verwendet wird.	Details in gesonderter Dokumentation. Namen und Version (und ggf. Kapitel) der Dokumentation:

Tabelle 16: Weitere Angaben zur TSE

5.2 Versicherung zu gemachten Angaben

Der Antragsteller versichert, dass die gemachten Angaben vollständig und wahr sind.

Der Antragsteller versichert zusätzlich, dass die TSE

- keine Funktionalität bereitstellt um zukünftige, aktuelle oder abgeschlossene Aufzeichnungen zu manipulieren oder eine ordnungsgemäße Verarbeitung zu verhindern,
- und dass das eingereichte Testobjekt funktionell dem finalen Stand entspricht und höchstens ein anderer Formfaktor gewählt wurde.

Datum / Name / Unterschrift Antragsteller

5.3 Zustimmung zur Veröffentlichung der Beschränkungen

Der Antragsteller stimmt der Veröffentlichung aller Beschränkungen, insbesondere der Angaben im ICS, der Technischen Sicherheitseinrichtung durch das BSI und das Bundesministerium der Finanzen zu.

Datum / Name / Unterschrift Antragsteller

6 Module

Innerhalb dieser Technischen Richtlinie erfolgt eine Gruppierung von Testfällen durch Module. Hierbei gruppiert ein Modul Testfälle für eine Komponente der Technischen Sicherheitseinrichtung. Die einzelnen Module sind bei Bedarf durch weitere Untermodule strukturiert.

Diese Technische Richtlinie definiert die folgenden Module:

Modul	Komponente
Storage	Speichermedium
Security Module	Sicherheitsmodul
Export	Exportschnittstelle
Integration Interface	Einbindungsschnittstelle

Testfälle können Positivtests (PT) oder Negativtests (NT) repräsentieren.

Herstellereklärungen erfordern eine formale Prüfung (FP) der Plausibilität.

In den folgenden Unterkapiteln erfolgen Kurzbeschreibungen der Testfälle einzelner Module.

6.1 Modul Storage – Speichermedium (STO)

Das Speichermedium der Technischen Sicherheitseinrichtung kann verschieden ausgeprägt/konfiguriert sein. Es kann sich um ein

- lokales Speichermedium oder
- fernverbundenes Speichermedium handeln.

Beide Ausprägungen durchlaufen grundlegende Basisprüfungen. Bei einem fernverbundenen Speichermedium wird ergänzend die spezifikationskonforme Verwendung eines abgesicherten Kanals für die Kommunikation geprüft.

6.1.1 Funktionale Prüfungen von Speichermedien (STO_FUN)

ID	Zielsetzung	Profile	Typ
STO_FUN_01	Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet Absicherungsschritte einer Transaktion mit den Phasen: <ul style="list-style-type: none"> • Start der Transaktion • einmalige Aktualisierung einer Transaktion • Beenden der Transaktion 	SM_AGG	PT
STO_FUN_02	Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet Absicherungsschritte einer Transaktion mit den Phasen: <ul style="list-style-type: none"> • Start der Transaktion • einmalige Aktualisierung einer Transaktion mit Absicherungsschritt • Beenden der Transaktion 	SM_NOAGG	PT

ID	Zielsetzung	Profile	Typ
STO_FUN_03	<p>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet Absicherungsschritte einer Transaktion mit den Phasen:</p> <ul style="list-style-type: none"> • Start der Transaktion • mehrere Aktualisierungen der Transaktion • Beenden der Transaktion 	SM_AGG	PT
STO_FUN_04	<p>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet Absicherungsschritte einer Transaktion mit den Phasen:</p> <ul style="list-style-type: none"> • Start der Transaktion • mehrere Aktualisierungen der Transaktion mit Absicherungsschritt • Beenden der Transaktion 	SM_NOAGG	PT
STO_FUN_05	<p>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet Absicherungsschritte für mehrere parallele Transaktionen mit den zeitlich versetzten Phasen:</p> <ul style="list-style-type: none"> • Start der Transaktion • mehrere Aktualisierungen der Transaktion • Beenden der Transaktion 	SM_AGG SM_MULTI	PT
STO_FUN_06	<p>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet Absicherungsschritte für mehrere parallele Transaktionen mit den zeitlich versetzten Phasen:</p> <ul style="list-style-type: none"> • Start der Transaktion • mehrere Aktualisierungen der Transaktion mit Absicherungsschritt • Beenden der Transaktion 	SM_NOAGG SM_MULTI	PT
STO_FUN_07	<p>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet einen Absicherungsschritt nach einer Aktualisierung der Zeitführung innerhalb des Sicherheitsmoduls.</p>	STORAGE_BASIC	PT
STO_FUN_08	<p>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet Absicherungsschritte, nach mehreren Aktualisierungen der Zeitführung im Sicherheitsmodul, während einer Transaktion.</p>	STORAGE_BASIC II_UPDATETIME	PT
STO_FUN_09	<p>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet den Absicherungsschritt für die Initialisierung der Technischen Sicherheitseinrichtung.</p>	STORAGE_BASIC	PT
STO_FUN_10	<p>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet den Absicherungsschritt für die Außerbetriebnahme des Sicherheitsmoduls.</p>	STORAGE_BASIC	PT

ID	Zielsetzung	Profile	Typ
STO_FUN_11	Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet den Absicherungsschritt für Audit-Daten , die vom Sicherheitsmodul erzeugt wurden.	STORAGE_BASIC	PT

Tabelle 17: Testfälle zur Funktionalität des Speichermediums

6.1.2 Prüfungen der Speicherkapazität von Speichermedien (STO_CAP)

ID	Zielsetzung	Profile	Typ
STO_CAP_01	Prüfen der Speicherkapazität des Speichermediums. Die Prüfung erfolgt auf Grundlage von Herstellerdokumenten.	STORAGE_BASIC	FP

Tabelle 18: Prüfungen der Speicherkapazität von Speichermedien

6.1.3 Prüfungen der Zuverlässigkeit von Speichermedien (STO_REL)

ID	Zielsetzung	Profile	Typ
STO_REL_01	Prüfen der Zuverlässigkeit des Speichermediums. Die Prüfung erfolgt auf Grundlage von Herstellerdokumenten.	STORAGE_BASIC	FP

Tabelle 19: Prüfungen der Zuverlässigkeit von Speichermedien

6.1.4 Prüfungen für fernverbundene Speichermedien (STO_REM)

Bei der Verwendung eines fernverbundenen Speichermediums sind zusätzlich nachfolgend aufgelistete Prüfungen erforderlich.:

ID	Zielsetzung	Profile	Typ
STO_REM_01	Prüfung, ob die Kommunikation zwischen der Einbindungsschnittstelle und dem fernverbundenen Speichermedium über einen abgesicherten Kanal (Secure Channel) stattfindet. Die Prüfung erfolgt auf Grundlage einer Herstellerdokumentation.	STORAGE_REMOTE	FP

Tabelle 20: Prüfungen für fernverbundene Speichermedien

6.2 Modul Security Module – Sicherheitsmodul (SM)

Dieses Modul enthält Prüfungen des Sicherheitsmoduls der Technischen Sicherheitseinrichtung.

6.2.1 Prüfung zu der genutzten Architektur des Sicherheitsmoduls (SM_ARCH)

Die folgenden zusätzlichen Prüfungen MÜSSEN von der Prüfstelle durchgeführt werden:

ID	Zielsetzung	Profile	Typ
SM_ARCH_01	Prüfung, ob die Technische Sicherheitseinrichtung genau einen eindeutigen Signaturschlüssel besitzt, welcher im Sicherheitsmodul gespeichert ist.	SM_BASIC	PT
SM_ARCH_02	Prüfung, ob jede Technische Sicherheitseinrichtung genau ein Sicherheitsmodul enthält.	SM_BASIC	FP
SM_ARCH_03	Prüfung, ob das Sicherheitsmodul jeder Technischen Sicherheitseinrichtung aus genau einer Sicherheitsmodulanwendung und genau einem Krypto-Kern besteht.	SM_BASIC	FP
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_BASIC	FP
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_BASIC	FP
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_BASIC	FP
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_BASIC	FP
SM_ARCH_08	Prüfung, ob ein Aufzeichnungssystem immer nur genau einer TSE zugeordnet wird, wenn die CSP-Einheit der TSE mit anderen logischen Einheiten zu einem sicherheitseinrichtungsübergreifenden CSP zusammengefasst wird.	CSP_ENTITY	PT
SM_ARCH_09	Prüfung, ob zeitnah aufgezeichnet wird, wenn die maximale Anzahl an Technische Sicherheitseinrichtungen mit dem (sicherheitseinrichtungsübergreifenden) CSP verbunden ist und jede dieser TSE mit der maximalen Anzahl an Aufzeichnungssystemen und Transaktionen parallel angesprochen wird.	SM_BASIC	PT

ID	Zielsetzung	Profile	Typ
SM_ARCH_10	Prüfung, ob bei Verwendung eines CSP-Light im gesicherten Rechenzentrum ein CSP-Light-Cluster verwendet wird.	CSP_LIGHT	FP
SM_ARCH_11	Prüfung, ob zu jeder Zeit genau eine CSP-Einheit im Cluster als Master den Signaturschlüssel aktiv verwendet und ob die anderen CSP-Einheiten den Signaturzähler des jeweiligen Masters für den Signaturschlüssel synchronisieren.	CSP_CLUSTER	FP

Tabelle 21: Prüfung zu der genutzten Architektur des Sicherheitsmoduls

6.2.2 Prüfungen zur Konkatenation und Signaturerstellung (SM_CON)

Die folgenden Testfälle prüfen die Konkatenation und Signaturerstellung. Bei den Prüfungen für die Protokollierung von Transaktionen werden **bei allen Testfällen Anwendungsdaten bei Beginn und Ende der Transaktion übergeben**.

ID	Zielsetzung	Profile	Typ
SM_CON_01	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • eine Transaktion • eine Aktualisierung • Aktualisierung erzeugt Absicherung 	SM_NOAGG	PT
SM_CON_02	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • eine Transaktion • eine Aktualisierung • ohne Absicherung 	SM_AGG	PT
SM_CON_03	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • eine Transaktion • mehrere Aktualisierungen • Aktualisierung erzeugt Absicherung 	SM_NOAGG	PT

ID	Zielsetzung	Profile	Typ
SM_CON_04	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • eine Transaktion • mehrere Aktualisierungen • ohne Absicherung 	SM_AGG	PT
SM_CON_05	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • eine Transaktion • mehrere Aktualisierungen • Aktualisierung bis eine Absicherung erfolgt 	SM_AGG	PT
SM_CON_06	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • mehrere Transaktionen parallel, versetzt • eine Aktualisierung pro Transaktion • Aktualisierung erzeugt Absicherung 	SM_NOAGG SM_MULTI	PT
SM_CON_07	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • mehrere Transaktionen parallel, versetzt • eine Aktualisierung pro Transaktion • ohne Absicherung 	SM_AGG SM_MULTI	PT
SM_CON_08	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • mehrere Transaktionen parallel, versetzt • mehrere Aktualisierungen pro Transaktion • Aktualisierung erzeugt Absicherung 	SM_NOAGG SM_MULTI	PT

ID	Zielsetzung	Profile	Typ
SM_CON09	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • mehrere Transaktionen parallel, versetzt • mehrere Aktualisierungen pro Transaktion • ohne Absicherung 	SM_AGG SM_MULTI	PT
SM_CON_10	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden.</p> <p>Der Test betrachtet jeweils die folgende Situation:</p> <ul style="list-style-type: none"> • mehrere Transaktionen parallel, versetzt • mehrere Aktualisierungen pro Transaktion • Aktualisierung bis eine Absicherung erfolgt 	SM_AGG SM_MULTI	PT
SM_CON_11	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden, wenn zwischen den verschiedenen Phasen zur Absicherung von Transaktionen vereinzelte Aktualisierungen der Zeit innerhalb des Sicherheitsmoduls stattfinden.</p> <p>Es werden die Absicherungen von mehreren parallelen Transaktionen betrachtet, wobei die Aktualisierungen der Transaktionen ohne Absicherungsschritte erfolgen.</p>	SM_MULTI SM_AGG	PT
SM_CON_12	<p>Prüfung, ob die Protokolldaten korrekt erstellt und die zu signierenden Elemente der Log-Nachricht korrekt konkateniert werden, wenn zwischen den verschiedenen Phasen zur Absicherung von Transaktionen vereinzelte Aktualisierungen der Zeit innerhalb des Sicherheitsmoduls stattfinden.</p> <p>Es werden die Absicherungen von mehreren parallelen Transaktionen betrachtet, wobei die Aktualisierungen der Transaktionen mit Absicherungsschritten erfolgen.</p>	SM_MULTI SM_NOAGG	PT

Tabelle 22: Testfälle zur Konkatenation und Signaturerstellung

6.2.3 Prüfungen zur Zeitführung im Sicherheitsmodul (SM_TME)

ID	Zielsetzung	Profile	Typ
SM_TME_01	Prüfung, ob bei einem Aufruf der Zeitaktualisierungsfunktion die Zeit im Sicherheitsmodul aktualisiert wird.	SM_BASIC	PT
SM_TME_02	Prüfung, ob das Sicherheitsmodul den Signaturzähler bei mehreren Aktualisierungen der Zeit im Sicherheitsmodul fortlaufend inkrementiert.	SM_BASIC	PT
SM_TME_03	Prüfung, ob das Sicherheitsmodul bei einer Aktualisierung der internen Zeit mit einem fehlerhaften Zeitwert <ul style="list-style-type: none"> • eine gültige Fehlermeldung auslöst und • den Wert für die interne Zeit nicht aktualisiert Das Format des neuen Zeitwerts ist nicht korrekt.	SM_BASIC NO_TIME_SYNC	NT
SM_TME_04	Prüfung, ob die vom Sicherheitsmodul bereitgestellte Zeit fortlaufend ist. Der Test betrachtet jeweils die folgenden Aktionen für mehrere parallele Transaktionen: <ul style="list-style-type: none"> • Starten der Transaktion • mehrere Aktualisierungen der Transaktion • Beenden der Transaktion Die Aktionen werden versetzt durchgeführt.	SM_MULTI SM_AGG	PT
SM_TME_05	Prüfung, ob die vom Sicherheitsmodul bereitgestellte Zeit fortlaufend ist. Der Test betrachtet jeweils die folgenden Aktionen für mehrere parallele Transaktionen: <ul style="list-style-type: none"> • Starten der Transaktion • mehrere Aktualisierungen der Transaktion mit Absicherungsschritt • Beenden der Transaktion Die Aktionen werden versetzt durchgeführt.	SM_MULTI SM_NOAGG	PT
SM_TME_06	Prüfung, ob die vom Sicherheitsmodul bereitgestellte Zeit fortlaufend ist. Der Test betrachtet jeweils die folgenden Aktionen: <ul style="list-style-type: none"> • Initialisierung der Technischen Sicherheitseinrichtung • mehrmalige Aktualisierung der Zeit innerhalb des Sicherheitsmoduls • Protokollierung einer Transaktion, mit einer Aktualisierung mit Absicherungsschritt • Absicherung von Audit-Daten, die vom Sicherheitsmodul erzeugt wurden Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung	SM_NOAGG	PT

ID	Zielsetzung	Profile	Typ
SM_TME_07	<p>Prüfung, ob die vom Sicherheitsmodul bereitgestellte Zeit fortlaufend ist.</p> <p>Der Test betrachtet jeweils die folgenden Aktionen:</p> <ul style="list-style-type: none"> • Initialisierung der Technischen Sicherheitseinrichtung • mehrmalige Aktualisierung der Zeit innerhalb des Sicherheitsmoduls • Protokollierung einer Transaktion, mit einer Aktualisierung ohne Absicherungsschritt • Absicherung von Audit-Daten, die vom Sicherheitsmodul erzeugt wurden <p>Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung</p>	SM_AGG	PT
SM_TME_08_Template	<p>Prüfung, ob die vom Sicherheitsmodul bereitgestellte Zeit fortlaufend ist.</p> <p>Der Test betrachtet jeweils die folgenden Aktionen:</p> <ul style="list-style-type: none"> • erfolgreiche Entsperrung der PIN-Eingabe für einen autorisierten Nutzer • erfolgreiche Authentifizierung eines autorisierten Nutzers • erfolgreiche Abmeldung eines authentifizierten Nutzers <p>Es werden die Nutzer aus Tabelle 24 getestet.</p>	Siehe Tabelle 24	PT
SM_TME_09	<p>Prüfung, ob als Reaktion auf jedes Stellen der Zeitführung einer CSP-Einheit bzw. des CSPs unmittelbar korrekte System-Log-Nachrichten des Typs updateTime nach [BSI TR-03151-1]erstellt werden und diese mit den jeweiligen privaten Schlüsseln der Technischen Sicherheitseinrichtungen signiert und durch diese gespeichert werden.</p>	SM_BASIC CENTRAL_TIME	PT
SM_TME_10	<p>Prüfung, ob die interne Zeit im Sicherheitsmodul nach einer Phase der Stromlosigkeit der Technischen Sicherheitseinrichtung, bei der eine korrekt laufende Zeitführung nicht aufrechterhalten werden konnte, mit einem definierten Wert neu startet, welcher eine „Nicht-Stellung“ der Uhrzeit eindeutig erkennbar macht.</p>	SM_BASIC NO_CENTRAL_TIME	PT
SM_TME_11	<p>Prüfung, ob in allen Aufzeichnungen und Logs, die im Rahmen der Konformitätsprüfung erstellt wurden, nicht mehr als eines der zulässigen Zeitformate verwendet.</p>	SM_BASIC	PT

ID	Zielsetzung	Profile	Typ
SM_TME_12	Prüfung, ob die Zeitführung im Krypto-Kern des Sicherheitsmoduls erfolgt.	SM_BASIC	FP

Tabelle 23: Testfälle zur Zeitführung im Sicherheitsmodul

ID Suffix	Zu verwendende Nutzer	Profile
_A	Ein Nutzer mit der Rolle logger.	SM_BASIC
_B	Ein Nutzer mit der Rolle admin.	SM_BASIC
_C	Ein Nutzer mit der Rolle timeadmin.	II_UPDATETIME

Tabelle 24: Auf Testfälle SM_TME_08_Template, SM_SIG_08_Template anzuwendende Verfeinerungen

6.2.4 Prüfungen zum Signaturzähler im Sicherheitsmodul (SM_SIG)

ID	Zielsetzung	Profile	Typ
SM_SIG_01	Prüfung, ob das Sicherheitsmodul einen fortlaufenden Signaturzähler bereitstellt, für <ul style="list-style-type: none"> • sequentielle Transaktionen • mit mehreren Aktualisierungen • mit Absicherungsschritten 	SM_NOAGG	PT
SM_SIG_02	Prüfung, ob das Sicherheitsmodul einen fortlaufenden Signaturzähler bereitstellt, für <ul style="list-style-type: none"> • sequentielle Transaktionen • mit mehreren Aktualisierungen • ohne Absicherungsschritte 	SM_AGG	PT
SM_SIG_03	Prüfung, ob das Sicherheitsmodul einen fortlaufenden Signaturzähler bereitstellt, für <ul style="list-style-type: none"> • mehrere parallele Transaktionen • mit mehreren Aktualisierungen • mit Absicherungsschritten 	SM_NOAGG SM_MULTI	PT
SM_SIG_04	Prüfung, ob das Sicherheitsmodul einen fortlaufenden Signaturzähler bereitstellt, für <ul style="list-style-type: none"> • mehrere parallele Transaktionen • mit mehreren Aktualisierungen • ohne Absicherungsschritte 	SM_AGG SM_MULTI	PT
SM_SIG_05	Prüfung, ob das Sicherheitsmodul einen Überlauf des Signaturzählers verhindert und mit Ausgabe eines Fehlers weitere Signaturerstellungen blockiert.	SM_BASIC	PT

ID	Zielsetzung	Profile	Typ
SM_SIG_06	<p>Prüfung, ob das Sicherheitsmodul einen fortlaufenden Signaturzähler bereitstellt, für die</p> <ul style="list-style-type: none"> • Initialisierung der Technischen Sicherheitseinrichtung • mehrmalige Aktualisierung der Zeit innerhalb des Sicherheitsmoduls • Protokollierung einer Transaktion, mit einmaliger Aktualisierung mit Absicherungsschritt • Absicherung von Audit-Daten, die vom Sicherheitsmodul erzeugt wurden • Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung 	SM_NOAGG	PT
SM_SIG_07	<p>Prüfung, ob das Sicherheitsmodul einen fortlaufenden Signaturzähler bereitstellt, für die</p> <ul style="list-style-type: none"> • Initialisierung der Technischen Sicherheitseinrichtung • mehrmalige Aktualisierung der Zeit innerhalb des Sicherheitsmoduls • Protokollierung einer Transaktion, mit einmaliger Aktualisierung ohne Absicherungsschritt • Absicherung von Audit-Daten, die vom Sicherheitsmodul erzeugt wurden • Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung 	SM_AGG	PT
SM_SIG_08_Template	<p>Prüfung, ob das Sicherheitsmodul einen fortlaufenden Signaturzähler bereitstellt, für die</p> <ul style="list-style-type: none"> • erfolgreiche Entsperrung der PIN-Eingabe für einen autorisierten Nutzer • erfolgreiche Authentifizierung eines autorisierten Nutzers • erfolgreiche Abmeldung eines authentifizierten Nutzers <p>Es werden die Nutzer aus Tabelle 24 getestet.</p>	Siehe Tabelle 24	PT

Tabelle 25: Testfälle für Signaturzähler

6.2.5 Prüfungen zur Transaktionsnummer im Sicherheitsmodul (SM_TRA)

ID	Zielsetzung	Profile	Typ
SM_TRA_01	<p>Prüfung, ob die Transaktionsnummern fortlaufend und lückenlos sind.</p> <p>Alle Transaktionen verlaufen nacheinander.</p>	SM_BASIC	PT

ID	Zielsetzung	Profile	Typ
SM_TRA_02	Prüfung, ob die Transaktionsnummern fortlaufend und lückenlos sind. Die Transaktionen starten nacheinander und ohne Beendigung der Transaktionen, bis die maximale Anzahl von offenen Transaktionen (siehe ICS) erreicht ist.	SM_MULTI	PT
SM_TRA_03	Prüfung, ob eine Fehlermeldung ausgelöst wird, beim Start einer neuen Transaktion, wenn die maximale Anzahl von parallelen Transaktionen bereits erreicht ist.	SM_BASIC	NT
SM_TRA_04	Prüfung, ob eine Fehlermeldung ausgelöst wird, bei Aktualisierung einer Transaktion mit einer Transaktionsnummer für die keine Transaktion gestartet wurde.	SM_BASIC	NT
SM_TRA_05	Prüfung, ob eine Fehlermeldung ausgelöst wird, bei Aktualisierung einer Transaktion mit einer Transaktionsnummer, deren zugehörige Transaktion bereits beendet wurde.	SM_BASIC	NT
SM_TRA_06	Prüfung, ob eine Fehlermeldung ausgelöst wird, bei Beenden einer Transaktion mit einer Transaktionsnummer, deren zugehörige Transaktion bereits beendet wurde.	SM_BASIC	NT
SM_TRA_07	Prüfung, ob ein Überlauf der Transaktionsnummer nicht möglich ist und das Sicherheitsmodul mit einer Fehlerausgabe weitere Anfragen blockiert.	SM_BASIC	PT

Tabelle 26: Testfälle zur Transaktionsnummer im Sicherheitsmodul

6.2.6 Prüfungen zur Kryptographieanwendung im Sicherheitsmodul (SM_KRY)

Prüfungen, ob das Sicherheitsmodul die Vorgaben der [BSI TR-03116-5] erfüllt.

ID	Zielsetzung	Profile	Typ
SM_KRY_01	Prüfung, ob die kryptographischen Angaben aus der Herstellererklärung und dem ICS den Vorgaben der [BSI TR-03116-5] entsprechen bzgl.: <ul style="list-style-type: none"> • Signaturverfahren, • Signaturformat, • Verwendung elliptischer Kurven, • Schlüssellänge • Hashfunktion, • Hashwertlänge, • EC-Domainparameter, • Klasse des Zufallzahlengenerators. 	SM_BASIC	FP
SM_KRY_02	Prüfung des Signaturverfahrens der Aufzeichnung durch externe Verifizierung der Signatur mit dem angegebenen Signaturverfahren.	SM_BASIC	PT
SM_KRY_03	Prüfung der Seriennummer der TSE durch externe Hashwertbildung über den öffentlichen Schlüssel dessen zugehöriger private Schlüssel für die Absicherung von Transaktions-Log-Nachrichten verwendet wird.	SM_BASIC	PT

Tabelle 27: Testfälle der Kryptographieanwendung des Sicherheitsmoduls

6.2.7 Prüfungen der Public-Key-Infrastruktur von Sicherheitsmodulen (SM_PKI)

ID	Zielsetzung	Profile	Typ
SM_PKI_01	Prüfung, ob die Zertifikate der gesamten Zertifikatskette (einschließlich des Vertrauensankers) der TSE von einer Public Key Infrastruktur ausgestellt werden, welche über eine gültige Zertifizierung nach Teil 5 der Technischen Richtlinie [BSI TR-03145] verfügt.	NO_INTE-RIM_PKI_RULING	PT
SM_PKI_02	Prüfung, ob die verwendeten Zertifikate aus dem Sicherheitsmodul den Vorgaben der [BSI TR-03116-5] entsprechen bzgl.: <ul style="list-style-type: none"> • Signaturverfahren, • Verwendung elliptischer Kurven, • Schlüssellänge, • Hashfunktion, • Hashwertlänge, • EC-Domainparameter. 	SM_BASIC	FP
SM_PKI_03	Prüfung der Zertifikate durch externe Verifizierung bzgl.: <ul style="list-style-type: none"> • Aussteller (Issuer) ist korrekt, • Zertifikatskette bis zur Root-CA ist korrekt, • Gültigkeit (Validity) ist plausibel, • Zertifikat ist nicht zurückgezogen (Revocation List), • Signaturverfahren korrekt, • Signatur valide. 	SM_BASIC	PT
SM_PKI_04	Prüfung, ob der Hersteller eine schlüssige Anleitung bereitstellt, wie über den Verzeichnisdienst Zertifikate von Technischen Sicherheitseinrichtungen gesucht und heruntergeladen werden können.	DIRECTORY_SERVICES	FP
SM_PKI_05	Prüfung, ob der Hersteller eine korrekte Anleitung bereitstellt, wie über den Verzeichnisdienst Zertifikaten von Technischen Sicherheitseinrichtungen gesucht und heruntergeladen werden können. Insbesondere wird geprüft, ob Technischen Sicherheitseinrichtungen über ihre Seriennummern gesucht werden können.	DIRECTORY_SERVICES	PT
SM_PKI_06	Prüfung, ob die Anforderung und Empfehlungen im Rahmen der PKI-Übergangsregelung an den Verzeichnisdienst eingehalten werden.	INTERIM_PKI_RULING	FP
SM_PKI_07	Prüfung, ob die Voraussetzungen für die Inanspruchnahme der PKI-Übergangsregelung vorliegen.	INTERIM_PKI_RULING	FP

Tabelle 28: Testfälle der Public-Key-Infrastruktur von Sicherheitsmodulen

6.2.8 Prüfungen für fernverbundene Sicherheitsmodule (SM_REM)

Dieses Modul enthält Prüfungen für fernverbundene Sicherheitsmodule.

ID	Zielsetzung	Profile	Typ
SM_REM_01	Prüfung, ob die Kommunikation zwischen der jeweiligen Einbindungsschnittstelle und dem Sicherheitsmodul über einen abgesicherten Kanal (Secure Channel) erfolgt.	SM_REMOTE	FP

Tabelle 29: Testfälle für fernverbundene Sicherheitsmodule

6.2.9 Prüfungen für die Sicherheitsmodulanwendung (SM_LOG)

Dieses Modul enthält Prüfungen für die Sicherheitsmodulanwendung.

ID	Zielsetzung	Profile	Typ
SM_LOG_01	Prüfung, ob die Datenfelder/Elemente role, authentication-Result und remainingRetries korrekt in der Log-Nachricht befüllt sind, wenn eine (produktspezifische) Anmeldung des Administrators der Sicherheitsmodulanwendung (smaadmin) an der Sicherheitsmodulanwendung (SMAERS) erfolgreich ist.	SMAADMIN_AVAILABLE	PT
SM_LOG_02	Prüfung, ob die Datenfelder/Elemente role, authentication-Result und remainingRetries korrekt in der Log-Nachricht befüllt sind, wenn eine (produktspezifische) Anmeldung des Administrators der Sicherheitsmodulanwendung (smaadmin) an der Sicherheitsmodulanwendung (SMAERS) fehlschlägt .	SMAADMIN_AVAILABLE	NT
SM_LOG_03	Prüfung, ob die Log-Nachricht, die erstellt wird, wenn die Sicherheitsmodulanwendung die Audit-Funktionalität startet, als eventData eine leere ASN.1-Sequenz enthält.	SM_BASIC	PT
SM_LOG_04	Prüfung, ob die Log-Nachricht, die erstellt wird, wenn die Sicherheitsmodulanwendung beim Vorherrschen von Fehlern in einen sicheren Zustand eintritt, die korrekte Zeit enthält, wenn diese Log-Nachricht nicht beim Auftreten des Events erstellt wird.	SM_BASIC	PT
SM_LOG_05	Prüfung, ob die Log-Nachricht, die erstellt wird, wenn die Sicherheitsmodulanwendung beim Vorherrschen von Fehlern in einen sicheren Zustand eintritt, die korrekte Zeit enthält, wenn diese Log-Nachricht beim Auftreten des Events erstellt wird.	SM_BASIC	PT
SM_LOG_06	Prüfung, ob die Log-Nachricht, die erstellt wird, wenn der sichere Zustand verlassen wird, als eventData eine leere ASN.1-Sequenz enthält.	SM_BASIC	PT

Tabelle 30: Testfälle für die Sicherheitsmodulanwendung

6.2.10 Deaktivierung des Sicherheitsmoduls (SM_AUD)

ID	Zielsetzung	Profile	Typ
SM_AUD_01	Prüfung, ob das Sicherheitsmodul deaktiviert wird, wenn die Einstellungen der Audit-Funktionalität der Sicherheitsmodulanwendung nach der initialen Einstellung verändert werden.	AUDIT_MODIFY	PT
SM_AUD_02	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.	SM_BASIC	PT

Tabelle 31: Testfälle zur Deaktivierung des Sicherheitsmoduls

6.3 Modul Integration Interface – Einbindungsschnittstelle

Alle Einbindungsschnittstellen müssen alle verpflichtenden Funktionen der Einheitlichen Digitalen Schnittstelle gemäß der [BSI TR-03153-1] mit allen in der [BSI TR-03151-1] definierten Schnittstelleneigenschaften unterstützen. Daher müssen für alle Implementierungen der Einbindungsschnittstelle die nachfolgenden Basisprüfungen zum Profil „II“ durchgeführt werden (s. Kapitel 6.3.1)

Die Einbindungsschnittstelle muss in mindestens einer Implementierung der Einbindungsschnittstelle nach [BSI TR-03151-2] vorliegen. Für diese Schnittstellen müssen zusätzlich die Prüfungen zum Profil „SDI“ durchgeführt werden (s. Kapitel 6.3.2).

Die Einbindungsschnittstelle kann zusätzlich, sofern konform zu den Vorgaben der [BSI TR-03151-1], als von der [BSI TR-03151-2] abweichende Implementierung vorliegen.

Die Einbindungsschnittstelle kann zusätzlich weitere Funktionalitäten bereitstellen, die nicht in der [BSI TR-03151-1] beschrieben sind. In diesem Fall sind zusätzliche Prüfungen zum Profil „ADDITIONAL_FUNCTIONALITIES“ erforderlich (s. Kapitel 6.3.3).

6.3.1 Basisprüfungen der Einbindungsschnittstelle (II)

Dieses Modul enthält Basisprüfungen für alle Einbindungsschnittstellen. Alle Tests sind über die Einheitliche Digitale Schnittstelle oder die entsprechende Funktionalität der herstellereigenen Schnittstelle aufzurufen.

6.3.1.1 Authentifizierung von Nutzern der Technischen Sicherheitseinrichtung (II_AUT)

ID	Zielsetzung	Profile	Typ
II_AUT_01_Template	Prüfung, ob die Authentifizierung eines Nutzers erfolgreich ist, wenn beim Aufruf der Funktion <ul style="list-style-type: none"> eine gültige User-ID und eine korrekte zugehörige PIN übergeben werden. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird. Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	PT

ID	Zielsetzung	Profile	Typ
II_AUT_02	Prüfung, ob die Authentifizierung eines Nutzers fehlschlägt, wenn beim Aufruf der Funktion eine ungültige User-ID übergeben wird.	II	NT
II_AUT_03_Template	Prüfung, ob die Authentifizierung eines Nutzers fehlschlägt, wenn beim Aufruf der Funktion <ul style="list-style-type: none"> • eine gültige User-ID und • eine ungültige PIN übergeben werden. Vor dem Funktionsaufruf ist der Wert des Fehlbedienungszählers für die PIN-Eingabe größer 1 . Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	NT
II_AUT_04_Template	Prüfung, ob die Authentifizierung eines Nutzers fehlschlägt, wenn beim Aufruf der Funktion <ul style="list-style-type: none"> • eine gültige User-ID und • eine ungültige PIN übergeben werden. Vor dem Funktionsaufruf hat der Fehlbedienungszähler für die PIN-Eingabe den Wert 1 . Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	NT
II_AUT_05_Template	Prüfung, ob die Authentifizierung eines Nutzers fehlschlägt, wenn die PIN-Eingabe zu einer User-ID gesperrt ist, obwohl beim Aufruf der Funktion <ul style="list-style-type: none"> • eine gültige User-ID und • eine korrekte zugehörige PIN übergeben werden. Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	NT
II_AUT_06_Template	Prüfung, ob ein nicht angemeldeter Nutzer Funktionen aufrufen kann, die nur von angemeldeten Nutzern verwendet werden dürfen. Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte. Es werden die Funktionalitäten aus Tabelle 34 getestet und es wird <code>ErrorUserNotAuthenticated</code> erwartet.	Siehe Tabelle 34	NT
II_AUT_07_Template	Prüfung, ob der Nutzer " logger " Funktionen aufrufen kann, die von ihm nicht verwendet werden dürfen. Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte. Es werden die Funktionalitäten aus Tabelle 35 getestet und es wird <code>ErrorUserNotAuthorized</code> erwartet.	Siehe Tabelle 35	NT

ID	Zielsetzung	Profile	Typ
II_AUT_08_Template	<p>Prüfung, ob der Nutzer "admin" Funktionen aufrufen kann, die von ihm nicht verwendet werden dürfen.</p> <p>Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte.</p> <p>Es werden die Funktionalitäten aus Tabelle 36 getestet und es wird <code>ErrorUserNotAuthorized</code> erwartet.</p>	Siehe Tabelle 36	NT
II_AUT_09_Template	<p>Prüfung, ob der Nutzer "timeadmin" Funktionen aufrufen kann, die von ihm nicht verwendet werden dürfen.</p> <p>Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte.</p> <p>Es werden die Funktionalitäten aus Tabelle 37 getestet und es wird <code>ErrorUserNotAuthorized</code> erwartet.</p>	Siehe Tabelle 37	NT
II_AUT_10_Template	<p>Prüfung, ob ein nicht angemeldeter Nutzer Funktionen aufrufen kann, die von nicht angemeldeten Nutzern verwendet werden dürfen.</p> <p>Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte.</p> <p>Es werden die Funktionalitäten aus Tabelle 38 getestet.</p>	Siehe Tabelle 38	PT
II_AUT_11_Template	<p>Prüfung, ob ein nicht angemeldeter Nutzer Funktionen aufrufen kann, die von nicht angemeldeten Nutzern verwendet werden dürfen.</p> <p>Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte.</p> <p>Zusätzlich wird geprüft, ob in der dabei entstandenen Log-Nachricht der korrekte Nutzer als Auslöser eingetragen ist.</p> <p>Es werden die Funktionalitäten aus Tabelle 39 getestet.</p>	Siehe Tabelle 39	PT
II_AUT_12_Template	<p>Prüfung, ob der Nutzer "logger" Funktionen aufrufen kann, die von ihm verwendet werden dürfen.</p> <p>Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte.</p> <p>Es werden die Funktionalitäten aus Tabelle 38 getestet.</p>	Siehe Tabelle 38	PT
II_AUT_13_Template	<p>Prüfung, ob der Nutzer "logger" Funktionen aufrufen kann, die von ihm verwendet werden dürfen.</p> <p>Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte.</p> <p>Zusätzlich wird geprüft, ob in der dabei entstandenen Log-Nachricht der korrekte Nutzer als Auslöser eingetragen ist.</p> <p>Es werden die Funktionalitäten aus Tabelle 40 getestet.</p>	Siehe Tabelle 40	PT

ID	Zielsetzung	Profile	Typ
II_AUT_14_Template	Prüfung, ob der Nutzer " admin " Funktionen aufrufen kann, die von ihm verwendet werden dürfen. Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte. Es werden die Funktionalitäten aus Tabelle 41 getestet.	Siehe Tabelle 41	PT
II_AUT_15_Template	Prüfung, ob der Nutzer "admin" Funktionen aufrufen kann, die von ihm verwendet werden dürfen. Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte. Zusätzlich wird geprüft, ob in der dabei entstandenen Log-Nachricht der korrekte Nutzer als Auslöser eingetragen ist. Es werden die Funktionalitäten aus Tabelle 42 getestet.	Siehe Tabelle 42	PT
II_AUT_16_Template	Prüfung, ob der Nutzer " timeadmin " Funktionen aufrufen kann, die von ihm verwendet werden dürfen. Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte. Es werden die Funktionalitäten aus Tabelle 43 getestet.	Siehe Tabelle 43	PT
II_AUT_17_Template	Prüfung, ob der Nutzer "timeadmin" Funktionen aufrufen kann, die von ihm verwendet werden dürfen. Es werden Parameter in der Form übergeben, dass ein berechtigter Nutzer die Funktion erfolgreich durchführen könnte. Zusätzlich wird geprüft, ob in der dabei entstandenen Log-Nachricht der korrekte Nutzer als Auslöser eingetragen ist. Es werden die Funktionalitäten aus Tabelle 44 getestet.	Siehe Tabelle 44	PT
II_AUT_18_Template	Prüfung, ob zuvor angemeldete Nutzer abgemeldet werden, wenn sich ein anderer Nutzer über die Funktionalität zur Authentifizierung von Nutzern anmeldet. Es werden die Ereignisse aus Tabelle 45 getestet.	Siehe Tabelle 45	PT
II_AUT_19	Prüfung, ob Fehlermeldungen der Funktionalität zum Abmelden von Nutzern an die aufrufende Funktionalität zur Authentifizierung von Nutzern weitergereicht werden, wenn erstere durch zweite ausgelöst wird.	II	FP
II_AUT_20_Template	Prüfung, ob der PIN Fehlbedienungsähler auf dem im ICS definierten Wert zurückgesetzt wird, wenn sich ein Nutzer erfolgreich authentifiziert hat. Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	PT
II_AUT_21	Prüfung, ob die TSE über die Einbindungsstelle von keinen weiteren Nutzern neben unauthenticated, logger, admin und timeadmin genutzt werden kann.	II	PT

ID	Zielsetzung	Profile	Typ
II_AUT_22	Prüfung, ob bei zentraler Zeitstellung der Nutzer central-timeadmin nicht über die Einbindungsschnittstelle angemeldet werden kann .	CENTRAL_TIME	NT
II_AUT_23	Prüfung, ob bei zentraler Zeitstellung der Nutzer central-timeadmin keine weiteren Funktionalitäten als die Zeitstellung ausführen kann.	CENTRAL_TIME	FP
II_AUT_24	Prüfung, ob der Nutzer smaadmin nicht über die Einbindungsschnittstelle angemeldet werden kann .	II	NT

Tabelle 32: Testfälle für die Einbindungsschnittstelle – Authentifizierung von Nutzern

ID Suffix	Zu verwendende Nutzer	Profile
_A	logger	II
_B	admin	II
_C	timeadmin	II_UPDATETIME

Tabelle 33: Auf Testfälle II_AUT_01_Template, II_AUT_03_Template, II_AUT_04_Template, II_AUT_05_Template, II_LGO_01_Template, II_LGO_02_Template, II_UBP_01_Template und II_UBP_02_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zum Abmelden von Nutzern.	II
_B	zur Initialisierung der TSE.	II
_C	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_D	zum Auslesen der Beschreibung der TSE.	II
_E	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_F	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II
_G	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME
_H	zur Konfiguration der Logging-Einstellungen der TSE.	II_CONFIGLOGGING
_I	zum Löschen der Log-Nachrichten.	II_DELETELOGS
_J	zur Wiedereinspielung von Backups von Log-Nachrichten..	II_RESTOREBACKUP
_K	zur Registrierung von Aufzeichnungssystemen.	II
_L	zur Deregistrierung von Aufzeichnungssystemen.	II

ID Suffix	Funktionalität...	Profile
_M	für das Starten einer Transaktion.	II
_N	für die Aktualisierung einer Transaktion.	II
_O	zum Beenden einer Transaktion.	II
_P	zur Unterbindung der Aufzeichnung von Transaktionen.	II_LOCKTRANSLOGGING
_Q	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UNLOCKTRANSLOGGING

Tabelle 34: Auf Testfall II_AUT_06_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Initialisierung der TSE.	II
_B	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_C	zum Auslesen der Beschreibung der TSE.	II
_D	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_E	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II
_F	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME
_G	zur Konfiguration der Logging-Einstellungen der TSE.	II_CONFIGLOGGING
_H	zum Löschen der Log-Nachrichten.	II_DELETELOGS
_I	zur Wiedereinspielung von Backups von Log-Nachrichten..	II_RESTOREBACKUP
_J	zur Unterbindung der Aufzeichnung von Transaktionen.	II_LOCKTRANSLOGGING
_K	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UNLOCKTRANSLOGGING

Tabelle 35: Auf Testfall II_AUT_07_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Konfiguration der Logging-Einstellungen der TSE.	II_CONFIGLOGGING
_B	für das Starten einer Transaktion.	II
_C	für die Aktualisierung einer Transaktion.	II
_D	zum Beenden einer Transaktion.	II

Tabelle 36: Auf Testfall II_AUT_08_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Initialisierung der TSE.	II_UPDATETIME
_B	zum Erstellen oder Ändern der Beschreibung der TSE.	II_UPDATETIME
_C	zum Auslesen der Beschreibung der TSE.	II_UPDATETIME
_D	zur Auslösung eines Selbsttests.	II_UPDATETIME
_E	zur Installation von Updates für die TSE.	II_UPDATETIME II_UPDATEDEVICE
_F	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II_UPDATETIME
_G	zur Konfiguration der Logging-Einstellungen der TSE.	II_UPDATETIME II_CONFIGLOGGING
_H	für den Export aller Log-Nachrichten, zur Verifikation benötigten Zertifikate und Zusatzdateien.	II_UPDATETIME
_I	zur Ausgabe der Zertifikate der Zertifikatskette.	II_UPDATETIME
_J	zum Löschen der Log-Nachrichten.	II_UPDATETIME II_DELETELOGS
_K	zur Ausgabe der Seriennummern.	II_UPDATETIME
_L	zur Ausgabe des aktuellen Stands des Signaturzählers.	II_UPDATETIME
_M	zur Wiedereinspielung von Backups von Log-Nachrichten.	II_UPDATETIME II_RESTOREBACKUP
_N	zur Ausgabe der zuletzt erzeugten Log-Nachricht.	II_UPDATETIME
_O	zur Registrierung von Aufzeichnungssystemen.	II_UPDATETIME
_P	zur Deregistrierung von Aufzeichnungssystemen.	II_UPDATETIME
_Q	für das Starten einer Transaktion.	II_UPDATETIME
_R	für die Aktualisierung einer Transaktion.	II_UPDATETIME
_S	zum Beenden einer Transaktion.	II_UPDATETIME
_T	zum Export von Transaktions-Log-Nachrichten mit Filter-Funktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	II_UPDATETIME II_EXPORTFILTERED

ID Suffix	Funktionalität...	Profile
_U	zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können.	II_UPDATETIME
_V	zur Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind.	II_UPDATETIME II_CURNOCLIENTS
_W	zur Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können.	II_UPDATETIME II_MAXNOCLIENTS
_X	zur Ausgabe der aktuell registrierten Aufzeichnungssysteme.	II_UPDATETIME II_REGISTEREDCLIENTS
_Y	zur Ausgabe der Anzahl von offenen Transaktionen.	II_UPDATETIME II_CURNOTRANSACTIONS
_Z	zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können.	II_UPDATETIME II_MAXNOTRANSACTIONS
_AA	zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet.	II_UPDATETIME II_TRANSACTIONSTATE
_AB	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	II_UPDATETIME II_OPENTRANSACTIONS
_AC	zur Ausgabe des aktuellen Stands des Transaktionszählers.	II_UPDATETIME
_AD	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	II_UPDATETIME II_LASTTRANSLOG
_AE	zur Unterbindung der Aufzeichnung von Transaktionen.	II_UPDATETIME II_LOCKTRANSLLOGGING
_AF	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UPDATETIME II_UNLOCKTRANSLLOGGING

Tabelle 37: Auf Testfall II_AUT_09_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Ausgabe der Gesamtkapazität des Speichermediums.	II_TOTALMEMORY
_B	zur Ausgabe der aktuell verwendeten Speicherkapazität.	II_USEDMEMORY
_C	zur Ausgabe der aktuell nicht verwendeten Speicherkapazität.	II_FREEMEMORY

ID Suffix	Funktionalität..	Profile
_D	zur Ausgabe von Zustandsdaten der TSE.	II_DEVICEHEALTH
_E	zur Ausgabe von Versionsinformationen über die TSE.	II_GETVERSIONS
_F	zur Ausgabe des Datums ab dem die Technische Sicherheits-einrichtung planmäßig nicht mehr zur Sicherung von Trans-aktionen verwendet werden kann.	II_ENDOFUSAGEDATE
_G	zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen.	II
_H	zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit.	II_CURRENTTIME
_I	für den Export aller Log-Nachrichten, zur Verifikation benö-tigten Zertifikate und Zusatzdateien.	II
_J	zur Ausgabe der Zertifikate der Zertifikatskette.	II
_K	zur Ausgabe der Seriennummern.	II
_L	zur Ausgabe des aktuellen Stands des Signaturzählers.	II
_M	zur Ausgabe der zuletzt erzeugten Log-Nachricht.	II
_N	zum Export von Transaktions-Log-Nachrichten mit Filter-Funktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	II_EXPORTFILTERED
_O	zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können.	II
_P	zur Ausgabe der Anzahl von Aufzeichnungssystemen, die ak-tuell an nicht beendeten Transaktionen beteiligt sind.	II_CURNOCLIENTS
_Q	zur Ausgabe der maximalen Anzahl von Aufzeichnungssys-temen, die gleichzeitig Transaktionen protokollieren kön-nen.	II_MAXNOCLIENTS
_R	zur Ausgabe der aktuell registrierten Aufzeichnungssysteme.	II_REGISTEREDCLIENTS
_S	zur Ausgabe der Anzahl von offenen Transaktionen.	II_CURNOTRANSACTIONS
_T	zur Ausgabe der maximalen Anzahl von offenen Transaktio-nen, die gleichzeitig von der Technischen Sicherheitseinrich-tung verwaltet werden können.	II_MAXNOTRANSACTIONS
_U	zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet.	II_TRANSACTIONSTATE

ID Suffix	Funktionalität...	Profile
_V	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	II_OPENTRANSACTIONS
_W	zur Ausgabe des aktuellen Stands des Transaktionszählers.	II
_X	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	II_LASTTRANSLOG

Tabelle 38: Auf Testfälle II_AUT_10_Template und II_AUT_12_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Authentifizierung von Nutzern.	II
_B	zur Auslösung eines Selbsttests	II

Tabelle 39: Auf Testfall II_AUT_11_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Authentifizierung von Nutzern.	II
_B	zum Abmelden von Nutzern.	II
_C	zum Entsperren der PIN eines autorisierten Nutzers.	II
_D	zur Auslösung eines Selbsttests.	II
_E	zur Registrierung von Aufzeichnungssystemen.	II
_F	zur Deregistrierung von Aufzeichnungssystemen.	II
_G	für das Starten einer Transaktion.	II
_H	für die Aktualisierung einer Transaktion.	II
_I	zum Beenden einer Transaktion.	II

Tabelle 40: Auf Testfall II_AUT_13_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zum Auslesen der Beschreibung der TSE.	II
_B	zur Ausgabe der Gesamtkapazität des Speichermediums.	II_TOTALMEMORY
_C	zur Ausgabe der aktuell verwendeten Speicherkapazität.	II_USEDMEMORY

ID Suffix	Funktionalität...	Profile
_D	zur Ausgabe der aktuell nicht verwendeten Speicherkapazität.	II_FREEMEMORY
_E	zur Ausgabe von Zustandsdaten der TSE.	II_DEVICEHEALTH
_F	zur Ausgabe von Versionsinformationen über die TSE.	II_GETVERSIONS
_G	zur Ausgabe des Datums ab dem die Technische Sicherheitseinrichtung planmäßig nicht mehr zur Sicherung von Transaktionen verwendet werden kann.	II_ENDOFUSAGEDATE
_H	zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen.	II
_I	zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit.	II_CURRENTTIME
_J	für den Export aller Log-Nachrichten, zur Verifikation benötigten Zertifikate und Zusatzdateien.	II
_K	zur Ausgabe der Zertifikate der Zertifikatskette.	II
_L	zur Ausgabe der Seriennummern.	II
_M	zur Ausgabe des aktuellen Stands des Signaturzählers.	II
_N	zur Wiedereinspielung von Backups von Log-Nachrichten.	II_RESTOREBACKUP
_O	zur Ausgabe der zuletzt erzeugten Log-Nachricht.	II
_P	zum Export von Transaktions-Log-Nachrichten mit Filterfunktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	II_EXPORTFILTERED
_Q	zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können.	II
_R	zur Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind.	II_CURNOCLIENTS
_S	zur Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können.	II_MAXNOCLIENTS
_T	zur Ausgabe der aktuell registrierten Aufzeichnungssysteme.	II_REGISTEREDCLIENTS
_U	zur Ausgabe der Anzahl von offenen Transaktionen.	II_CURNOTTRANSACTIONS
_V	zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können.	II_MAXNOTTRANSACTIONS

ID Suffix	Funktionalität...	Profile
_W	zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet.	II_TRANSACTIONSTATE
_X	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	II_OPENTRANSACTIONS
_Y	zur Ausgabe des aktuellen Stands des Transaktionszählers.	II
_Z	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	II_LASTTRANSLOG

Tabelle 41: Auf Testfall II_AUT_14_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Authentifizierung von Nutzern.	II
_B	zum Abmelden von Nutzern.	II
_C	zum Entsperren der PIN eines autorisierten Nutzers.	II
_D	zur Initialisierung der TSE.	II
_E	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_F	zur Auslösung eines Selbsttests.	II
_G	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_H	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II
_I	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME
_J	zum Löschen der Log-Nachrichten.	II_DELETELOGS
_K	zur Registrierung von Aufzeichnungssystemen.	II
_L	zur Deregistrierung von Aufzeichnungssystemen.	II
_M	zur Unterbindung der Aufzeichnung von Transaktionen.	II_LOCKTRANSLOGGING
_N	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UNLOCKTRANSLOGGING

Tabelle 42: Auf Testfall II_AUT_15_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Ausgabe der Gesamtkapazität des Speichermediums	II_UPDATETIME II_TOTALMEMORY
_B	zur Ausgabe der aktuell verwendeten Speicherkapazität	II_UPDATETIME II_USEDMEMORY
_C	zur Ausgabe der aktuell nicht verwendeten Speicherkapazität	II_UPDATETIME II_FREEMEMORY
_D	zur Ausgabe von Zustandsdaten der TSE.	II_UPDATETIME II_DEVICEHEALTH
_E	zur Ausgabe von Versionsinformationen über die TSE.	II_UPDATETIME II_GETVERSIONS
_F	zur Ausgabe des Datums ab dem die Technische Sicherheitseinrichtung planmäßig nicht mehr zur Sicherung von Transaktionen verwendet werden kann.	II_UPDATETIME II_ENDOFUSAGEDATE
_G	zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen.	II_UPDATETIME
_H	zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit.	II_UPDATETIME II_CURRENTTIME

Tabelle 43: Auf Testfall II_AUT_16_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Authentifizierung von Nutzern.	II_UPDATETIME
_B	zum Abmelden von Nutzern.	II_UPDATETIME
_C	zum Entsperren der PIN eines autorisierten Nutzers.	II_UPDATETIME
_D	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME

Tabelle 44: Auf Testfall II_AUT_17_Template anzuwendende Verfeinerungen

ID Suffix	Ereignis	Profile
_A	Nachdem admin angemeldet war, meldet sich ein logger an.	II
_B	Nachdem logger angemeldet war, meldet sich ein admin an.	II
_C	Nachdem admin angemeldet war, meldet sich ein timeadmin an.	II_UPDATETIME

ID Suffix	Ereignis	Profile
_D	Nachdem logger angemeldet war, meldet sich ein timeadmin an.	II_UPDATETIME
_E	Nachdem timeadmin angemeldet war, meldet sich ein admin an.	II_UPDATETIME
_F	Nachdem timeadmin angemeldet war, meldet sich ein logger an.	II_UPDATETIME
_G	Ein admin meldet sich wiederholt an.	II
_H	Ein logger meldet sich wiederholt an.	II
_I	Ein timeadmin meldet sich wiederholt an.	II_UPDATETIME

Tabelle 45: Auf Testfall II_AUT_18_Template anzuwendende Verfeinerungen

6.3.1.2 Abmeldung von Nutzern der Technischen Sicherheitseinrichtung (II_LGO)

ID	Zielsetzung	Profile	Typ
II_LGO_01	Prüfung, ob die Abmeldung für einen authentifizierten Nutzer erfolgreich ist, wenn die Funktionalität zum Abmelden von Nutzern aufgerufen wird. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird. Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	PT
II_LGO_02	Prüfung, ob die TSE authentifizierte Nutzer automatisch abmeldet, wenn über einen definierten Zeitraum keine Funktionen aufrufen werden, für die eine Authentifizierung erforderlich ist. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht. Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	PT

Tabelle 46: Testfälle für die Einbindungsschnittstelle – Abmelden von Nutzern

6.3.1.3 Entsperrn von Nutzern (II_UBP)

ID	Zielsetzung	Profile	Typ
II_UBP_01_Template	Prüfung, ob das Entsperrn der PIN-Eingabe für einen Nutzer erfolgreich ist, wenn die Funktionalität zum Entsperrn der PIN eines autorisierten Nutzers mit <ul style="list-style-type: none"> einer gültigen User-ID, der korrekten zugehörigen PUK und einem neuen Wert für die PIN aufgerufen wird. Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	PT
II_UBP_02_Template	Prüfung, ob das Entsperrn der PIN-Eingabe eines autorisierten Nutzers fehlschlägt , wenn die Funktionalität zum Entsperrn der PIN eines autorisierten Nutzers mit <ul style="list-style-type: none"> einer gültigen User-ID und der falschen PUK aufgerufen wird. Es werden die Nutzer aus Tabelle 33 getestet.	Siehe Tabelle 33	NT
II_UBP_03	Prüfung, ob die Funktionalität zum Entsperrn der PIN eines autorisierten Nutzers Gegenmaßnahmen gegen Angriffe in Bezug auf das Erraten der PUK implementiert.	II	PT
II_UBP_04	Prüfung, ob die Funktionalität zum Entsperrn der PIN eines autorisierten Nutzers die Fehlermeldung <code>ErrorPukIsTemporarilyBlocked</code> auslöst und damit die wiederholte Ausführung zeitweise blockiert wird, wenn ein Password Guessing Attack erkannt wird.	II PUK_BLOCKABLE	NT
II_UBP_05	Prüfung, ob die Funktionalität zum Entsperrn der PIN eines autorisierten Nutzers für den Nutzer admin keinen leeren String als neuen PIN akzeptiert.	II	NT
II_UBP_06	Prüfung, ob die Funktionalität zum Entsperrn der PIN eines autorisierten Nutzers für den Nutzer timeadmin keinen leeren String als neuen PIN akzeptiert.	II_UPDATETIME	NT

Tabelle 47: Testfälle für die Einbindungsschnittstelle – Entsperrn der PIN eines autorisierten Nutzers

6.3.1.4 Initialisierung der Technischen Sicherheitseinrichtung (II_INI)

ID	Zielsetzung	Profile	Typ
II_INI_01	Prüfung, ob die Funktionalität zur Initialisierung der TSE die folgenden Aktionen durchführt: <ul style="list-style-type: none"> • Abfragen der Log-Nachricht-Teile vom Sicherheitsmodul • Speichern der Log-Nachricht-Teile im Speichermedium. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_INI_02	Prüfung, ob bei einer wiederholten Initialisierung der Technischen Sicherheitseinrichtung eine gültige Fehlermeldung ausgegeben wird.	II	NT

Tabelle 48: Testfälle für die Einbindungsschnittstelle – Initialisierung der Technischen Sicherheitseinrichtung

6.3.1.5 Setzen von Beschreibungen in der TSE (II_SDE)

ID	Zielsetzung	Profile	Typ
II_SDE_01	Prüfung, ob die Funktionalität zum Erstellen oder Ändern der Beschreibung der TSE verschiedene Längen (bis zu 64 Zeichen) als Eingabeparameter akzeptiert. Zusätzlich wird geprüft, ob die neu gesetzt Beschreibung in der TSE verwendet wird, ob die Ausführung ohne Fehlermeldung beendet wird und, ob die Log-Nachricht korrekt erstellt wird.	II	PT
II_SDE_02	Prüfung, ob die Funktionalität zum Erstellen oder Ändern der Beschreibung der TSE die Fehlermeldung ErrorStoring-DataFailed auslöst, wenn die neue Beschreibung nicht auf dem Speicher abgelegt werden kann.	II	NT

Tabelle 49: Testfälle für die Einbindungsschnittstelle – Setzen von Beschreibungen in der TSE

6.3.1.6 Abfrage der TSE Beschreibung (II_GDE)

ID	Zielsetzung	Profile	Typ
II_GDE_01	Prüfung, ob die Funktionalität zum Auslesen der Beschreibung der TSE eine bis zu 64 Zeichen lange Beschreibung zurückgibt. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird. Die Beschreibung wurde durch einen Nutzer gesetzt.	II	PT

ID	Zielsetzung	Profile	Typ
II_GDE_02	Prüfung, ob die Funktionalität zum Auslesen der Beschreibung der TSE eine bis zu 64 Zeichen lange Beschreibung zurückgibt. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird. Die Beschreibung wurde durch den Hersteller gesetzt und durch den Nutzer nicht geändert.	DESCRIPTION_SET	PT
II_GDE_03	Prüfung, ob die Funktionalität zum Auslesen der Beschreibung der TSE einen leeren String zurückgibt, wenn die Beschreibung nicht durch den Hersteller oder den Nutzer gesetzt wurde.	DESCRIPTION_NOT_SET	PT
II_GDE_04	Prüfung, ob die Funktionalität zum Auslesen der Beschreibung der TSE die Fehlermeldung ErrorGetDescriptionFailed ausgibt, wenn die gesetzte Beschreibung nicht ermittelt werden kann.	II	NT

Tabelle 50: Testfälle für die Einbindungsschnittstelle – Abfrage der Beschreibung der TSE

6.3.1.7 Auslösen eines Selbsttests (II_STE)

ID	Zielsetzung	Profile	Typ
II_STE_01	Prüfung, ob die Funktionalität zur Auslösung eines Selbsttests einen Selbsttest auslöst und ob eine Log-Message erzeugt wird. Zusätzlich erfolgt eine Prüfung des Rückgabewerts selfTestResults, der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_STE_02	Prüfung, ob Warnungen, die im Falle eines fehlgeschlagenen Selbsttests ausgegeben werden können, allgemein verständlich verfasst sind.	II	PT
II_STE_03	Prüfung, ob die Funktionalität zur Auslösung eines Selbsttests die Fehlermeldung ErrorSelfTestFailed ausgibt, wenn bei der Durchführung des Selbsttest ein Fehler auftritt.	II	NT

Tabelle 51: Testfälle für die Einbindungsschnittstelle – Auslösen eines Selbsttests

6.3.1.8 Geräte-Update (II_UDD)

ID	Zielsetzung	Profile	Typ
II_UDD_01	Prüfung, ob ein Update mit der Funktionalität zur Installation von Updates für die TSE durchgeführt werden kann. Zusätzlich werden die beiden zu erstellenden Log-Nachrichten und der Rückgabewert geprüft. Es wird geprüft, ob die Log-Nachricht updateDevice die geforderten Informationen über den aktuellen Versionsstand jeder Komponente enthält und ob die Log-Nachricht updateDeviceCompleted die geforderten Informationen über den neuen Versionsstand jeder Komponente enthält.	II_UPDATEDEVICE	PT
II_UDD_02	Prüfung, ob bei einem Update einer fernverbundenen Komponente des Sicherheitsmoduls , während die TSE nicht in Betrieb ist, direkt beim ersten Start nach dem Update eine entsprechende Meldung protokolliert wird.	SM_REMOTE_COMPONENTS UPDATE_EXTERNAL	PT
II_UDD_03	Prüfung, ob bei einem Update des fernverbundenen Speichermediums , während die TSE nicht in Betrieb ist, direkt beim ersten Start nach dem Update eine entsprechende Meldung protokolliert wird.	STORAGE_REMOTE UPDATE_EXTERNAL	PT
II_UDD_04	Prüfung, ob die Funktionalität zur Installation von Updates für die TSE eine Log-Nachricht erstellt, wenn das Update vollständig fehlschlägt . Zusätzlich wird der Inhalt der zu erstellende Log-Nachrichte updateDeviceCompleted auf Korrektheit geprüft.	II_UPDATEDEVICE	NT
II_UDD_05	Prüfung, ob die Funktionalität zur Installation von Updates für die TSE eine Log-Nachricht erstellt, wenn das Update teilweise fehlschlägt . Zusätzlich wird der Inhalt der zu erstellende Log-Nachrichte updateDeviceCompleted auf Korrektheit geprüft.	II_UPDATEDEVICE	NT
II_UDD_06	Prüfung, ob die Funktionalität zur Installation von Updates für die TSE die Fehlermeldung ErrorOpenTransactionFound ausgibt, wenn es offene, nicht als verwaist eingestufte Transaktionen gibt, die derzeit vom Secure Element verwaltet werden.	II_UPDATEDEVICE	NT
II_UDD_07	Prüfung, ob ein Update durch eine externe Funktionalität angestoßen werden kann. Zusätzlich werden die beiden zu erstellenden Log-Nachrichten geprüft. Es wird geprüft, ob die Log-Nachricht updateDevice die geforderten Informationen über den aktuellen Versionsstand jeder Komponente enthält und ob die Log-Nachricht updateDeviceCompleted die geforderten Informationen über den neuen Versionsstand jeder Komponente enthält.	UPDATE_EXTERNAL UPDATE_EXTERNAL_LOGGED	

ID	Zielsetzung	Profile	Typ
II_UDD_08	Prüfung, ob ein Update durch eine externe Funktionalität angestoßen werden kann. Zusätzlich wird die zu erstellende Log-Nachricht geprüft. Es wird geprüft, ob die Log-Nachricht updateDeviceCompleted die geforderten Informationen über den neuen Versionsstand jeder Komponente (componentName, manufacturer, model, version, ggf. certificationID) enthält.	UPDATE_EXTERNAL UPDATE_EXTERNAL_NOT_LOGGED	

Tabelle 52: Testfälle für die Einbindungsschnittstelle – Geräte-Update

6.3.1.9 Außerbetriebnahme des Sicherheitsmoduls der Technischen Sicherheitseinrichtung (II_DSE)

ID	Zielsetzung	Profile	Typ
II_DSE_01	Prüfung, ob das Sicherheitsmodul nach einem Aufruf der Funktionalität zur Außerbetriebnahme des Sicherheitsmoduls der TSE deaktiviert wurde. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird und, ob die Log-Nachricht korrekt erstellt wird.	II	PT
II_DSE_02	Prüfung, ob bei Deaktivierung des Sicherheitsmoduls durch die Funktionalität zur Außerbetriebnahme des Sicherheitsmoduls der TSE die Audit-Funktionalität im Sicherheitsmodul gestoppt wird.	II	PT
II_DSE_03	Prüfung, ob die Funktionalität zur Außerbetriebnahme des Sicherheitsmoduls der TSE die Fehlermeldung ErrorDisableSecureElementFailed auslöst, wenn die Deaktivierung des Sicherheitsmoduls fehlschlägt.	II	NT

Tabelle 53: Testfälle für die Einbindungsschnittstelle – Außerbetriebnahme des Sicherheitsmoduls

6.3.1.10 Abfrage zur Gesamtkapazität des Speichermediums (II_GTM)

ID	Zielsetzung	Profile	Typ
II_GTM_01	Prüfung, ob die Funktionalität zur Ausgabe der Gesamtkapazität des Speichermediums die zurückgegebene Gesamtkapazität des Speichermediums in Bytes (im Parameter totalMemory) der Angabe im ICS entspricht. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II_TOTALMEMORY	PT

ID	Zielsetzung	Profile	Typ
II_GTM_02	Prüfung, ob die Funktionalität zur Ausgabe der Gesamtkapazität des Speichermediums die Fehlermeldung ErrorGetTotalMemoryFailed ausgibt, wenn die Kapazität des Speichermediums nicht festgestellt werden kann.	II_TOTALMEMORY	NT

Tabelle 54: Testfälle für die Einbindungsschnittstelle – Abfrage der Gesamtkapazität des Speichermediums

6.3.1.11 Abfrage zur aktuell verwendeten Speicherkapazität (II_GUM)

ID	Zielsetzung	Profile	Typ
II_GUM_01	Prüfung, ob die Funktionalität zur Ausgabe der aktuell verwendeten Speicherkapazität die aktuell verwendete Speicherkapazität in Bytes zurückgibt. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II_USEDMEMORY	PT
II_GUM_02	Prüfung, ob die Funktionalität zur Ausgabe der aktuell verwendeten Speicherkapazität die Fehlermeldung ErrorGetUsedMemoryFailed ausgibt, wenn die aktuell verwendete Speicherkapazität nicht festgestellt werden kann.	II_USEDMEMORY	NT

Tabelle 55: Testfälle für die Einbindungsschnittstelle – Abfrage der aktuell verwendeten Speicherkapazität

6.3.1.12 Abfrage zur freien Speicherkapazität (II_GFM)

ID	Zielsetzung	Profile	Typ
II_GFM_01	Prüfung, ob die Funktionalität zur Ausgabe der aktuell nicht verwendeten Speicherkapazität die aktuell nicht verwendete Speicherkapazität in Bytes zurückgibt. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II_FREEMEMORY	PT
II_GFM_02	Prüfung, ob die Funktionalität zur Ausgabe der aktuell nicht verwendeten Speicherkapazität die Fehlermeldung ErrorGetFreeMemoryFailed ausgibt, wenn die aktuell nicht verwendete Speicherkapazität nicht festgestellt werden kann.	II_FREEMEMORY	NT

Tabelle 56: Testfälle für die Einbindungsschnittstelle – Abfrage der freien Speicherkapazität

6.3.1.13 Abfrage zum Gesundheitszustand aller Komponenten der TSE (II_GDH)

ID	Zielsetzung	Profile	Typ
II_GDH_01	Prüfung, ob der Parameter healthInformationSet, den die Funktionalität zur Ausgabe von Zustandsdaten der TSE zurückgibt, der vorgegebenen ASN.1 Definition entspricht.	II_DEVICEHEALTH	PT

ID	Zielsetzung	Profile	Typ
II_GDH_02	Prüfung, ob der Parameter healthInformationSet, den die Funktionalität zur Ausgabe von Zustandsdaten der TSE zurückgibt, eine ASN.1 DER Kodierung aufweist.	II_DEVICEHEALTH	PT
II_GDH_03	Prüfung, ob die Funktionalität zur Ausgabe von Zustandsdaten der TSE den aktuellen Gesundheitszustand aller Komponenten zurückgibt und ob das Element additionalDescription eine für Menschen lesbare Begründung enthält. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II_DEVICEHEALTH	PT
II_GDH_04	Prüfung, ob die Funktionalität zur Ausgabe von Zustandsdaten der TSE die Fehlermeldung ErrorGetDeviceHealthFailed ausgibt, wenn der aktuelle Gesundheitszustand aller Komponenten nicht festgestellt werden kann.	II_DEVICEHEALTH	NT

Tabelle 57: Testfälle für die Einbindungsschnittstelle – Abfrage zum Gesundheitszustand aller Komponenten der TSE

6.3.1.14 Abfrage der TSE Version (II_GCV)

ID	Zielsetzung	Profile	Typ
II_GCV_01	Prüfung, ob die Funktionalität zur Ausgabe von Versionsinformationen über die TSE die gleichen Informationen über das Gerät zurückgibt, wie sie in der Datei info.csv enthalten sind. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II_GETVERSIONS	PT
II_GCV_02	Prüfung, ob der Parameter deviceInformationSet, den die Funktionalität zur Ausgabe von Versionsinformationen über die TSE zurückgibt, der vorgegebenen ASN.1 Definition entspricht.	II_GETVERSIONS	PT
II_GCV_03	Prüfung, ob der Parameter deviceInformationSet, den die Funktionalität zur Ausgabe von Versionsinformationen über die TSE zurückgibt, eine ASN.1 DER Kodierung aufweist.	II_GETVERSIONS	PT
II_GCV_04	Prüfung, ob die Funktionalität zur Ausgabe von Versionsinformationen über die TSE die Fehlermeldung ErrorGetComponentVersionsFailed ausgibt, wenn die Informationen über das Gerät, wie sie in der Datei info.csv enthalten sind nicht festgestellt werden können.	II_GETVERSIONS	NT

Tabelle 58: Testfälle für die Einbindungsschnittstelle – Abfrage der TSE Version

6.3.1.15 Abfrage zum Datum des voraussichtlichen Nutzungsendes (II_GEU)

ID	Zielsetzung	Profile	Typ
II_GEU_01	Prüfung, ob die Funktionalität zur Ausgabe des Datums, ab dem die TSE planmäßig nicht mehr zur Sicherung von Transaktionen verwendet werden kann, ein solches Datum zurückgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.	II_ENDOFUSAGE- DATE	PT
II_GEU_02	Prüfung, ob die Funktionalität zur Ausgabe des Datums, ab dem die TSE planmäßig nicht mehr zur Sicherung von Transaktionen verwendet werden kann, die Fehlermeldung ErrorGetEndOfUsageDateFailed ausgibt, wenn ein solches Datum nicht festgestellt werden kann.	II_ENDOFUSAGE- DATE	NT

Tabelle 59: Testfälle für die Einbindungsschnittstelle – Abfrage zum Datum des voraussichtlichen Nutzungsendes

6.3.1.16 Aktualisierung der Uhrzeit (II_UDT)

ID	Zielsetzung	Profile	Typ
II_UDT_01	Prüfung, ob die Funktionalität zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls die Zeit mit übergebenen Werten (newDateTime) aktualisiert und ob eine Log-MESSAGE erzeugt wird. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird und, ob die Log-Nachricht korrekt erstellt wird.	II_UPDATETIME NO_TIME_SYNC	PT
II_UDT_02	Prüfung, ob die Funktionalität zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls die Zeit bei einem Sicherheitsmodul mit eigenem Zeitsynchronisationsmechanismus (ohne übergebene Zeitwerte) aktualisiert und ob eine Log-MESSAGE erzeugt wird. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird und, ob die Log-Nachricht korrekt erstellt wird.	II_UPDATETIME TIME_SYNC	PT
II_UDT_03	Prüfung, ob die Funktionalität zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls die Zeit mit übergebenen falschen Werten nicht aktualisiert und ob keine Log-MESSAGE erzeugt wird. Zusätzlich wird geprüft, ob eine gültige Fehlermeldung zurückgegeben wird.	II_UPDATETIME NO_TIME_SYNC	NT

ID	Zielsetzung	Profile	Typ
II_UDT_04	Prüfung, ob die Funktionalität zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls die Zeit nicht aktualisiert und ob keine Log-Message erzeugt wird, wenn die Funktionalität mit einem Parameter , in einem laut ICS nicht unterstützten Format , aufgerufen wird. Zusätzlich wird geprüft, ob eine gültige Fehlermeldung zurückgegeben wird.	II_UPDATETIME NO_TIME_SYNC	NT
II_UDT_05	Prüfung, ob die Funktionalität zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls beendet und die Fehlermeldung ErrorUnsupportedTimeSyncVariant ausgelöst wird, wenn die Funktionalität ohne Parameter aufgerufen wird und die API-Implementierung der Funktionalität einen solchen Aufruf ermöglicht, obwohl keine Zeitsynchronisierungsfunktion implementiert ist.	II_UPDATETIME NO_TIME_SYNC	NT
II_UDT_06	Prüfung, ob die Funktionalität zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls beendet und die Fehlermeldung ErrorUnsupportedTimeSyncVariant ausgelöst wird, wenn die Funktionalität mit Parameter aufgerufen wird und die API-Implementierung der Funktionalität einen solchen Aufruf ermöglicht, obwohl die direkte Aktualisierung der Zeit durch Übergabe von Parametern nicht implementiert ist.	II_UPDATETIME TIME_SYNC	NT
II_UDT_07	Prüfung, ob bei zentraler Zeitstellung der Nutzer central-timeadmin als auslösende Rolle in Log-Nachrichten für die Aktualisierung der Zeit genannt wird.	CENTRAL_TIME	PT

Tabelle 60: Testfälle für die Einbindungsschnittstelle - Aktualisierung der Zeit im Sicherheitsmodul

6.3.1.17 Abfrage der unterstützten Variante zur Aktualisierung der Zeit (II_TSV)

ID	Zielsetzung	Profile	Typ
II_TSV_01	Prüfung, ob die Funktionalität zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen die unterstützte Variante zur Aktualisierung der Zeit korrekt ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_TSV_02	Prüfung, ob die Funktionalität zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen die Fehlermeldung ErrorGetTimeSyncVariantFailed ausgibt, wenn die unterstützte Variante zur Aktualisierung der Zeit nicht festgestellt werden kann.	II	NT

Tabelle 61: Testfälle für die Einbindungsschnittstelle – Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen

6.3.1.18 Abfrage der aktuellen eingestellten Zeit (II_GCT)

ID	Zielsetzung	Profile	Typ
II_GCT_01	Prüfung, ob die Funktionalität zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit die aktuell eingestellte Zeit ausgibt, die auch für die Zeitstempelung der Log-Nachrichten verwendet wird. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.	II_CURRENTTIME	PT
II_GCT_02	Prüfung, ob die Fehlermeldung ErrorGetCurrentSeTimeFailed ausgelöst wird, wenn die Funktionalität zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit die aktuelle Zeit nicht vom Sicherheitsmodul beziehen kann.	II_CURRENTTIME	NT

Tabelle 62: Testfälle für die Einbindungsschnittstelle – Abfrage der aktuellen eingestellten Zeit

6.3.1.19 Konfiguration der Protokollierung von Ereignissen (II_CLG)

ID	Zielsetzung	Profile	Typ
II_CLG_01	Prüfung, ob die Protokolldaten für die Konfiguration von Ereignissen korrekt erstellt werden.	II_CONFIGLOGGING	PT

Tabelle 63: Testfälle zu Protokolldateien für die Konfiguration von Ereignissen

6.3.1.20 Export des TAR-Containers (II_EXP)

ID	Zielsetzung	Profile	Typ
II_EXP_01	Prüfung, ob Funktionalität für den Export aller Log-Nachrichten und der zur Verifikation benötigten Zertifikate und Zusatzdateien einen Datenexport über die Exportschnittstelle anstößt. Es wird geprüft, ob die Rückgabe eines TAR-Containers erfolgt.	II	PT
II_EXP_02	Prüfung, ob die Funktion für den Datenexport die Fehlermeldung ErrorStorageMediumDisconnected ausgibt, wenn der folgende Zustand gilt: Die Verbindung zwischen der Einbindungsschnittstelle und dem Speichermedium ist unterbrochen.	II STORAGE_REMOTE	NT
II_EXP_03	Prüfung, ob die Funktionalität für den Export aller Log-Nachrichten und der zur Verifikation benötigten Zertifikate und Zusatzdateien erfolgreich aufgerufen werden kann, wenn die Zeit nicht gestellt ist .	II_UPDATETIME	PT

ID	Zielsetzung	Profile	Typ
II_EXP_04	Prüfung, ob die Funktionalität für den Export aller Log-Nachrichten und der zur Verifikation benötigten Zertifikate und Zusatzdateien erfolgreich aufgerufen werden kann, wenn die Verbindung zu Teilen des Sicherheitsmoduls getrennt ist.	II SM_REMOTE_COMPONENTS	PT
II_EXP_05	Prüfung, ob die Funktionalität für den Export aller Log-Nachrichten und der zur Verifikation benötigten Zertifikate und Zusatzdateien alle gespeicherten Daten und einen korrekten Namen für den TAR-Container ausgibt . Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_EXP_06	Prüfung, ob die Funktionalität für den Export aller Log-Nachrichten und der zur Verifikation benötigten Zertifikate und Zusatzdateien erfolgreich aufgerufen werden kann, wenn das Sicherheitsmodul deaktiviert ist .	II	PT
II_EXP_07	Prüfung, ob die Funktionalität für den Export aller Log-Nachrichten und der zur Verifikation benötigten Zertifikate und Zusatzdateien alle gespeicherten Daten und einen korrekten Namen für den TAR-Container ausgibt, wenn der folgende Zustand gilt: <ul style="list-style-type: none"> • Nach der Initialisierung der TSE wurden keine weiteren Funktionen aufgerufen. 	II	PT
II_EXP_08	Prüfung, ob die Funktionalität für den Export aller Log-Nachrichten und der zur Verifikation benötigten Zertifikate und Zusatzdateien alle gespeicherten Daten und einen korrekten Namen für den TAR-Container ausgibt, wenn der folgende Zustand gilt: <ul style="list-style-type: none"> • Der verfügbare Speicher des Speichermediums ist zur Hälfte belegt. 	II	PT
II_EXP_09	Prüfung, ob die Funktionalität für den Export aller Log-Nachrichten und der zur Verifikation benötigten Zertifikate und Zusatzdateien alle gespeicherten Daten und einen korrekten Namen für den TAR-Container ausgibt, wenn der folgende Zustand gilt: <ul style="list-style-type: none"> • Der verfügbare Speicher des Speichermediums ist komplett belegt. 	II	PT

Tabelle 64: Testfälle für die Einbindungsschnittstelle – Export aller Log-Nachrichten, zur Verifikation benötigten Zertifikate und Zusatzdateien

6.3.1.21 Zertifikatsexport (II_EXC)

ID	Zielsetzung	Profile	Typ
II_EXC_01	Prüfung, ob nach einem Aufruf der Funktionalität zur Ausgabe der Zertifikate der Zertifikatskette einen TAR-Container mit den korrekten Zertifikaten exportiert wird. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_EXC_02	Prüfung, ob die Fehlermeldung ErrorExportLoggingCertificateFailed ausgelöst wird, wenn die Funktionalität zur Ausgabe der Zertifikate der Zertifikatskette die benötigten Zertifikate nicht ausgeben kann.	II	NT

Tabelle 65: Testfälle für die Einbindungsschnittstelle - Ausgabe der Zertifikate der Zertifikatskette

6.3.1.22 Löschen von gespeicherten Daten im Speichermedium (II_DLM)

ID	Zielsetzung	Profile	Typ
II_DLM_01	Prüfung, ob nach dem Aufruf der Funktionalität zum Löschen der Log-Nachrichten alle Daten im Speichermedium gelöscht werden, wenn alle Daten im Speichermedium bereits exportiert wurden. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II_DELETELOGS	PT
II_DLM_02	Prüfung, ob nach dem Aufruf der Funktionalität zum Löschen der Log-Nachrichten <ul style="list-style-type: none"> • keine Daten gelöscht werden, die noch nicht exportiert wurden und • die Fehlermeldung ErrorUnexportedLogMessages ausgelöst wird, wenn sich Daten im Speichermedium befinden, die noch nicht exportiert wurden.	II_DELETELOGS	NT
II_DLM_03	Prüfung, ob die Funktionalität zum Löschen der Log-Nachrichten die Fehlermeldung ErrorDeleteLogMessagesFailed auslöst, wenn die Kommunikationsverbindung zwischen der Einbindungsschnittstelle und dem Speichermedium unterbrochen ist.	II_DELETELOGS STORAGE_REMOTE	NT
II_DLM_04	Prüfung, ob die Fehlermeldung ErrorDeleteLogMessagesFailed ausgelöst wird, wenn die Funktionalität zum Löschen der Log-Nachrichten die zu löschenden Log-Nachrichten nicht löschen kann .	II_DELETELOGS	NT

Tabelle 66: Testfälle für die Einbindungsschnittstelle - Löschen der Log-Nachrichten

6.3.1.23 Export von Seriennummern (II_ESN)

ID	Zielsetzung	Profile	Typ
II_ESN_01	Prüfung, ob nach einem Aufruf der Funktionalität zur Ausgabe der Seriennummern die Seriennummer ² in der ASN.1-Struktur zurückgegeben wird, die in [BSI TR-03151-1] vorgegeben wird. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_ESN_02	Prüfung, ob nach einem Aufruf der Funktionalität zur Ausgabe der Seriennummer genau eine Seriennummer ² zurückgegeben wird. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_ESN_03	Prüfung, ob nach einem Aufruf der Funktionalität zur Ausgabe der Seriennummern der Hashwert , der die Seriennummer ² repräsentiert, korrekt ist. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_ESN_04	Prüfung, ob die Fehlermeldung ErrorExportSerialNumbersFailed ausgelöst wird, wenn die Funktionalität zur Ausgabe der Seriennummern die zu exportierende Seriennummer ² nicht ausgeben kann.	II	NT

Tabelle 67: Testfälle für die Einbindungsschnittstelle – Ausgabe der Seriennummern

6.3.1.24 Prüfungen zum aktuellen Stand der Signaturzähler (II_CSC)

ID	Zielsetzung	Profile	Typ
II_CSC_01	Prüfung, ob die Funktionalität zur Ausgabe des aktuellen Stands des Signaturzählers den aktuellen Stand der Signaturzähler ausgibt. Zusätzlich erfolgen Prüfungen, ob die Ausführung ohne Fehlermeldung beendet wird und ob das richtige Format für den Rückgabeparameter verwendet wird.	II	PT
II_CSC_02	Prüfung, ob die Funktionalität zur Ausgabe des aktuellen Stands des Signaturzählers die Fehlermeldung ErrorGetCurrentSignatureCounterFailed ausgibt, wenn der aktuelle Stand des Signaturzählers nicht festgestellt werden kann.	II	NT

² Der Begriff Seriennummer bezeichnet in diesem Zusammenhang den Hashwert über den öffentlichen Schlüssel, der zur Verifikation von Log-Nachrichten notwendig ist.

Tabelle 68: Testfälle für die Einbindungsschnittstelle – Ausgabe des aktuellen Stands des Signaturzählers

6.3.1.25 Wiederherstellung durch ein Backup (II_RFB)

ID	Zielsetzung	Profile	Typ
II_RFB_01	<p>Prüfung, ob nach einem Aufruf der Funktionalität zur Wiedereinspielung von Backups von Log-Nachrichten die Daten aus dem übergebenen TAR-Container nach den vorgegebenen Regeln wiederhergestellt werden.</p> <p>Der TAR-Container enthält keine Log-Nachrichten, zu denen bereits Log-Nachrichten mit gleichem Dateinamen im Speichermedium gespeichert sind.</p> <p>Der TAR-Container enthält keine Zertifikate, zu denen bereits Zertifikate mit gleichem Dateinamen in der TSE verwaltet werden.</p> <p>Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II_RESTOREBACKUP	PT
II_RFB_02	<p>Prüfung, ob nach einem Aufruf der Funktionalität zur Wiedereinspielung von Backups von Log-Nachrichten die Daten aus dem übergebenen TAR-Container nach den vorgegebenen Regeln wiederhergestellt werden.</p> <p>Der TAR-Container enthält Log-Nachrichten, zu denen bereits Log-Nachrichten mit gleichem Dateinamen im Speichermedium gespeichert sind.</p> <p>Das Backup enthält Zertifikate, zu denen bereits Zertifikate mit gleichem Dateinamen in der TSE verwaltet werden.</p> <p>Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II_RESTOREBACKUP	PT
II_RFB_03	<p>Prüfung, ob nach einem Aufruf der Funktionalität zur Wiedereinspielung von Backups von Log-Nachrichten bei einer fehlenden Verbindung von der Einbindungsschnittstelle zum Speichermedium eine gültige Fehlermeldung erfolgt.</p>	II_RESTOREBACKUP STORAGE_REMOTE	NT
II_RFB_04	<p>Prüfung, ob die Funktionalität zur Wiedereinspielung von Backups von Log-Nachrichten die Fehlermeldung ErrorRestoreFailed auslöst, wenn die übergebenen Log-Nachrichten nicht fehlerfrei gespeichert werden können.</p>	II_RESTOREBACKUP	NT
II_RFB_05	<p>Prüfung, ob die Funktionalität zur Wiedereinspielung von Backups von Log-Nachrichten die Fehlermeldung ErrorRestoreFailed auslöst, wenn die übergebenen Zertifikate nicht fehlerfrei gespeichert werden können.</p>	II_RESTOREBACKUP	NT

ID	Zielsetzung	Profile	Typ
II_RFB_06	Prüfung, ob die Funktionalität zur Wiedereinspielung von Backups von Log-Nachrichten bei Übergabe von Log-Nachrichten, die nicht von dieser TSE erstellt wurden, den Import der Log-Nachrichten ablehnt, die Fehlermeldung ErrorRestoreFailed auslöst und die Ausführung beendet.	II_RESTOREBACKUP	

Tabelle 69: Testfälle für die Einbindungsschnittstelle – Wiedereinspielung von Backups von Log-Nachrichten

6.3.1.26 Lesen der letzten Log-Nachricht (II_GLL)

ID	Zielsetzung	Profile	Typ
II_GLL_01	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Log-Nachricht die zuletzt erstellte Log-Nachricht und einen korrekten Namen diese Log-Nachricht ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird. Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion nicht aggregieren.	II SM_NOAGG	PT
II_GLL_02	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Log-Nachricht die zuletzt erstellte Log-Nachricht und einen korrekten Namen diese Log-Nachricht ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird. Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion aggregieren .	II SM_AGG	PT
II_GLL_03	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Log-Nachricht die Fehlermeldung ErrorReadingLog-Message auslöst, wenn die zuletzt erstellte Log-Nachricht nicht ausgegeben werden kann.	II	NT

Tabelle 70: Testfälle für die Einbindungsschnittstelle – Ausgabe der zuletzt erzeugten Log-Nachricht

6.3.1.27 Registrieren von Aufzeichnungssystemen (II_REC)

ID	Zielsetzung	Profile	Typ
II_REC_01	Prüfung, ob es nach Ausführung der Funktionalität zur Registrierung von Aufzeichnungssystemen möglich ist, die Funktionalitäten für das Starten, für die Aktualisierung und für die Beendigung von Transaktion mit einer speziellen Seriennummer eines Aufzeichnungssystems auszuführen. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_REC_02	Prüfung, ob die Funktionalität zur Registrierung von Aufzeichnungssystemen alle zugelassenen Zeichen als Seriennummer eines Aufzeichnungssystems akzeptiert. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_REC_03	Prüfung, ob die Funktionalität zur Registrierung von Aufzeichnungssystemen beendet wird und die Fehlermeldung ErrorClientLimitReached ausgelöst wird, wenn die maximale Anzahl an Aufzeichnungssystemen bereits registriert ist.	LIMITED_CLIENTS_TRACKED	NT
II_REC_04	Prüfung, ob die Funktionalität zur Registrierung von Aufzeichnungssystemen beendet wird und die Fehlermeldung ErrorInvalidClientIdCharacter ausgelöst wird, wenn die übergebene Seriennummer eines Aufzeichnungssystems ungültige Zeichen enthält.	II	NT
II_REC_05	Prüfung, ob die Funktionalität zur Registrierung von Aufzeichnungssystemen beendet wird und die Fehlermeldung ErrorClientAlreadyRegistered ausgelöst wird, wenn die übergebene Seriennummer eines Aufzeichnungssystems bereits registriert ist.	II	NT
II_REC_06	Prüfung, ob die Funktionalität zur Registrierung von Aufzeichnungssystemen beendet wird und die Fehlermeldung ErrorRegisterClientFailed ausgelöst wird, wenn das Aufzeichnungssystem nicht registriert werden kann .	II	NT

Tabelle 71: Testfälle für die Einbindungsschnittstelle – Registrieren von Aufzeichnungssystemen

6.3.1.28 Deregistrieren von Aufzeichnungssystemen (II_DRC)

ID	Zielsetzung	Profile	Typ
II_DRC_01	Prüfung, ob die Funktionalität zur Deregistrierung von Aufzeichnungssystemen es verhindert die Funktionalitäten für das Starten, für die Aktualisierung und zum Beenden von Transaktionen mit einer speziellen Seriennummer eines Aufzeichnungssystems erfolgreich auszuführen. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_DRC_02	Prüfung, ob die Funktionalität zur Deregistrierung von Aufzeichnungssystemen beendet wird und die Fehlermeldung ErrorClientNotRegistered ausgelöst wird, wenn die übergebene Seriennummer eines Aufzeichnungssystems nicht registriert ist.	II	NT
II_DRC_03	Prüfung, ob die Funktionalität zur Deregistrierung von Aufzeichnungssystemen beendet wird und die Fehlermeldung ErrorDeregisterClientFailed ausgelöst wird, wenn die erfolgreiche Ausführung der Funktionalitäten für das Starten, für die Aktualisierung und zum Beenden von Transaktion mit der übergebenen Seriennummer eines Aufzeichnungssystems nicht verhindert werden kann .	II	NT

Tabelle 72: Testfälle für die Einbindungsschnittstelle – Deregistrierung von Aufzeichnungssystemen

6.3.1.29 Starten einer Transaktion (II_STA)

ID	Zielsetzung	Profile	Typ
II_STA_01	<p>Prüfung, ob die Funktionalität für das Starten einer Transaktion die folgenden Aktionen durchführt:</p> <ul style="list-style-type: none"> • Abfragen der Log-Nachricht-Teile vom Sicherheitsmodul • Speichern der Log-Nachricht-Teile im Speichermedium • Rückgabe der folgenden Daten: <ul style="list-style-type: none"> ○ Transaktionsnummer ○ Zeitpunkt der Signaturerstellung ○ Hashwert über den öffentlichen Schlüssel des Schlüsselpaares, das für die Prüfwerterzeugung in Transaktions-Log-Nachrichten verwendet wird ○ Signaturzähler ○ Prüfwert. <p>Der Test übergibt beim Aufruf der Funktion</p> <ul style="list-style-type: none"> • die Seriennummer des Aufzeichnungssystems, • die Daten des Vorgangs und • die Art des Vorgangs. <p>Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II	PT
II_STA_02	<p>Prüfung, ob die Funktionalität für das Starten einer Transaktion bis zu 100 Zeichen für die Art des Vorgangs akzeptiert. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II	PT
II_STA_03	<p>Prüfung, ob die Funktionalität für das Starten einer Transaktion beendet wird und die Fehlermeldung <code>ErrorLimitOfSimultaneousOpenTransactionsReached</code> ausgelöst wird, wenn die Anzahl der offene Transaktionen, die im Sicherheitsmodul verwaltet werden, der maximalen Anzahl von Transaktionen entspricht, die im ICS angegeben wird.</p>	II	NT
II_STA_04	<p>Prüfung, ob die Funktionalität für das Starten einer Transaktion überprüft, ob die übergebene Seriennummer des Aufzeichnungssystems registriert ist, damit diese für die Aufzeichnung von Transaktionen verwendet werden kann. Die übergebene Seriennummer des Aufzeichnungssystems wurde zuvor noch nie registriert.</p>	II	NT

Tabelle 73: Testfälle für die Einbindungsschnittstelle – Starten einer Transaktion

6.3.1.30 Aktualisierung einer Transaktion (II_UPD)

ID	Zielsetzung	Profile	Typ
II_UPD_01	<p>Prüfung, ob die Funktionalität für die Aktualisierung einer Transaktion für eine Aktualisierung mit Absicherungsschritt die folgenden Aktionen durchführt:</p> <ul style="list-style-type: none"> • Abfragen der Log-Nachricht-Teile vom Sicherheitsmodul • Speichern der Log-Nachricht-Teile im Speichermedium • Rückgabe der folgenden Daten <ul style="list-style-type: none"> ○ Zeitpunkt der Aktualisierung ○ Prüfwert ○ Signaturzähler <p>Der Test übergibt beim Funktionsaufruf die</p> <ul style="list-style-type: none"> • Seriennummer des Aufzeichnungssystems, • Transaktionsnummer, • Art des Vorgangs und • Daten des Vorgangs. <p>Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	SM_NOAGG	PT
II_UPD_02	<p>Prüfung, ob die Funktionalität für die Aktualisierung einer Transaktion bei einer Aktualisierung ohne Absicherungsschritt keine Werte für</p> <ul style="list-style-type: none"> • den Zeitpunkt der Aktualisierung • den Signaturzähler und • den Prüfwert <p>zurückgibt.</p> <p>Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.</p> <p>Der Test übergibt beim Funktionsaufruf die Seriennummer des Aufzeichnungssystems, die Transaktionsnummer, die Art des Vorgangs und die Daten des Vorgangs.</p>	SM_AGG	PT
II_UPD_03	<p>Prüfung, ob der Parameter forceSignature von der Funktionalität für die Aktualisierung einer Transaktion ignoriert wird, wenn Aktualisierungen (Updates) direkt signiert und nicht aggregiert werden.</p>	SM_NOAGG II	PT
II_UPD_04	<p>Prüfung, ob die Funktionalität für die Aktualisierung einer Transaktion Aktualisierungen mit erzwungenen Absicherungsschritt ohne weitere Aggregation sichert. Zusätzlich werden die Rückgabeparameter und die erstellte Log-Nachricht auf Format und Inhalt geprüft.</p>	SM_AGG II	PT

ID	Zielsetzung	Profile	Typ
II_UPD_05	Prüfung, ob die Funktionalität für die Aktualisierung einer Transaktion bis zu 100 Zeichen für die Art des Vorgangs akzeptiert. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_UPD_06	Prüfung, ob die Funktionalität für die Aktualisierung einer Transaktion vorherige Aktualisierungen sichert, wenn eine Aktualisierung mit einer anderen Seriennummer des Aufzeichnungssystems erfolgt. Zusätzlich wird die erstellte Log-Nachricht auf Format und Inhalt geprüft.	SM_AGG	PT
II_UPD_07	Prüfung, ob die Funktionalität für die Aktualisierung einer Transaktion vorherige Aktualisierungen sichert, wenn eine Aktualisierung mit einer anderen Art des Vorgangs erfolgt. Zusätzlich wird die erstellte Log-Nachricht auf Format und Inhalt geprüft.	SM_AGG	PT
II_UPD_08	Prüfung, ob die Funktionalität für die Aktualisierung einer Transaktion eine Aktualisierung einer Transaktion sichert, wenn nach längerer Zeit (MAX_PROTECTION_DELAY) keine weitere Aktualisierung vorgenommen wurde. Zusätzlich wird die erstellte Log-Nachricht auf Format und Inhalt geprüft.	SM_AGG	PT
II_UPD_09	Prüfung, ob die Funktionalität für die Aktualisierung einer Transaktion überprüft, ob die übergebene Seriennummer des Aufzeichnungssystems registriert ist, damit diese für die Aufzeichnung von Transaktionen verwendet werden kann. Die übergebene Seriennummer des Aufzeichnungssystems wurde zuvor noch nie registriert.	II	NT
II_UPD_10	Prüfung, ob die Fehlermeldung ErrorUpdateTransactionFailed ausgelöst wird, wenn die Funktionalität für die Aktualisierung einer Transaktion ohne direkte Erstellung einer Log-Nachricht fehlschlägt.	SM_AGG	NT

Tabelle 74: Testfälle für die Einbindungsschnittstelle – Aktualisieren einer Transaktion

6.3.1.31 Beenden einer Transaktion (II_FIN)

ID	Zielsetzung	Profile	Typ
II_FIN_01	<p>Prüfung, ob die Funktionalität zum Beenden einer Transaktion die folgenden Aktionen durchführt:</p> <ul style="list-style-type: none"> • Abfragen der Log-Nachricht-Teile vom Sicherheitsmodul • Speicherung der Log-Nachricht-Teile im Speichermedium • Rückgabe der folgenden Daten: <ul style="list-style-type: none"> ○ Information, dass keine Log-Nachricht für eine vorherige Aktualisierung erstellt wurde ○ Zeitpunkt der Beendigung ○ Prüfwert ○ Signaturzähler ○ Keine weiteren Daten <p>Der Test übergibt beim Aufruf der Funktion die</p> <ul style="list-style-type: none"> • Seriennummer des Aufzeichnungssystems, • Transaktionsnummer, • Daten des Vorgangs und • Art des Vorgangs. <p>Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht für die Beendigung der Transaktion und, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II	PT

ID	Zielsetzung	Profile	Typ
II_FIN_02	<p>Prüfung, ob die Funktionalität zum Beenden einer Transaktion die folgenden Aktionen durchführt:</p> <ul style="list-style-type: none"> • Sicherung von vorherigen bisher ungesicherten Aktualisierungen der Transaktion • Abfragen der Log-Nachricht-Teile vom Sicherheitsmodul • Speicherung der Log-Nachricht-Teile im Speichermedium • Rückgabe der folgenden Daten: <ul style="list-style-type: none"> ○ Information, dass eine Log-Nachricht für eine vorherige Aktualisierung erstellt wurde ○ Zeitpunkt der Aktualisierung ○ Prüfwert der Log-Nachricht für die Aktualisierung ○ Signaturzählerstand nach Erstellung der Log-Nachricht für die Aktualisierung ○ Zeitpunkt der Beendigung ○ Prüfwert der Log-Nachricht für die Beendigung ○ Signaturzähler nach Erstellung der Log-Nachricht für die Beendigung <p>Der Test übergibt beim Aufruf der Funktion die</p> <ul style="list-style-type: none"> • Seriennummer des Aufzeichnungssystems, • Transaktionsnummer, • Daten des Vorgangs und • Art des Vorgangs. <p>Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachrichten für die Aktualisierung und die Beendigung der Transaktion und, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II SM_AGG	PT
II_FIN_03	<p>Prüfung, ob die Funktionalität zum Beenden einer Transaktion bis zu 100 Zeichen für die Art des Vorgangs akzeptiert. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II	PT
II_FIN_04	<p>Prüfung, ob die Funktionalität zum Beenden einer Transaktion eine Fehlermeldung auslöst, wenn eine Transaktionsnummer übergeben wird, die noch nicht vergeben wurde.</p>	II	NT
II_FIN_05	<p>Prüfung, ob die Funktionalität zum Beenden einer Transaktion eine Fehlermeldung auslöst, wenn eine Transaktionsnummer übergeben wird, die zu einer bereits beendeten Transaktion gehört.</p>	II	NT

ID	Zielsetzung	Profile	Typ
II_FIN_06	Prüfung, ob die Funktionalität zum Beenden einer Transaktion überprüft, ob die übergebene Seriennummer des Aufzeichnungssystems registriert ist, und somit für die Aufzeichnung von Transaktionen verwendet werden kann. Die übergebene Seriennummer des Aufzeichnungssystems wurde zuvor noch nie registriert.	II	NT

Tabelle 75: Testfälle für die Einbindungsschnittstelle – Beenden einer Transaktion

6.3.1.32 Export von Transaktions-Log-Nachrichten (II_EXF)

ID	Zielsetzung	Profile	Typ
II_EXF_01	Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten bei einem Aufruf mit dem Eingabeparameter transactionNumber die folgende Aktion durchführt: <ul style="list-style-type: none"> Export von Log-Nachrichten, für die übergebene Transaktionsnummer. <p>In dem Intervall von der Log-Nachricht für den Start der Transaktion und der Log-Nachricht für die Beendigung der Transaktion sind ausschließlich Transaktions-Log-Nachrichten enthalten.</p>	II_EXPORTFILTERED	PT
II_EXF_02	Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten bei einem Aufruf mit dem Eingabeparameter transactionNumber die folgende Aktion durchführt: <ul style="list-style-type: none"> Export von Log-Nachrichten für die übergebene Transaktionsnummer. <p>In dem Intervall von der Log-Nachricht für den Start der Transaktion und der Log-Nachricht für die Beendigung der Transaktion sind auch System-Log-Nachrichten und Audit-Log-Nachrichten enthalten.</p>	II_EXPORTFILTERED	PT
II_EXF_03	Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit dem Eingabeparameter transactionNumber. Es wird geprüft, ob die Fehlermeldung ErrorTransactionNumberNotFound ausgelöst wird, wenn im Speichermedium keine Log-Nachrichten für die Transaktionsnummer gefunden werden.	II_EXPORTFILTERED	NT

ID	Zielsetzung	Profile	Typ
II_EXF_04	<p>Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten bei einem Aufruf mit den Eingabeparametern transactionNumber und clientId die folgende Aktion durchführt:</p> <ul style="list-style-type: none"> Export von Log-Nachrichten für die Transaktionsnummer und Client-ID. <p>In dem Intervall von der Log-Nachricht für den Start der Transaktion und der Log-Nachricht für die Beendigung der Transaktion sind ausschließlich Transaktions-Log-Nachrichten enthalten.</p>	II_EXPORTFILTERED	PT
II_EXF_05	<p>Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten bei einem Aufruf mit den Eingabeparametern transactionNumber und clientId die folgende Aktion durchführt:</p> <ul style="list-style-type: none"> Export von Log-Nachrichten für die übergebene Transaktionsnummer und Client-ID. <p>In dem Intervall von der Log-Nachricht für den Start der Transaktion und der Log-Nachricht für die Beendigung der Transaktion sind auch System-Log-Nachrichten und Audit-Log-Nachrichten enthalten.</p>	II_EXPORTFILTERED	PT
II_EXF_06	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern transactionNumber und clientId.</p> <p>Es wird geprüft, ob die Funktion die Fehlermeldung Error-TransactionNumberNotFound auslöst, wenn keine Log-Nachrichten für die Transaktionsnummer gefunden werden.</p>	II_EXPORTFILTERED	NT
II_EXF_07	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern transactionNumber und clientId.</p> <p>Es wird geprüft, ob die Funktion die Fehlermeldung ErrorClientIdNotFound auslöst, wenn keine Log-Nachrichten für die Client-ID gefunden werden.</p>	II_EXPORTFILTERED	NT

ID	Zielsetzung	Profile	Typ
II_EXF_08	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber und • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob die Funktion nur Log-Nachrichten exportiert, die im Intervall von firstTransactionNumber und lastTransactionNumber liegen.</p> <p>In dem Intervall sind ausschließlich Transaktions-Log-Nachrichten enthalten.</p>	II_EXPORTFILTERED	PT
II_EXF_09	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber und • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob die Funktion nur Log-Nachrichten exportiert, die im Intervall von firstTransactionNumber und lastTransactionNumber liegen.</p> <p>In dem Intervall sind neben den Transaktions-Log-Nachrichten zusätzlich System-Log-Nachrichten und Audit-Log-Nachrichten enthalten.</p>	II_EXPORTFILTERED	PT
II_EXF_10	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber • clientId und • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob die Funktion nur Log-Nachrichten exportiert, die im Intervall von firstTransactionNumber und lastTransactionNumber liegen. In Bezug auf exportierte Transaktions-Log-Nachrichten wird zusätzlich geprüft, ob diese zu der übergebenen clientId korrespondieren.</p> <p>In dem Intervall sind ausschließlich Transaktions-Log-Nachrichten enthalten.</p>	II_EXPORTFILTERED	PT

ID	Zielsetzung	Profile	Typ
II_EXF_11	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber • clientId und • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob die Funktion nur Log-Nachrichten exportiert, die im Intervall von firstTransactionNumber und lastTransactionNumber liegen. In Bezug auf exportierte Transaktions-Log-Nachrichten wird zusätzlich geprüft, ob diese zu der übergebenen clientId korrespondieren.</p> <p>In dem Intervall sind neben Transaktions-Log-Nachrichten zusätzlich System-Log-Nachrichten und Audit-Log-Nachrichten enthalten.</p>	II_EXPORTFILTERED	PT
II_EXF_12	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber und • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob die Fehlermeldung ErrorTransactionNumberNotFound ausgelöst wird, wenn keine Log-Nachricht gefunden wird, die im Intervall aus firstTransactionNumber und lastTransactionNumber enthalten ist.</p>	II_EXPORTFILTERED	NT
II_EXF_13	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber • clientId und • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob die Fehlermeldung ErrorClientIdNotFound ausgelöst wird, wenn keine Log-Nachricht zu der übergebenen Client-ID gefunden wird, die im Intervall aus firstTransactionNumber und lastTransactionNumber enthalten ist.</p>	II_EXPORTFILTERED	NT

ID	Zielsetzung	Profile	Typ
II_EXF_14	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber • maximumNumberRecords mit einem Wert größer 0. <p>Die Anzahl der angeforderten Log-Nachrichten ist kleiner als der Wert von maximumNumberRecords.</p> <p>Es wird geprüft, ob die Funktion Log-Nachrichten exportiert, die in dem Intervall von firstTransactionNumber und lastTransactionNumber liegen.</p>	II_EXPORTFILTERED	PT
II_EXF_15	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit den Eingabeparametern</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber • maximumNumberRecords mit einem Wert größer 0. <p>Die Anzahl der angeforderten Log-Nachrichten ist gleich dem Wert von maximumNumberRecords.</p> <p>Es wird geprüft, ob die Funktion Log-Nachrichten exportiert, die in dem Intervall von firstTransactionNumber und lastTransactionNumber liegen.</p>	II_EXPORTFILTERED	PT
II_EXF_16	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • firstTransactionNumber • lastTransactionNumber • maximumNumberRecords mit einem Wert größer 0. <p>Es wird geprüft, ob die Fehlermeldung ErrorTooManyRecords ausgelöst wird, wenn die Anzahl der angeforderten Log-Nachrichten größer als der Wert von maximumNumberRecords ist.</p>	II_EXPORTFILTERED	NT

ID	Zielsetzung	Profile	Typ
II_EXF_17	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter:</p> <ul style="list-style-type: none"> • startDate • endDate • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen startDate und endDate liegen.</p> <p>In dem Zeitraum liegen ausschließlich Transaktions-Log-Nachrichten.</p>	II_EXPORTFILTERED	PT
II_EXF_18	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • startDate • endDate • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen startDate und endDate liegen.</p> <p>In dem Zeitraum liegen zusätzlich zu Transaktions-Log-Nachrichten auch System-Log-Nachrichten und Audit-Log-Nachrichten.</p>	II_EXPORTFILTERED	PT
II_EXF_19	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • startDate • endDate • clientId • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen startDate und endDate liegen. Für exportierte Transaktions-Log-Nachrichten wird zusätzlich geprüft, ob diese zu der übergebenen clientId korrespondieren.</p>	II_EXPORTFILTERED	PT

ID	Zielsetzung	Profile	Typ
II_EXF_20	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • startDate • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen startDate und dem aktuellsten Erstellungsdatum einer Log-Nachricht liegen.</p>	II_EXPORTFIL-TERED	PT
II_EXF_21	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • startDate • clientId • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen startDate und dem aktuellsten Erstellungsdatum einer Log-Nachricht liegen. Für exportierte Transaktions-Log-Nachrichten wird zusätzlich geprüft, ob diese zu der übergebenen clientId korrespondieren.</p>	II_EXPORTFIL-TERED	PT
II_EXF_22	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • endDate • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen dem ältesten Erstellungsdatum einer Log-Nachricht und endDate liegen.</p>	II_EXPORTFIL-TERED	PT

ID	Zielsetzung	Profile	Typ
II_EXF_23	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • endDate • clientId • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen dem ältesten Erstellungsdatum einer Log-Nachricht und endDate liegen. Für exportierte Transaktions-Log-Nachrichten wird zusätzlich geprüft, ob diese zu der übergebenen clientId korrespondieren.</p>	II_EXPORTFILTERED	PT
II_EXF_24	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • startDate • endDate • maximumNumberRecords mit einem Wert größer 0. <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen startDate und endDate liegen. Die Anzahl der angeforderten Log-Nachrichten soll kleiner als der Wert für maximumNumberRecords sein.</p>	II_EXPORTFILTERED	PT
II_EXF_25	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter</p> <ul style="list-style-type: none"> • startDate • endDate • maximumNumberRecords mit einem Wert größer 0 <p>Es wird geprüft, ob nur die Log-Nachrichten exportiert werden, die in dem Zeitraum zwischen startDate und endDate liegen. Die Anzahl der angeforderten Log-Nachrichten soll gleich dem Wert für maximumNumberRecords sein.</p>	II_EXPORTFILTERED	PT

ID	Zielsetzung	Profile	Typ
II_EXF_26	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter:</p> <ul style="list-style-type: none"> • startDate • endDate • maximumNumberRecords mit dem Wert 0. <p>Es wird geprüft, ob die Fehlermeldung ErrorNoDataAvailable ausgelöst wird, wenn keine Log-Nachricht gefunden wird, die in dem Zeitraum zwischen startDate und endDate liegt.</p>	II_EXPORTFILTERED	NT
II_EXF_27	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter:</p> <ul style="list-style-type: none"> • startDate • endDate • clientId • maximumNumberRecords mit dem Wert 0 <p>Es wird geprüft, ob die Fehlermeldung ErrorClientIdNotFound ausgelöst wird, wenn keine Transaktions-Log-Nachricht zu der übergebenen clientId gefunden wird, die in dem Zeitraum zwischen startDate und endDate liegt.</p>	II_EXPORTFILTERED	NT
II_EXF_28	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter:</p> <ul style="list-style-type: none"> • startDate, • endDate, • maximumNumberRecords mit einem Wert größer 0. <p>Es wird geprüft, ob die Fehlermeldung ErrorTooManyRecords ausgelöst wird, wenn die Anzahl der angeforderten Log-Nachrichten größer ist, als der Wert von maximumNumberRecords.</p>	II_EXPORTFILTERED	NT

ID	Zielsetzung	Profile	Typ
II_EXF_29	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter:</p> <ul style="list-style-type: none"> • startDate, • endDate, • maximumNumberRecords mit dem Wert 0. <p>Der Wert für startDate liegt zeitlich hinter dem Wert für endDate.</p> <p>Es wird geprüft, ob die Fehlermeldung ErrorParameterMismatch ausgelöst wird.</p>	II_EXPORTFILTERED	NT
II_EXF_30	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter:</p> <ul style="list-style-type: none"> • startDate, • endDate, • maximumNumberRecords. <p>Der Wert für endDate enthält keinen gültigen Zeitpunkt.</p> <p>Es wird geprüft, ob die Fehlermeldung ErrorParameterMismatch ausgelöst wird.</p>	II_EXPORTFILTERED	NT
II_EXF_31	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit Werten für die Eingabeparameter:</p> <ul style="list-style-type: none"> • startDate, • endDate, • maximumNumberRecords. <p>Der Wert für startDate enthält keinen gültigen Zeitpunkt.</p> <p>Es wird geprüft, ob die Fehlermeldung ErrorParameterMismatch ausgelöst wird.</p>	II_EXPORTFILTERED	NT
II_EXF_32	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit dem Wert 0 für den Eingabeparameter maximumNumberRecords.</p> <p>Es ist eine Transaktions-Log-Nachricht im Speichermedium enthalten.</p> <p>Es wird geprüft, ob alle Log-Nachrichten, die sich im Speichermedium befinden, exportiert werden.</p>	II_EXPORTFILTERED	PT

ID	Zielsetzung	Profile	Typ
II_EXF_33	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit dem Wert 0 für den Eingabeparameter maximumNumberRecords.</p> <p>Es sind mehrere Transaktions-Log-Nachrichten im Speichermedium enthalten.</p> <p>Es wird geprüft, ob alle Log-Nachrichten, die sich im Speichermedium befinden, exportiert werden.</p>	II_EXPORTFILTERED	PT
II_EXF_34	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit einem Wert größer 0 für den Eingabeparameter maximumNumberRecords.</p> <p>Die Anzahl der angeforderten Log-Nachrichten ist kleiner als der Wert für maximumNumberRecords.</p> <p>Es wird geprüft, ob alle Log-Nachrichten, die sich im Speichermedium befinden, exportiert werden.</p>	II_EXPORTFILTERED	PT
II_EXF_35	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit einem Wert größer 0 für den Eingabeparameter maximumNumberRecords.</p> <p>Die Anzahl der angeforderten Log-Nachrichten ist gleich dem Wert für maximumNumberRecords.</p> <p>Es wird geprüft, ob alle Log-Nachrichten, die sich im Speichermedium befinden, exportiert werden.</p>	II_EXPORTFILTERED	PT
II_EXF_36	<p>Der Test betrachtet einen Aufruf der Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten mit einem Wert größer 0 für den Eingabeparameter maximumNumberRecords.</p> <p>Es wird geprüft, ob die Fehlermeldung ErrorTooManyRecords ausgelöst wird, wenn die Anzahl der angeforderten Log-Nachrichten größer ist, als der Wert für maximumNumberRecords.</p>	II_EXPORTFILTERED	NT
II_EXF_37	<p>Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten eine Fehlermeldung ausgibt, wenn nur ein Parameter von firstTransactionNumber und lastTransactionNumber übergeben wird.</p>	II_EXPORTFILTERED	NT

ID	Zielsetzung	Profile	Typ
II_EXF_38	Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten einen korrekten Namen für den TAR-Container ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.	II_EXPORTFIL- TERED	PT
II_EXF_39	Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten eine Fehlermeldung ausgibt, wenn zusätzlich zum Parameter transactionNumber auch startDate oder endDate übergeben werden.	II_EXPORTFIL- TERED	PT
II_EXF_40	Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten eine Fehlermeldung ausgibt, wenn zusätzlich zu den Parametern firstTransactionNumber und lastTransactionNumber auch startDate oder endDate übergeben werden.	II_EXPORTFIL- TERED	PT
II_EXF_41	Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten für einen gefilterten Export erfolgreich aufgerufen werden kann, wenn die Zeit nicht gestellt ist.	II_EXPORTFIL- TERED II_UPDATETIME NO_CENTRAL_TIME	PT
II_EXF_42	Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten für einen gefilterten Export erfolgreich aufgerufen werden kann, wenn die Verbindung zu einem Teil des Sicherheitsmoduls getrennt ist.	II_EXPORTFILTERED SM_REMOTE_COM- PONENTS	PT
II_EXF_43	Prüfung, ob die Funktionalität zum gefilterten Export von Transaktions-Log-Nachrichten für einen gefilterten Export erfolgreich aufgerufen werden kann, wenn das Sicherheitsmodul deaktiviert ist.	II_EXPORTFIL- TERED	PT

Tabelle 76: Testfälle für die Einbindungsschnittstelle – gefilterter Export von Transaktions-Log-Nachrichten

6.3.1.33 Abfrage der unterstützten Varianten für die Aktualisierung von Transaktionen (II_UTV)

ID	Zielsetzung	Profile	Typ
II_UTV_01	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können, zurückgibt, die unterstützten Varianten für die Aktualisierung von Transaktionen im Sicherheitsmodul repräsentiert.</p> <p>Die Prüfung des zurückgegebenen Wertes erfolgt gegen die angegebenen Varianten im ICS und das tatsächliche Verhalten der Funktionalität für die Aktualisierung der Transaktion.</p> <p>Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II	PT
II_UTV_01	<p>Prüfung, ob die Funktionalität zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können, die Fehlermeldung ErrorGetSupportedUpdateVariantsFailed ausgibt, wenn die unterstützten Varianten für die Aktualisierung von Transaktionen im Sicherheitsmodul nicht festgestellt werden können.</p>	II	NT

Tabelle 77: Testfälle für die Einbindungsschnittstelle – Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können

6.3.1.34 Abfrage der aktuellen Anzahl von Aufzeichnungssystemen der Technischen Sicherheitseinrichtung (II_CNC)

ID	Zielsetzung	Profile	Typ
II_CNC_01	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der Anzahl von Aufzeichnungssystemen zurückgibt, dem Wert für die aktuelle Anzahl von Aufzeichnungssystemen der TSE entspricht. Die Aufzeichnungssysteme sind hierbei aktuell an nicht beendeten Transaktionen beteiligt.</p> <p>Die TSE wird von keinem Aufzeichnungssystem für die Protokollierung von Transaktionen verwendet.</p> <p>Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II_CURNOCLIENTS	PT

ID	Zielsetzung	Profile	Typ
II_CNC_02	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der Anzahl von Aufzeichnungssystemen zurückgibt, dem Wert für die aktuelle Anzahl von Aufzeichnungssystemen der TSE entspricht. Die Aufzeichnungssysteme sind hierbei aktuell an nicht beendeten Transaktionen beteiligt.</p> <p>Die TSE wird von einem Aufzeichnungssystem für die Protokollierung von Transaktionen verwendet.</p> <p>Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II_CURNOCLIENTS	PT
II_CNC_03	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der Anzahl von Aufzeichnungssystemen zurückgibt, dem Wert für die aktuelle Anzahl von Aufzeichnungssystemen der TSE entspricht. Die Aufzeichnungssysteme sind hierbei aktuell an nicht beendeten Transaktionen beteiligt.</p> <p>Die TSE wird von mehreren Aufzeichnungssystemen für die Protokollierung von Transaktionen genutzt. Die Anzahl von Aufzeichnungssystemen ist hierbei kleiner als die maximale Anzahl von Aufzeichnungssystemen, die im ICS angegeben wird.</p> <p>Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II_CURNOCLIENTS MULTI_CLIENT	PT
II_CNC_04	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der Anzahl von Aufzeichnungssystemen zurückgibt, dem Wert für die aktuelle Anzahl von Aufzeichnungssystemen der TSE entspricht. Die Aufzeichnungssysteme sind hierbei aktuell an nicht beendeten Transaktionen beteiligt.</p> <p>Die TSE wird von der maximalen Anzahl von Aufzeichnungssystemen, die im ICS angegeben wird, für die Protokollierung von Transaktionen verwendet. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.</p>	II_CURNOCLIENTS MULTI_CLIENT LIMITED_CLIENTS_TRACKED	PT

ID	Zielsetzung	Profile	Typ
II_CNC_05	Prüfung, ob die Funktionalität zur Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind, die Fehlermeldung ErrorCurrentNumberOfClientsNotTracked ausgibt, wenn eine unbegrenzte Anzahl an Aufzeichnungssystemen unterstützt aber die aktuelle Anzahl der Aufzeichnungssysteme nicht nachgehalten wird.	II_CURNOCLIENTS MULTI_CLIENT UNLIMITED_CLIENTS _NOT_TRACKED	NT
II_CNC_06	Prüfung, ob die Funktionalität zur Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind, die Fehlermeldung ErrorGetCurrentNumberOfClientsFailed ausgibt, wenn der Wert für die aktuelle Anzahl von Aufzeichnungssystemen der TSE nicht festgestellt werden kann.	II_CURNOCLIENTS	

Tabelle 78: Testfälle für die Einbindungsschnittstelle – Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind

6.3.1.35 Abfrage der maximalen Anzahl von simultanen Aufzeichnungssystemen der Technischen Sicherheitseinrichtung (II_MNC)

ID	Zielsetzung	Profile	Typ
II_MNC_01	Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können, zurückgibt, dem Wert für die maximale Anzahl von simultanen Aufzeichnungssystemen entspricht, der im ICS angegeben wird. Zusätzlich wird geprüft, ob die Ausführung ohne Fehlermeldung beendet wird.	II_MAXNOCLIENTS	PT
II_MNC_02	Prüfung, ob die Funktionalität zur Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können, die Fehlermeldung ErrorGetMaxNumberOfClientsFailed ausgibt, wenn der Wert für die maximale Anzahl von simultanen Aufzeichnungssystemen nicht festgestellt werden kann.	II_MAXNOCLIENTS	PT

Tabelle 79: Testfälle für die Einbindungsschnittstelle – Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können

6.3.1.36 Abfrage zu registrierten Aufzeichnungssystemen (II_GRC)

ID	Zielsetzung	Profile	Typ
II_GRC_01	Prüfung, ob die Funktionalität zur Ausgabe der aktuell registrierten Aufzeichnungssysteme die Seriennummern der aktuell registrierten Aufzeichnungssysteme im richtigen Format ausgibt. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II_REGISTEREDCLIENTS	PT
II_GRC_02	Prüfung, ob die Funktionalität zur Ausgabe der aktuell registrierten Aufzeichnungssysteme die Seriennummern der aktuell registrierten Aufzeichnungssysteme ausgibt, wenn die maximale Anzahl an möglichen Aufzeichnungssystemen gleichzeitig registriert ist. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II_REGISTEREDCLIENTS	PT
II_GRC_03	Prüfung, ob die Funktionalität zur Ausgabe der aktuell registrierten Aufzeichnungssysteme die Seriennummern der aktuell registrierten Aufzeichnungssysteme ausgibt, wenn kein Aufzeichnungssystem registriert ist. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II_REGISTEREDCLIENTS	PT
II_GRC_04	Prüfung, ob die Funktionalität zur Ausgabe der aktuell registrierten Aufzeichnungssysteme die Seriennummern der aktuell registrierten Aufzeichnungssysteme ausgibt, wenn weniger als die maximale Anzahl an möglichen Aufzeichnungssystemen (mehr als 0) gleichzeitig registriert ist. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II_REGISTEREDCLIENTS	PT
II_GRC_05	Prüfung, ob die Funktionalität zur Ausgabe der aktuell registrierten Aufzeichnungssysteme die Fehlermeldung Error-GetRegisteredClientsFailed ausgibt, wenn die Seriennummern der aktuell registrierten Aufzeichnungssysteme nicht festgestellt werden können.	II_REGISTEREDCLIENTS	NT

Tabelle 80: Testfälle für die Einbindungsschnittstelle – Abfrage zu registrierten Aufzeichnungssystemen

6.3.1.37 Abfrage der aktuellen Anzahl von parallel geöffneten Transaktionen (II_CNT)

ID	Zielsetzung	Profile	Typ
II_CNT_01	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der Anzahl von offenen Transaktionen zurückgibt, der aktuellen Anzahl von parallel geöffneten Transaktionen entspricht, die im Sicherheitsmodul verwaltet werden.</p> <p>Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.</p> <p>Es wird keine Transaktion im Sicherheitsmodul verwaltet.</p>	II_CURNOTRANSAC-TIONS	PT
II_CNT_02	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der Anzahl von offenen Transaktionen zurückgibt, der aktuellen Anzahl von parallel geöffneten Transaktionen entspricht, die im Sicherheitsmodul verwaltet werden.</p> <p>Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.</p> <p>Es wird eine offene Transaktion im Sicherheitsmodul verwaltet.</p>	II_CURNOTRANSAC-TIONS	PT
II_CNT_03	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der Anzahl von offenen Transaktionen zurückgibt, der aktuellen Anzahl von parallel geöffneten Transaktionen entspricht, die im Sicherheitsmodul verwaltet werden.</p> <p>Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.</p> <p>Es werden mehrere offene Transaktionen im Sicherheitsmodul verwaltet. Die Anzahl der Transaktionen ist kleiner als die maximale Anzahl von Transaktionen, die im ICS angegeben wird.</p>	II_CURNOTRANSAC-TIONS SM_MULTI	PT
II_CNT_04	<p>Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der Anzahl von offenen Transaktionen zurückgibt, der aktuellen Anzahl von parallel geöffneten Transaktionen entspricht, die im Sicherheitsmodul verwaltet werden.</p> <p>Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.</p> <p>Die Anzahl der offene Transaktionen, die im Sicherheitsmodul verwaltet werden, entspricht der maximalen Anzahl von Transaktionen, die im ICS angegeben wird.</p>	II_CURNOTRANSAC-TIONS SM_MULTI	PT

ID	Zielsetzung	Profile	Typ
II_CNT_05	Prüfung, ob die Funktionalität zur Ausgabe der Anzahl von offenen Transaktionen die Fehlermeldung ErrorGetCurrentNumberOfTransactionsFailed ausgibt, wenn die aktuelle Anzahl von parallel geöffneten Transaktionen, die im Sicherheitsmodul verwaltet werden, nicht festgestellt werden kann.	II_CURNOTRANSAC-TIONS	NT

Tabelle 81: Testfälle für die Einbindungsschnittstelle – Ausgabe der Anzahl von offenen Transaktionen

6.3.1.38 Abfrage der maximalen Anzahl von parallelen Transaktionen (II_MNT)

ID	Zielsetzung	Profile	Typ
II_MNT_01	Prüfung, ob der Wert, den die Funktionalität zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können, zurückgibt, dem Wert für die maximale Anzahl von parallelen Transaktionen entspricht, die im Sicherheitsmodul verwaltet werden können. Die Prüfung des zurückgegebenen Wertes erfolgt gegen den Wert, der im ICS angegeben wird. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.	II_MAXNOT-RANSAC-TIONS	PT
II_MNT_02	Prüfung, ob die Funktionalität zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können, die Fehlermeldung ErrorGetMaxNumberTransactionsFailed ausgibt, wenn die maximalen Anzahl von parallel geöffneten Transaktionen, die im Sicherheitsmodul verwaltet werden, nicht festgestellt werden kann.	II_MAXNOT-RANSAC-TIONS	NT

Tabelle 82: Testfälle für die Einbindungsschnittstelle – Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig verwaltet werden können

6.3.1.39 Abfrage zum Stadium einer Transaktion (II_GTS)

ID	Zielsetzung	Profile	Typ
II_GTS_01	Prüfung, ob die Funktionalität zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet den korrekten Zustand von Transaktionen ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird.	II_TRANSACTIONS-TATE	PT

ID	Zielsetzung	Profile	Typ
II_GTS_02	Prüfung, ob die Funktionalität zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet überprüft, ob eine Transaktion mit der übergebenen Transaktionsnummer existiert. Wenn keine Transaktion mit der übergebenen Transaktionsnummer verwaltet wird, muss die Funktion die Fehlermeldung <code>ErrorTransactionNumberNotFound</code> auslösen und die Funktion beenden.	II_TRANSACTIONS-TATE	NT
II_GTS_03	Prüfung, ob die Funktionalität zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet die Fehlermeldung <code>ErrorGetTransactionStateFailed</code> ausgibt, wenn das Stadium der angefragten Transaktion nicht festgestellt werden kann.	II_TRANSACTIONS-TATE	NT

Tabelle 83: Testfälle für die Einbindungsschnittstelle – Ausgabe des Stadiums in welchem sich eine Transaktion befindet

6.3.1.40 Abfrage der Transaktionsnummern aller nicht beendeten Transaktionen (II_GOT)

ID	Zielsetzung	Profile	Typ
II_GOT_01	Prüfung, ob die Funktionalität zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen die Transaktionsnummern aller offenen Transaktionen im richtigen Format ausgibt. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II_OPENTRANSAC-TIONS	PT
II_GOT_02	Prüfung, ob die Funktionalität zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen die Transaktionsnummern aller offenen Transaktionen ausgibt, wenn aktuell eine Transaktion offen ist. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II_OPENTRANSAC-TIONS	PT
II_GOT_03	Prüfung, ob die Funktionalität zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen die Transaktionsnummern aller offenen Transaktionen ausgibt, wenn die Anzahl der offenen Transaktionen der maximalen Anzahl der parallel geöffneten Transaktionen entspricht, die das Sicherheitsmodul verwalten kann. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II_OPENTRANSAC-TIONS	PT

ID	Zielsetzung	Profile	Typ
II_GOT_04	Prüfung, ob die Funktionalität zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen die Transaktionsnummern aller offenen Transaktionen ausgibt, wenn aktuell keine Transaktion offenen ist. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II_OPENTRANSAC-TIONS	PT
II_GOT_05	Prüfung, ob die Funktionalität zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen die Fehlermeldung ErrorGetOpenTransactionsFailed ausgibt, wenn die Transaktionsnummern aller offenen Transaktionen nicht festgestellt werden können.	II_OPENTRANSAC-TIONS	NT

Tabelle 84: Testfälle für die Einbindungsschnittstelle – Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen

6.3.1.41 Abfrage zum aktuellen Transaktionszählers (II_CTC)

ID	Zielsetzung	Profile	Typ
II_CTC_01	Prüfung, ob die Funktionalität zur Ausgabe des aktuellen Stands des Transaktionszählers eine korrekte Ausgabe liefert, wenn noch keine Transaktion gestartet wurde. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_CTC_02	Prüfung, ob die Funktionalität zur Ausgabe des aktuellen Stands des Transaktionszählers die Transaktionsnummer der zuletzt gestarteten Transaktion ausgibt, wenn schon mehrere Transaktionen gestartet wurden. Zusätzlich wird geprüft ob die Ausführung ohne Fehlermeldung beendet wird.	II	PT
II_CTC_03	Prüfung, ob die Funktionalität zur Ausgabe des aktuellen Stands des Transaktionszählers die Fehlermeldung ErrorGetCurrentTransactionCounterFailed ausgibt, wenn die Transaktionsnummer der zuletzt gestarteten Transaktion nicht festgestellt werden kann.	II	NT

Tabelle 85: Testfälle für die Einbindungsschnittstelle – Ausgabe des aktuellen Stands des Transaktionszählers

6.3.1.42 Ausgabe der letzten Transaktions-Log-Nachricht (II_GLT)

ID	Zielsetzung	Profile	Typ
II_GLT_01	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht die zuletzt erstellte Transaktions-Log-Nachricht und einen korrekten Namen für diese Log-Nachricht ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird. Es wird keine Transaktionsnummer übergeben . Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion nicht aggregieren.	II_LASTTRANSLOG SM_NOAGG	PT
II_GLT_02	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht die zuletzt erstellte Transaktions-Log-Nachricht und einen korrekten Namen für diese Log-Nachricht ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird. Es wird keine Transaktionsnummer übergeben . Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion aggregieren .	II_LASTTRANSLOG SM_AGG	PT
II_GLT_03	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht die zuletzt erstellte Transaktions-Log-Nachricht und einen korrekten Namen für diese Log-Nachricht ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird. Es wird eine Transaktionsnummer übergeben . Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion nicht aggregieren.	II_LASTTRANSLOG SM_NOAGG	PT
II_GLT_04	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht die zuletzt erstellte Transaktions-Log-Nachricht und einen korrekten Namen für diese Log-Nachricht ausgibt. Zusätzlich erfolgt eine Prüfung, ob die Ausführung ohne Fehlermeldung beendet wird. Es wird eine Transaktionsnummer übergeben . Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion aggregieren .	II_LASTTRANSLOG SM_AGG	PT
II_GLT_05	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht beendet wird und die Fehlermeldung ErrorNoLogMessageFound ausgibt, wenn für die übergebene Transaktionsnummer keine Log-Nachrichten vorliegen.	II_LASTTRANSLOG	NT

ID	Zielsetzung	Profile	Typ
II_GLT_06	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht beendet wird und die Fehlermeldung ErrorNoLogMessageFound ausgibt, wenn keine Transaktionsnummer übergeben wird und keine Log-Nachrichten vorliegen.	II_LASTTRANSLOG	NT
II_GLT_07	Prüfung, ob die Funktionalität zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht beendet wird und die Fehlermeldung ErrorReadingLogMessage ausgibt, wenn die zuletzt erzeugte Transaktions-Log-Nachricht nicht ausgegeben werden kann.	II_LASTTRANSLOG	NT

Tabelle 86: Testfälle für die Einbindungsschnittstelle – Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht

6.3.1.43 Sperren von Log-Nachrichten von Transaktionen (II_LTL)

ID	Zielsetzung	Profile	Typ
II_LTL_01	Prüfung, ob die Funktionalität zur Unterbindung der Aufzeichnung von Transaktionen das Ausführen der Funktionalitäten für das Starten, für die Aktualisierung und zum Beenden von Transaktion unterbindet. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.	II_LOCKTRANSLOGGING	PT
II_LTL_02	Prüfung, ob die Funktionalität zur Unterbindung der Aufzeichnung von Transaktionen mit einem Fehler beendet wird, wenn offene, noch nicht verwaiste Transaktionen im Speicher liegen.	II_LOCKTRANSLOGGING	NT
II_LTL_03	Prüfung, ob die Funktionalität zur Unterbindung der Aufzeichnung von Transaktionen beendet wird und die Fehlermeldung ErrorLockTransactionLoggingFailed ausgibt, wenn das Ausführen der Funktionalitäten für das Starten, für die Aktualisierung und zum Beenden von Transaktion nicht unterbunden werden kann.	II_LOCKTRANSLOGGING	NT

Tabelle 87: Testfälle für die Einbindungsschnittstelle – Unterbindung der Aufzeichnung von Transaktionen

6.3.1.44 Entsperrern von Log-Nachrichten von Transaktionen (II_UTL)

ID	Zielsetzung	Profile	Typ
II_UTL_01	Prüfung, ob die Funktionalität zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger das Ausführen der Funktionalitäten für das Starten, für die Aktualisierung und zum Beenden von Transaktion ermöglicht. Zusätzlich erfolgt eine Prüfung der erstellten Log-Nachricht und, ob die Ausführung ohne Fehlermeldung beendet wird.	II_UNLOCK- TRANSLOGGING	PT
II_UTL_02	Prüfung, ob die Funktionalität zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger mit einem Fehler beendet wird, wenn die Protokollierung von Transaktionen aktuell nicht gesperrt ist.	II_UNLOCK- TRANSLOGGING	NT
II_UTL_03	Prüfung, ob die Funktionalität zur Ermöglichung der Aufzeichnung von Transaktionen beendet wird und die Fehlermeldung <code>ErrorUnlockTransactionLoggingFailed</code> ausgibt, wenn das Ausführen der Funktionalitäten für das Starten, für die Aktualisierung und zum Beenden von Transaktion nicht ermöglicht werden kann.	II_UNLOCK- TRANSLOGGING	NT

Tabelle 88: Testfälle zum Entsperrern von Log-Nachrichten von Transaktionen

6.3.1.45 Verwendung der Technischen Sicherheitseinrichtung durch mehrere Aufzeichnungssysteme (II_MCU)

ID	Zielsetzung	Profile	Typ
II_MCU_01	Prüfung, ob mehrere Aufzeichnungssysteme parallel jeweils eine Transaktion starten, einmalig mit Absicherungsschritt aktualisieren und beenden können.	MULTI_CLIENT SM_NOAGG SM_MULTI	PT
II_MCU_02	Prüfung, ob mehrere Aufzeichnungssysteme parallel jeweils eine Transaktion starten, einmalig ohne Absicherungsschritt aktualisieren und beenden können.	MULTI_CLIENT SM_AGG SM_MULTI	PT
II_MCU_03	Prüfung, ob die maximale Anzahl von Aufzeichnungssystemen parallel jeweils eine Transaktion starten, einmalig mit Absicherungsschritt aktualisieren und beenden können.	MULTI_CLIENT SM_NOAGG SM_MULTI	PT

ID	Zielsetzung	Profile	Typ
II_MCU_04	Prüfung, ob die maximale Anzahl von Aufzeichnungssystemen jeweils eine Transaktion starten, einmalig ohne Absicherungsschritt aktualisieren und beenden können.	MULTI_CLIENT SM_AGG SM_MULTI	PT
II_MCU_05	Prüfung, ob und welche Verzögerungen und Probleme bei dem Betrieb der TSE mit mehreren Aufzeichnungssystemen auftreten und ob diese den dokumentierten Verzögerungen und Problemen entsprechen.	MULTI_CLIENT SM_MULTI	PT

Tabelle 89: Testfälle für die Einbindungsschnittstelle – Verwendung der Technischen Sicherheitseinrichtung durch mehrere Aufzeichnungssysteme

6.3.1.46 Allgemeine Fehlermeldungen (II_ERR)

ID	Zielsetzung	Profile	Typ
II_ERR_01_Template	Prüfung, ob die Funktionalitäten aus Tabelle 91 beendet werden und je die Fehlermeldung ErrorDevice-NotInitialized ausgeben, wenn die Technische Sicherheitseinrichtung nicht initialisiert wurde. Es werden Parameter in der Form übergeben, dass die Funktionalitäten bei einer initialisierten TSE ohne Fehlermeldung beendet werden würden.	Siehe Tabelle 91	PT
II_ERR_02_Template	Prüfung, ob die Funktionalitäten aus Tabelle 92 beendet werden und je die Fehlermeldung ErrorTime-NotSet ausgeben, wenn der folgende Zustand gilt: Nach der Inbetriebnahme der Technischen Sicherheitseinrichtung, wurde die Zeit innerhalb des Sicherheitsmoduls nicht aktualisiert. Es werden Parameter in der Form übergeben, dass die Funktionalitäten bei aktualisierter Zeit ohne Fehlermeldung beendet werden würden.	Siehe Tabelle 92	NT
II_ERR_03_Template	Prüfung, ob die Funktionalitäten aus Tabelle 92 beendet werden und je die Fehlermeldung ErrorTime-NotSet ausgeben, wenn der folgende Zustand gilt: Nach einer Phase der Stromlosigkeit für die Technische Sicherheitseinrichtung, wurde die Zeit innerhalb des Sicherheitsmoduls nicht aktualisiert. Es werden Parameter in der Form übergeben, dass die Funktionalitäten bei aktualisierter Zeit ohne Fehlermeldung beendet werden würden.	Siehe Tabelle 92	NT

ID	Zielsetzung	Profile	Typ
II_ERR_04_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 93 beendet werden nachdem die entsprechende Log-Nachricht abgelegt wurde und je die Fehlermeldung ErrorCertificateExpired ausgegeben, wenn der folgende Zustand gilt: Das Zertifikat zu dem öffentlichen Schlüssel des Schlüsselpaars für die Prüfwertzeugung in System-Log-Nachrichten ist abgelaufen.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn das Zertifikat zu dem öffentlichen Schlüssel des Schlüsselpaars für die Prüfwertzeugung in System-Log-Nachrichten ist nicht abgelaufen wäre.</p>	Siehe Tabelle 93	PT
II_ERR_05_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 94 beendet werden und je die Fehlermeldung ErrorSecureElementDisabled ausgegeben, wenn das Sicherheitsmodul der Technischen Sicherheitseinrichtung deaktiviert wurde.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten bei nicht deaktivierten Sicherheitsmodul ohne Fehlermeldung beendet werden würden.</p>	Siehe Tabelle 94	NT
II_ERR_06_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 95 beendet werden und die Fehlermeldung ErrorParameterTooLong ausgegeben, wenn beim Aufruf der Funktionalitäten die maximale Inputlänge überschritten wird.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn beim Aufruf der Funktionalitäten die maximale Inputlänge nicht überschritten wäre. Die maximale Inputlänge ist dem ICS zu entnehmen.</p>	Siehe Tabelle 95	
II_ERR_07_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 96 beendet werden und die Fehlermeldung ErrorParameterSyntax ausgegeben, wenn beim Aufruf der Funktionalitäten eine falsche Syntax für Parameter verwendet wird.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn beim Aufruf der Funktionalitäten keine falsche Syntax verwendet worden wäre.</p>	Siehe Tabelle 96	NT

ID	Zielsetzung	Profile	Typ
II_ERR_08_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 97 beendet werden und je die Fehlermeldung ErrorSignatureCounterOverflow ausgegeben, wenn der Signaturzähler seinen maximalen Wert erreicht hat und eine weitere Signatur erstellt werden soll.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn der Signaturzähler niedriger wäre.</p>	Siehe Tabelle 97	NT
II_ERR_09_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 97 beendet werden und je die Fehlermeldung ErrorSignatureCounterExhausted ausgegeben, wenn der Verdacht besteht, dass der physische Speicher des Signaturzählers nicht mehr fehlerfrei funktioniert und eine weitere Signatur erstellt werden soll.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn kein Verdacht bestehen würde, dass der physische Speicher des Signaturzählers nicht mehr fehlerfrei funktioniert.</p>	Siehe Tabelle 97	NT
II_ERR_10_Template	<p>Prüfung, ob die Fehlermeldung ErrorFunctionNotSupported ausgelöst wird, wenn die nicht unterstützte Funktionalitäten aus Tabelle 98 aufgerufen wird.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn sie unterstützt werden würden.</p>	Siehe Tabelle 98	NT
II_ERR_11_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 97 beendet werden und je die Fehlermeldung ErrorSigningEventDataFailed ausgegeben, wenn die Funktionalität des Sicherheitsmoduls fehlschlägt, die die notwendigen Bestandteile der Log-Nachricht bestimmen soll.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn die Funktionalität des Sicherheitsmoduls nicht fehlschlagen würde, die die notwendigen Bestandteile der Log-Nachricht bestimmen soll.</p>	Siehe Tabelle 97	NT

ID	Zielsetzung	Profile	Typ
II_ERR_12_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 97 beendet werden und je die Fehlermeldung ErrorRetrieveLogMessageFailed ausgegeben, wenn die Antwort des Sicherheitsmoduls nicht empfangen wird.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn die Antwort des Sicherheitsmoduls empfangen worden wäre.</p>	Siehe Tabelle 97	NT
II_ERR_13_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 97 beendet werden und je die Fehlermeldung ErrorStoringLogMessageFailed ausgegeben, wenn eine Log-Nachricht nicht auf dem Speicher abgelegt werden kann.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn die Log-Nachricht auf dem Speicher abgelegt werden könnte.</p>	Siehe Tabelle 97	NT
II_ERR_14_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 99 beendet werden und je die Fehlermeldung ErrorSecureElementPartsDisconnected ausgegeben, wenn logische oder physische Teile des Sicherheitsmoduls nicht mehr verbunden sind.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn alle logischen und physischen Teile des Sicherheitsmoduls verbunden wären.</p>	Siehe Tabelle 99	NT
II_ERR_15_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 100 beendet werden und je die Fehlermeldung ErrorStorageMediumDisconnected ausgegeben, wenn der fernverbundene Speicher nicht mehr verbunden ist.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn der fernverbundene Speicher verbunden wäre.</p>	Siehe Tabelle 100	NT

ID	Zielsetzung	Profile	Typ
II_ERR_16_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 101 beendet werden und je die Fehlermeldung ErrorStorageMemoryFull ausgegeben, wenn die aktuell nicht verwendete Speicherkapazität nicht ausreicht, um die abzulegenden Daten zu speichern.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn die aktuell nicht verwendete Speicherkapazität ausreichen würde, um die abzulegenden Daten zu speichern.</p>	Siehe Tabelle 101	NT
II_ERR_17_Template	<p>Prüfung, ob die Funktionalitäten aus Tabelle 102 beendet werden und je die Fehlermeldung ErrorStorageMemoryFull ausgegeben, wenn die aktuell nicht verwendete Speicherkapazität nicht ausreicht, um die abzulegenden Daten zu speichern.</p> <p>Es werden Parameter in der Form übergeben, dass die Funktionalitäten ohne Fehlermeldung beendet werden würden, wenn die aktuell nicht verwendete Speicherkapazität ausreichen würde, um die abzulegenden Daten zu speichern.</p> <p>Es werden die Funktionalitäten getestet, bei denen die Fehlermeldung erst nach der regulären Ausführung der der Funktionalität ausgelöst wird.</p>	Siehe Tabelle 102	NT

Tabelle 90: Testfälle für Allgemeine Fehlermeldungen von Funktionen

ID Suffix	Funktionalität...	Profile
_A	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_B	zum Auslesen der Beschreibung der TSE.	II
_C	zur Auslösung eines Selbsttests.	II
_D	zur Installation von Updates für die TSE.	II_UPDATEDDEVICE
_E	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II
_F	zur Ausgabe der Gesamtkapazität des Speichermediums.	II_TOTALMEMORY
_G	zur Ausgabe der aktuell verwendeten Speicherkapazität.	II_USEDMEMORY
_H	zur Ausgabe der aktuell nicht verwendeten Speicherkapazität.	II_FREEMEMORY
_I	zur Ausgabe von Zustandsdaten der TSE.	II_DEVICEHEALTH

ID Suffix	Funktionalität...	Profile
_J	zur Ausgabe von Versionsinformationen über die TSE.	II_GETVERSIONS
_K	zur Ausgabe des Datums ab dem die Technische Sicherheits-einrichtung planmäßig nicht mehr zur Sicherung von Trans-aktionen verwendet werden kann.	II_ENDOFUSAGEDATE
_L	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME
_M	zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen.	II
_N	für den Export aller Log-Nachrichten, zur Verifikation benö-tigten Zertifikate und Zusatzdateien.	II
_O	zur Ausgabe der Zertifikate der Zertifikatskette.	II
_P	zum Löschen der Log-Nachrichten.	II_DELETELOGS
_Q	zur Ausgabe der Seriennummern.	II
_R	zur Ausgabe des aktuellen Stands des Signaturzählers.	II
_S	zur Wiedereinspielung von Backups von Log-Nachrichten.	II_RESTOREBACKUP
_T	zur Ausgabe der zuletzt erzeugten Log-Nachricht.	II
_U	zur Registrierung von Aufzeichnungssystemen.	II
_V	zur Deregistrierung von Aufzeichnungssystemen.	II
_W	für das Starten einer Transaktion.	II
_X	für die Aktualisierung der Transaktion.	II
_Y	zum Beenden einer Transaktion.	II
_Z	zum Export von Transaktions-Log-Nachrichten mit Filter-Funktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	II_EXPORTFILTERED
_AA	zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können.	II
_AB	zur Ausgabe der Anzahl von Aufzeichnungssystemen, die ak-tuell an nicht beendeten Transaktionen beteiligt sind.	II_CURNOCIENTS
_AC	zur Ausgabe der maximalen Anzahl von Aufzeichnungssys-temen, die gleichzeitig Transaktionen protokollieren kön-nen.	II_MAXNOCIENTS
_AD	zur Ausgabe der aktuell registrierten Aufzeichnungssysteme.	II_REGISTEREDCLIENTS

ID Suffix	Funktionalität...	Profile
_AE	zur Ausgabe der Anzahl von offenen Transaktionen.	II_CURNOTRANSACTIONS
_AF	zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können.	II_MAXNOTRANSACTIONS
_AG	zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet.	II_TRANSACTIONSTATE
_AH	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	II_OPENTRANSACTIONS
_AI	zur Ausgabe des aktuellen Stands des Transaktionszählers.	II
_AJ	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	II_LASTTRANSLOG
_AK	zur Unterbindung der Aufzeichnung von Transaktionen.	II_LOCKTRANSLOGGING
_AL	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UNLOCKTRANSLOGGING

Tabelle 91: Auf Testfall II_ERR_01_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_B	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_C	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II
_D	zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit.	II_CURRENTTIME
_E	zum Löschen der Log-Nachrichten.	II_DELETELOGS
_F	zur Registrierung von Aufzeichnungssystemen.	II
_G	zur Deregistrierung von Aufzeichnungssystemen.	II
_H	für das Starten einer Transaktion.	II
_I	für die Aktualisierung der Transaktion.	II
_J	zum Beenden einer Transaktion.	II
_K	zur Unterbindung der Aufzeichnung von Transaktionen.	II_LOCKTRANSLOGGING
_L	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UNLOCKTRANSLOGGING

Tabelle 92: Auf Testfälle II_ERR_02_Template und II_ERR_03_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Initialisierung der TSE.	II
_B	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_C	zur Auslösung eines Selbsttests.	II
_D	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_E	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME
_F	zur Registrierung von Aufzeichnungssystemen.	II
_G	zur Deregistrierung von Aufzeichnungssystemen.	II
_H	für das Starten einer Transaktion.	II
_I	für die Aktualisierung der Transaktion.	II
_J	zum Beenden einer Transaktion.	II
_K	zur Unterbindung der Aufzeichnung von Transaktionen.	II_LOCKTRANSLOGGING
_L	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UNLOCKTRANSLOGGING

Tabelle 93: Auf Testfall II_ERR_04_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Authentifizierung von Nutzern.	II
_B	zum Abmelden von Nutzern.	II
_C	zum Entsperren der PIN eines autorisierten Nutzers.	II
_D	zur Initialisierung der TSE.	II
_E	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_F	zur Auslösung eines Selbsttests.	II
_G	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_H	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II
_I	zur Ausgabe von Versionsinformationen über die TSE.	II_GETVERSIONS

ID Suffix	Funktionalität...	Profile
_J	zur Ausgabe des Datums ab dem die Technische Sicherheitseinrichtung planmäßig nicht mehr zur Sicherung von Transaktionen verwendet werden kann.	II_ENDOFUSAGEDATE
_K	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME
_L	zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen.	II
_M	zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit.	II_CURRENTTIME
_N	zum Löschen der Log-Nachrichten.	II_DELETELOGS
_O	zur Ausgabe des aktuellen Stands des Signaturzählers.	II
_P	zur Ausgabe der zuletzt erzeugten Log-Nachricht.	II
_Q	zur Registrierung von Aufzeichnungssystemen.	II
_R	zur Deregistrierung von Aufzeichnungssystemen.	II
_S	für das Starten einer Transaktion.	II
_T	für die Aktualisierung der Transaktion.	II
_U	zum Beenden einer Transaktion.	II
_V	zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können.	II
_W	zur Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind.	II_CURNOCLIENTS
_X	zur Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können.	II_MAXNOCLIENTS
_Y	zur Ausgabe der aktuell registrierten Aufzeichnungssysteme.	II_REGISTEREDCLIENTS
_Z	zur Ausgabe der Anzahl von offenen Transaktionen.	II_CURNOTRANSACTIONS
_AA	zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können.	II_MAXNOTRANSACTIONS
_AB	zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet.	II_TRANSACTIONSTATE
_AC	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	II_OPENTRANSACTIONS

ID Suffix	Funktionalität..	Profile
_AD	zur Ausgabe des aktuellen Stands des Transaktionszählers.	II
_AE	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	II_LASTTRANSLOG
_AF	zur Unterbindung der Aufzeichnung von Transaktionen.	II_LOCKTRANSLOGGING
_AG	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UNLOCKTRANSLOGGING

Tabelle 94: Auf Testfall II_ERR_05_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität..	Profile
_A	zur Authentifizierung von Nutzern.	II
_B	zum Entsperren der PIN eines autorisierten Nutzers.	II
_C	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_D	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_E	zur Wiedereinspielung von Backups von Log-Nachrichten.	II_RESTOREBACKUP
_F	zur Registrierung von Aufzeichnungssystemen.	II
_G	zur Deregistrierung von Aufzeichnungssystemen.	II
_H	für das Starten einer Transaktion.	II
_I	für die Aktualisierung der Transaktion.	II
_J	zum Beenden einer Transaktion.	II
_K	zum Export von Transaktions-Log-Nachrichten mit Filterfunktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	II_EXPORTFILTERED

Tabelle 95: Auf Testfall II_ERR_06_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität..	Profile
_A	zur Authentifizierung von Nutzern.	II
_B	zum Entsperren der PIN eines autorisierten Nutzers.	II
_C	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_D	zum Auslesen der Beschreibung der TSE.	II

ID Suffix	Funktionalität...	Profile
_E	zur Auslösung eines Selbsttests.	II
_F	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_G	zur Ausgabe der Gesamtkapazität des Speichermediums.	II_TOTALMEMORY
_H	zur Ausgabe der aktuell verwendeten Speicherkapazität.	II_USEDMEMORY
_I	zur Ausgabe der aktuell nicht verwendeten Speicherkapazität.	II_FREEMEMORY
_J	zur Ausgabe von Zustandsdaten der TSE.	II_DEVICEHEALTH
_K	zur Ausgabe von Versionsinformationen über die TSE.	II_GETVERSIONS
_L	zur Ausgabe des Datums ab dem die Technische Sicherheitseinrichtung planmäßig nicht mehr zur Sicherung von Transaktionen verwendet werden kann.	II_ENDOFUSAGEDATE
_M	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME
_N	zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen.	II
_O	zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit.	II_CURRENTTIME
_P	für den Export aller Log-Nachrichten, zur Verifikation benötigten Zertifikate und Zusatzdateien.	II
_Q	zur Ausgabe der Zertifikate der Zertifikatskette.	II
_R	zur Ausgabe der Seriennummern.	II
_S	zur Ausgabe des aktuellen Stands des Signaturzählers.	II
_T	zur Wiedereinspielung von Backups von Log-Nachrichten.	II_RESTOREBACKUP
_U	zur Ausgabe der zuletzt erzeugten Log-Nachricht.	II
_V	zur Registrierung von Aufzeichnungssystemen.	II
_W	zur Deregistrierung von Aufzeichnungssystemen.	II
_X	für das Starten einer Transaktion.	II
_Y	für die Aktualisierung der Transaktion.	II
_Z	zum Beenden einer Transaktion.	II

ID Suffix	Funktionalität..	Profile
_AA	zum Export von Transaktions-Log-Nachrichten mit Filter-Funktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	II_EXPORTFILTERED
_AB	zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können.	II
_AC	zur Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind.	II_CURNOCLIENTS
_AD	zur Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können.	II_MAXNOCLIENTS
_AE	zur Ausgabe der aktuell registrierten Aufzeichnungssysteme.	II_REGISTEREDCLIENTS
_AF	zur Ausgabe der Anzahl von offenen Transaktionen.	II_CURNOTRANSACTIONS
_AG	zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können.	II_MAXNOTRANSACTIONS
_AH	zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet.	II_TRANSACTIONSTATE
_AI	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	II_OPENTRANSACTIONS
_AJ	zur Ausgabe des aktuellen Stands des Transaktionszählers.	II
_AK	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	II_LASTTRANSLOG

Tabelle 96: Auf Testfall II_ERR_07_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität..	Profile
_A	zur Authentifizierung von Nutzern.	II
_B	zum Abmelden von Nutzern.	II
_C	zum Entsperren der PIN eines autorisierten Nutzers.	II
_D	zur Initialisierung der TSE.	II
_E	zum Erstellen oder Ändern der Beschreibung der TSE.	II
_F	zur Auslösung eines Selbsttests.	II

ID Suffix	Funktionalität...	Profile
_G	zur Installation von Updates für die TSE.	II_UPDATEDEVICE
_H	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II
_I	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_UPDATETIME
_J	zum Löschen der Log-Nachrichten.	II_DELETELOGS
_K	zur Registrierung von Aufzeichnungssystemen.	II
_L	zur Deregistrierung von Aufzeichnungssystemen.	II
_M	für das Starten einer Transaktion.	II
_N	für die Aktualisierung der Transaktion.	II
_O	zum Beenden einer Transaktion.	II
_P	zur Unterbindung der Aufzeichnung von Transaktionen.	II_LOCKTRANSLOGGING
_Q	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_UNLOCKTRANSLOGGING

Tabelle 97: Auf Testfälle II_ERR_08_Template, II_ERR_09_Template, II_ERR_11_Template, II_ERR_12_Template und II_ERR_13_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Installation von Updates für die TSE.	II_NO_UPDATEDEVICE
_B	zur Ausgabe der Gesamtkapazität des Speichermediums.	II_NO_TOTALMEMORY
_C	zur Ausgabe der aktuell verwendeten Speicherkapazität.	II_NO_USEDMEMORY
_D	zur Ausgabe der aktuell nicht verwendeten Speicherkapazität.	II_NO_FREEMEMORY
_E	zur Ausgabe von Zustandsdaten der TSE.	II_NO_DEVICEHEALTH
_F	zur Ausgabe von Versionsinformationen über die TSE.	II_NO_GETVERSIONS
_G	zur Ausgabe des Datums ab dem die Technische Sicherheitseinrichtung planmäßig nicht mehr zur Sicherung von Transaktionen verwendet werden kann.	II_NO_ENDOFUSAGEDATE
_H	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II_NO_UPDATETIME
_I	zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit.	II_NO_CURRENTTIME
_J	zum Löschen der Log-Nachrichten.	II_NO_DELETELOGS

ID Suffix	Funktionalität...	Profile
_K	zur Wiedereinspielung von Backups von Log-Nachrichten.	II_NO_RESTOREBACKUP
_L	zum Export von Transaktions-Log-Nachrichten mit Filter-Funktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	II_NO_EXPORTFILTERED
_M	zur Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind.	II_NO_CURNOCLIENTS
_N	zur Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können.	II_NO_MAXNOCLIENTS
_O	zur Ausgabe der aktuell registrierten Aufzeichnungssysteme.	II_NO_REGISTEREDCLIENTS
_P	zur Ausgabe der Anzahl von offenen Transaktionen.	II_NO_CURNOTRANSACTIIONS
_Q	zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können.	II_NO_MAXNOTRANSACTIIONS
_R	zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet.	II_NO_TRANSACTIONS-TATE
_S	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	II_NO_OPENTRANSACTIIONS
_T	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	II_NO_LASTTRANSLOG
_U	zur Unterbindung der Aufzeichnung von Transaktionen.	II_NO_LOCKTRANSLOGGING
_V	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II_NO_UNLOCKTRANSLOGGING

Tabelle 98: Auf Testfall II_ERR_10_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Authentifizierung von Nutzern.	SM_REMOTE_COMPONENTS

ID Suffix	Funktionalität...	Profile
_B	zum Abmelden von Nutzern.	SM_REMOTE_COMPONENTS
_C	zum Entsperren der PIN eines autorisierten Nutzers.	SM_REMOTE_COMPONENTS
_D	zur Initialisierung der TSE.	SM_REMOTE_COMPONENTS
_E	zum Erstellen oder Ändern der Beschreibung der TSE.	SM_REMOTE_COMPONENTS
_F	zur Auslösung eines Selbsttests.	SM_REMOTE_COMPONENTS
_G	zur Installation von Updates für die TSE.	SM_REMOTE_COMPONENTS II_UPDATEDDEVICE
_H	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	SM_REMOTE_COMPONENTS
_I	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	SM_REMOTE_COMPONENTS II_UPDATETIME
_J	zum Löschen der Log-Nachrichten.	SM_REMOTE_COMPONENTS II_DELETELOGS
_K	zur Registrierung von Aufzeichnungssystemen.	SM_REMOTE_COMPONENTS
_L	zur Deregistrierung von Aufzeichnungssystemen.	SM_REMOTE_COMPONENTS
_M	für das Starten einer Transaktion.	SM_REMOTE_COMPONENTS
_N	für die Aktualisierung der Transaktion.	SM_REMOTE_COMPONENTS
_O	zum Beenden einer Transaktion.	SM_REMOTE_COMPONENTS
_P	zur Unterbindung der Aufzeichnung von Transaktionen.	SM_REMOTE_COMPONENTS II_LOCKTRANSLLOGGING

ID Suffix	Funktionalität...	Profile
_Q	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	SM_REMOTE_COMPONENTS II_UNLOCKTRANSLOGGING

Tabelle 99: Auf Testfall II_ERR_14_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Authentifizierung von Nutzern.	STORAGE_REMOTE
_B	zum Abmelden von Nutzern.	STORAGE_REMOTE
_C	zum Entsperrn der PIN eines autorisierten Nutzers.	STORAGE_REMOTE
_D	zur Initialisierung der TSE.	STORAGE_REMOTE
_E	zum Erstellen oder Ändern der Beschreibung der TSE.	STORAGE_REMOTE
_F	zum Auslesen der Beschreibung der TSE.	STORAGE_REMOTE
_G	zur Auslösung eines Selbsttests.	STORAGE_REMOTE
_H	zur Installation von Updates für die TSE.	STORAGE_REMOTE II_UPDATEDDEVICE
_I	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	STORAGE_REMOTE
_J	zur Ausgabe der Gesamtkapazität des Speichermediums.	STORAGE_REMOTE II_TOTALMEMORY
_K	zur Ausgabe der aktuell verwendeten Speicherkapazität.	STORAGE_REMOTE II_USEDMEMORY
_L	zur Ausgabe der aktuell nicht verwendeten Speicherkapazität.	STORAGE_REMOTE II_FREEMEMORY
_M	zur Ausgabe von Zustandsdaten der TSE.	STORAGE_REMOTE II_DEVICEHEALTH
_N	zur Ausgabe von Versionsinformationen über die TSE.	STORAGE_REMOTE II_GETVERSIONS
_O	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	STORAGE_REMOTE II_UPDATETIME
_P	für den Export aller Log-Nachrichten, zur Verifikation benötigten Zertifikate und Zusatzdateien.	STORAGE_REMOTE

ID Suffix	Funktionalität...	Profile
_Q	zur Ausgabe der Zertifikate der Zertifikatskette.	STORAGE_REMOTE
_R	zum Löschen der Log-Nachrichten.	STORAGE_REMOTE II_DELETELOGS
_S	zur Ausgabe der Seriennummern.	STORAGE_REMOTE
_T	zur Wiedereinspielung von Backups von Log-Nachrichten.	STORAGE_REMOTE II_RESTOREBACKUP
_U	zur Ausgabe der zuletzt erzeugten Log-Nachricht.	STORAGE_REMOTE
_V	zur Registrierung von Aufzeichnungssystemen.	STORAGE_REMOTE
_W	zur Deregistrierung von Aufzeichnungssystemen.	STORAGE_REMOTE
_X	für das Starten einer Transaktion.	STORAGE_REMOTE
_Y	für die Aktualisierung der Transaktion.	STORAGE_REMOTE
_Z	zum Beenden einer Transaktion.	STORAGE_REMOTE
_AA	zum Export von Transaktions-Log-Nachrichten mit Filter-Funktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	STORAGE_REMOTE II_EXPORTFILTERED
_AB	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	STORAGE_REMOTE II_LASTTRANSLOG
_AC	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	STORAGE_REMOTE II_OPENTRANSACTIONS
_AD	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	STORAGE_REMOTE II_LASTTRANSLOG
_AE	zur Unterbindung der Aufzeichnung von Transaktionen.	STORAGE_REMOTE II_LOCKTRANSLOGGING
_AF	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	STORAGE_REMOTE II_UNLOCKTRANSLOGGING

Tabelle 100: Auf Testfall II_ERR_15_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zum Erstellen oder Ändern der Beschreibung der TSE.	II

ID Suffix	Funktionalität...	Profile
_B	zur Installation von Updates für die TSE.	II II_UPDATEDEVICE
_C	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	II
_D	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	II II_UPDATETIME
_E	zur Wiedereinspielung von Backups von Log-Nachrichten.	II II_RESTOREBACKUP
_F	zur Registrierung von Aufzeichnungssystemen.	II
_G	zur Deregistrierung von Aufzeichnungssystemen.	II
_H	für das Starten einer Transaktion.	II
_I	für die Aktualisierung der Transaktion.	II
_J	zum Beenden einer Transaktion.	II
_K	zur Unterbindung der Aufzeichnung von Transaktionen.	II II_LOCKTRANSLOGGING
_L	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	II II_UNLOCKTRANSLOGGING
_M	zum Erstellen oder Ändern der Beschreibung der TSE.	II

Tabelle 101: Auf Testfall II_ERR_16_Template anzuwendende Verfeinerungen

ID Suffix	Funktionalität...	Profile
_A	zur Authentifizierung von Nutzern	II
_B	zur Abmeldung von Nutzern	II
_C	zum Entsperren der PIN eines autorisierten Nutzers	II
_D	zur Initialisierung der TSE	II
_E	zur Auslösung eines Selbsttests.	II
_F	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls	II_UPDATETIME NO_TIME_SYNC

ID Suffix	Funktionalität...	Profile
_G	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls	II_UPDATETIME TIME_SYNC

Tabelle 102 Auf Testfall II_ERR_17_Template anzuwendende Verfeinerungen

6.3.1.47 Unterstützung von herstellereigene Funktionalitäten der Einbindungsschnittstelle (II_ADD)

ID	Zielsetzung	Profile	Typ
II_ADD_01	Prüfung, ob die Einbindungsschnittstelle neben den Funktionen der Einheitlichen Digitalen Schnittstelle gemäß der [BSI TR-03153-1] weitere Funktionen unterstützt.	NO_ADDITIONAL_FUNCTIONALITIES	FP

Tabelle 103: Testfälle für die Einbindungsschnittstelle – Unterstützung von herstellereigene Funktionalitäten der Einbindungsschnittstelle

6.3.2 Prüfungen der Standardschnittstellen gemäß BSI TR-03151-2 (SDI)

Dieses Modul enthält Tests für die Implementierung der Einbindungsschnittstelle nach [BSI TR-03151-2].

6.3.2.1 Verwendete Varianten der Einbindungsschnittstelle (SDI_IMP)

ID	Zielsetzung	Profile	Typ
SDI_IMP_01	Prüfung, ob die Einbindungsschnittstelle in mindestens einer durch die [BSI TR-03151-2] vorgegebene Implementierung vorliegt.	SDI	FP

Tabelle 104: Testfälle zu verwendeten Variante der Einbindungsschnittstelle

6.3.2.2 Funktionsnamen der Standardschnittstelle (SDI_FUN)

ID	Zielsetzung	Profile	Typ
SDI_FUN_01_Template	Prüfung, ob die Funktionalitäten aus Tabelle 106 unter den Funktionsnamen aus Tabelle 106 bereitgestellt werden.	Siehe Tabelle 106	PT

Tabelle 105: Prüfungen der Beschreibung der herstellereigene Funktionalitäten der Einbindungsschnittstelle

ID Suffix	Funktionalität...	Funktionsname	Profile
_A	zur Authentifizierung von Nutzern.	authenticateUser	SDI

ID Suffix	Funktionalität...	Funktionsname	Profile
_B	zum Abmelden von Nutzern.	logOut	SDI
_C	zum Entsperren der PIN eines autorisierten Nutzers.	unlockPin	SDI
_D	zur Initialisierung der TSE.	initialize	SDI
_E	zum Erstellen oder Ändern der Beschreibung der TSE.	setDescription	SDI
_F	zum Auslesen der Beschreibung der TSE.	getDescription	SDI
_G	zur Auslösung eines Selbsttests.	selfTest	SDI
_H	zur Installation von Updates für die TSE.	updateDevice	SDI II_UPDATEDEVICE
_I	zur Außerbetriebnahme des Sicherheitsmoduls der TSE.	disableSecureElement	SDI
_J	zur Ausgabe der Gesamtkapazität des Speichermediums.	getTotalMemory	SDI II_TOTALMEMORY
_K	zur Ausgabe der aktuell verwendeten Speicherkapazität.	getUsedMemory	SDI II_USEDMEMORY
_L	zur Ausgabe der aktuell nicht verwendeten Speicherkapazität.	getFreeMemory	SDI II_FREEMEMORY
_M	zur Ausgabe von Zustandsdaten der TSE.	getDeviceHealth	SDI II_DEVICEHEALTH
_N	zur Ausgabe von Versionsinformationen über die TSE.	GetComponentVersions	SDI II_GETVERSIONS
_O	zur Ausgabe des Datums ab dem die Technische Sicherheitseinrichtung planmäßig nicht mehr zur Sicherung von Transaktionen verwendet werden kann.	getEndOfUsageDate	SDI II_ENDOFUSAGEDATE
_P	zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.	updateTime	SDI II_UPDATETIME
_Q	zur Ausgabe der Möglichkeit über die Schnittstelle die Zeit zu stellen.	getTimeSyncVariant	SDI
_R	zur Ausgabe der aktuell im Krypto-Kern gestellten Zeit.	getCurrentSeTime	SDI II_CURRENTTIME

ID Suffix	Funktionalität...	Funktionsname	Profile
_S	zur Konfiguration der Logging-Einstellungen der TSE.	configureLogging	SDI II_CONFIGLOGGING
_T	für den Export aller Log-Nachrichten, zur Verifikation benötigten Zertifikate und Zusatzdateien.	exportLogMessages	SDI
_U	zur Ausgabe der Zertifikate der Zertifikatskette.	exportLoggingCertificates	SDI
_V	zum Löschen der Log-Nachrichten.	deleteLogMessages	SDI II_DELETELOGS
_W	zur Ausgabe der Seriennummern.	exportSerialNumbers	SDI
_X	zur Ausgabe des aktuellen Stands des Signaturzählers.	getCurrentLoggingSignatureCounters	SDI
_Y	zur Wiedereinspielung von Backups von Log-Nachrichten..	restoreLogsFromBackup	SDI II_RESTOREBACKUP
_Z	zur Ausgabe der zuletzt erzeugten Log-Nachricht.	getLastLogMessage	SDI
_AA	zur Registrierung von Aufzeichnungssystemen.	registerClient	SDI
_AB	zur Deregistrierung von Aufzeichnungssystemen.	deregisterClient	SDI
_AC	für das Starten einer Transaktion.	startTransaction	SDI
_AD	für die Aktualisierung einer Transaktion.	updateTransaction	SDI
_AE	zum Beenden einer Transaktion.	finishTransaction	SDI
_AF	zum Export von Transaktions-Log-Nachrichten mit Filter-Funktion sowie der zur Verifikation benötigten Zertifikate und Zusatzdateien.	exportFilteredTransactionLogs	SDI II_EXPORTFILTERED
_AG	zur Ausgabe der möglichen Varianten, wie Updates für Transaktionen durchgeführt werden können.	getSupportedTransactionUpdateVariants	SDI

ID Suffix	Funktionalität...	Funktionsname	Profile
_AH	zur Ausgabe der Anzahl von Aufzeichnungssystemen, die aktuell an nicht beendeten Transaktionen beteiligt sind.	getCurrentNumberOfClients	SDI II_CURNOCLIENTS
_AI	zur Ausgabe der maximalen Anzahl von Aufzeichnungssystemen, die gleichzeitig Transaktionen protokollieren können.	getMaxNumberOfClients	SDI II_MAXNOCLIENTS
_AJ	zur Ausgabe der aktuell registrierten Aufzeichnungssysteme.	getRegisteredClients	SDI II_REGISTEREDCLIENTS
_AK	zur Ausgabe der Anzahl von offenen Transaktionen.	getCurrentNumberOfTransactions	SDI II_CURNOTRANSACTIONS
_AL	zur Ausgabe der maximalen Anzahl von offenen Transaktionen, die gleichzeitig von der Technischen Sicherheitseinrichtung verwaltet werden können.	getMaxNumberOfTransactions	SDI II_MAXNOTRANSACTIONS
_AM	zur Ausgabe des Stadiums in welchem sich eine Transaktion befindet.	getTransactionState	SDI II_TRANSACTIONSTATE
_AN	zur Ausgabe der Transaktionsnummern aller nicht beendeten Transaktionen.	getOpenTransactions	SDI II_OPENTRANSACTIONS
_AO	zur Ausgabe des aktuellen Stands des Transaktionszählers.	getCurrentTransactionCounter	SDI
_AP	zur Ausgabe der zuletzt erzeugten Transaktions-Log-Nachricht.	getLastTransactionLogMessage	SDI II_LASTTRANSLLOG
_AQ	zur Unterbindung der Aufzeichnung von Transaktionen.	lockTransactionLogging	SDI II_LOCKTRANSLLOGGING
_AR	zur Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger.	unlockTransactionLogging	SDI II_UNLOCKTRANSLLOGGING

Tabelle 106: Auf Testfälle SDI_FUN_01_Template und SDI_ERR_01_Template anzuwendende Verfeinerungen

6.3.2.3 Fehlermeldungen der Standardschnittstelle (SDI_ERR)

ID	Zielsetzung	Profile	Typ
SDI_ERR_01_Template	Prüfung, ob die Fehlermeldungen der Funktionen aus Tabelle 106 nicht von den in der [BSI TR-03151-1] vorgegebenen Bezeichnern und Werten abweichen.	Siehe Tabelle 106	PT

Tabelle 107: Prüfungen der Parameter der Standardschnittstelle

6.3.2.4 Parameter der Standardschnittstelle (SDI_PAR)

ID	Zielsetzung	Profile	Typ
SDI_PAR_01_Template	Prüfung, ob die Funktionen aus Tabelle 109 die in der [BSI TR-03151-1] definierte Reihenfolge und Anzahl für Eingabe- und Ausgabeparameter einhalten und ob die in [BSI TR-03151-2] definierten Datentypen verwendet werden.	Siehe Tabelle 109	PT

Tabelle 108: Prüfungen der Parameter der Standardschnittstelle

ID Suffix	Funktionsname	Profile
_A	authenticateUser	SDI
_B	unblockPin	SDI
_C	setDescription	SDI
_D	getDescription	SDI
_E	selfTest	SDI
_F	updateDevice	SDI II_UPDATEDDEVICE
_G	getTotalMemory	SDI II_TOTALMEMORY
_H	getUsedMemory	SDI II_USEDMEMORY
_I	getFreeMemory	SDI II_FREEMEMORY
_J	getDeviceHealth	SDI II_DEVICEHEALTH

ID Suffix	Funktionsname	Profile
_K	getComponentVersions	SDI II_GETVERSIONS
_L	getEndOfUsageDate	SDI II_ENDOFUSAGEDATE
_M	updateTime	SDI II_UPDATETIME
_N	getTimeSyncVariant	SDI
_O	getCurrentSeTime	SDI II_CURRENTTIME
_P	configureLogging	SDI II_CONFIGLOGGING
_Q	exportLogMessages	SDI
_R	exportLoggingCertificates	SDI
_S	exportSerialNumbers	SDI
_T	getCurrentLoggingSignatureCounters	SDI
_U	restoreLogsFromBackup	SDI II_RESTOREBACKUP
_V	getLastLogMessage	SDI
_W	registerClient	SDI
_X	deregisterClient	SDI
_Y	startTransaction	SDI
_Z	updateTransaction	SDI
_AA	finishTransaction	SDI
_AB	exportFilteredTransactionLogs	SDI II_EXPORTFILTERED
_AC	getSupportedTransactionUpdateVariants	SDI
_AD	getCurrentNumberOfClients	SDI II_CURNOCIENTS
_AE	getMaxNumberOfClients	SDI II_MAXNOCIENTS

ID Suffix	Funktionsname	Profile
_AF	getRegisteredClients	SDI II_REGISTEREDCLIENTS
_AG	getCurrentNumberOfTransactions	SDI II_CURNOTRANSACTIONS
_AH	getMaxNumberOfTransactions	SDI II_MAXNOTRANSACTIONS
_AI	getTransactionState	SDI II_TRANSACTIONSTATE
_AJ	getOpenTransactions	SDI II_OPENTRANSACTIONS
_AK	getCurrentTransactionCounter	SDI
_AL	getLastTransactionLogMessage	SDI II_LASTTRANSLOG

Tabelle 109: Auf Testfall SDI_PAR_01_Template anzuwendende Verfeinerungen

6.3.3 Prüfungen für herstellerepezifische Funktionalitäten der Einbindungsschnittstelle (ADD)

Dieses Modul enthält Tests für herstellerepezifische Funktionalitäten der Einbindungsschnittstelle, die nicht in [BSI TR-03151-1] beschrieben sind.

6.3.3.1 Beschreibung der Funktionalitäten (ADD_DOC)

ID	Zielsetzung	Profile	Typ
ADD_DOC_01	Prüfung, ob der Hersteller eine detaillierte Beschreibung der zusätzlichen Funktionalitäten der Einbindungsschnittstelle bereitstellt.	ADDITIONAL_FUNCTIONALITIES	FP
ADD_DOC_02	Prüfung, ob die zusätzlichen Funktionalitäten der Einbindungsschnittstelle den in den Technischen Richtlinien und Schutzprofilen vorgegeben Methoden, Abläufen, Grundideen und Sicherheitsvorgaben entsprechen.	ADDITIONAL_FUNCTIONALITIES	FP
ADD_DOC_03	Prüfung, ob die zusätzlichen Funktionalitäten der Einbindungsschnittstelle mit dem zuständigen Referat des BSI abgestimmt sind und freigegeben wurden.	ADDITIONAL_FUNCTIONALITIES	FP

Tabelle 110: Prüfungen der Beschreibung der herstellerepezifische Funktionalitäten der Einbindungsschnittstelle

6.3.3.2 Unterscheidbarkeit herstellerspezifische Funktionalitäten zur Standardschnittstelle (ADD_DIF)

ID	Zielsetzung	Profile	Typ
ADD_DIF_01	Prüfung, ob die zusätzlichen Funktionalitäten der Einbindungsschnittstelle klar erkennbar abgeteilt und als Zusatzfunktionen ersichtlich sind.	ADDITIO-NAL_FUNCTIONALITIES	FP

Tabelle 111: Prüfungen der Unterscheidbarkeit herstellerspezifische Funktionalitäten zur Einbindungsschnittstelle gemäß BSI TR-03151-1

6.3.3.3 Abwandlungen von Standardfunktionen (ADD_ABW)

ID	Zielsetzung	Profile	Typ
ADD_ABW_01	Prüfung, ob zusätzlichen Funktionalitäten der Einbindungsschnittstelle, die eine Abwandlungen von Standardfunktionen darstellen gleich den Standardfunktionen funktionieren. Insbesondere wird das Verhalten im Fehlerfall untersucht.	ADDITIO-NAL_FUNCTIONALITIES	PT

Tabelle 112: Prüfungen der herstellerspezifische Funktionalitäten die Abwandlungen von Standardfunktionen sind

6.4 Prüfungen der Exportdaten gemäß BSI TR-03153-1 (EXP)

Die Testfälle dieses Moduls beziehen sich auf die exportierten Daten der Exportschnittstelle.

6.4.1 TAR-Format (EXP_TAR)

ID	Zielsetzung	Profile	Typ
EXP_TAR_01	Prüfung, ob die Datei, die die Exportschnittstelle bei einem Export zurückgibt, das definierte TAR-Format hat.	SM_BASIC	PT
EXP_TAR_02	Prüfung, ob die Datei, die die Exportschnittstelle bei einem Export zurückgibt, das definierte TAR-Format hat, wenn der folgende Zustand gilt: Der verfügbare Speicher des Speichermediums ist komplett belegt.	SM_BASIC	PT
EXP_TAR_03	Prüfung, ob in den TAR-Containern, die während der Prüfung erstellt wurden, Dateien enthalten sind, die nicht von der BSI TR-03153-1 oder einer referenzierten TR vorgegeben werden.	SM_BASIC	PT

Tabelle 113: Prüfungen der Exportschnittstelle gemäß BSI TR-03153-1 – TAR-Format

6.4.2 Datei info.csv (EXP_INF)

ID	Zielsetzung	Profile	Typ
EXP_INF_01	Prüfung der exportierten Datei info.csv. Der Test prüft den Dateinamen.	SM_BASIC	PT
EXP_INF_02	Prüfung der exportierten Datei info.csv. Der Test prüft die enthaltenen Daten. Die Beschreibung der TSE wurden nicht durch den Hersteller oder den Nutzer gesetzt.	DESCRIPTION_NOT_SET SM_BASIC	PT
EXP_INF_03	Prüfung der exportierten Datei info.csv. Der Test prüft die enthaltenen Daten. Die Beschreibung der TSE wurde durch den Hersteller gesetzt und durch den Nutzer nicht geändert.	SM_BASIC DESCRIPTION_SET	PT
EXP_INF_04	Prüfung der exportierten Datei info.csv. Der Test prüft die enthaltenen Daten. Die Beschreibung der TSE wurde durch den Nutzer geändert.	SM_BASIC	PT
EXP_INF_05	Prüfung der exportierten Datei info.csv. Der Test prüft das Format der Datei. Die Beschreibung der TSE wurde nicht durch den Hersteller oder den Nutzer gesetzt.	DESCRIPTION_NOT_SET SM_BASIC	PT
EXP_INF_06	Prüfung der exportierten Datei info.csv. Der Test prüft das Format der Datei. Die Beschreibung der TSE wurde durch den Hersteller gesetzt und durch den Nutzer nicht geändert.	SM_BASIC DESCRIPTION_SET	PT
EXP_INF_07	Prüfung der exportierten Datei info.csv. Der Test prüft das Format der Datei. Die Beschreibung der TSE wurde durch den Nutzer geändert.	SM_BASIC	PT

Tabelle 114: Prüfungen der Exportschnittstelle gemäß BSI TR-03153-1 – Initialisierungsdaten

6.4.3 Log-Nachrichten (EXP_LOG)

ID	Zielsetzung	Profile	Typ
EXP_LOG_01 _Template	Prüfung, ob eine Log-Nachricht für die Protokollierung einer Systemfunktionalität erstellt wird. Es werden die Ereignisse aus Tabelle 116 betrachtet.	Siehe Tabelle 116	PT
EXP_LOG_02 _Template	Prüfung, ob die nicht funktionspezifischen Inhalte ³ der Log-Nachricht für die Protokollierung einer Systemfunktionalität den Vorgaben der BSI TR-03151-1 entsprechen. Es werden die Ereignisse aus Tabelle 116 betrachtet.	Siehe Tabelle 116	PT

³ Siehe Kapitel "Contents of system log messages" der [BSI TR-03151-1]

ID	Zielsetzung	Profile	Typ
EXP_LOG_03_Template	<p>Prüfung, ob der Dateiname der Log-Nachricht für die Protokollierung einer Systemfunktionalität den Vorgaben der BSI TR-03151-1 entsprechen.</p> <p>Es werden die Ereignisse aus Tabelle 116 betrachtet.</p>	Siehe Tabelle 116	PT
EXP_LOG_04_Template	<p>Prüfung, ob die ASN.1-Struktur nicht funktionsspezifischer Anteile⁴ der Log-Nachrichten für die Protokollierung von Systemfunktionalitäten, den Vorgaben der BSI TR-03151-1 entspricht.</p> <p>Es dürfen nur die vorgegebenen Elemente in den Log-Nachrichten enthalten sein.</p> <p>Es werden die Ereignisse aus Tabelle 116 betrachtet.</p>	Siehe Tabelle 116	PT
EXP_LOG_05	<p>Prüfung, ob die nicht funktionsspezifischen Inhalte⁵ der Log-Nachricht für die Protokollierung von Audit-Daten den Vorgaben der BSI TR-03151-1 entsprechen.</p> <p>Es werden alle Log-Nachrichten für die Protokollierung von Audit-Daten betrachtet, die vom Sicherheitsmodul erzeugt werden können.</p>	SM_BASIC	PT
EXP_LOG_06	<p>Prüfung, ob der Dateiname der Log-Nachricht für die Protokollierung von Audit-Daten, die vom Sicherheitsmodul erzeugt werden, den Vorgaben der BSI TR-03151-1 entsprechen.</p> <p>Es werden alle Log-Nachrichten für die Protokollierung von Audit-Daten betrachtet, die vom Sicherheitsmodul erzeugt werden können.</p>	SM_BASIC	PT
EXP_LOG_07	<p>Prüfung, ob die ASN.1-Struktur nicht funktionsspezifischer Anteile⁶ der Log-Nachrichten für die Protokollierung von Audit-Daten den Vorgaben der BSI TR-03151-1 entspricht.</p> <p>Es dürfen nur die vorgegebenen Elemente in den Log-Nachrichten enthalten sein.</p> <p>Es werden alle Log-Nachrichten für die Protokollierung von Audit-Daten betrachtet, die vom Sicherheitsmodul erzeugt werden können.</p>	SM_BASIC	PT
EXP_LOG_08	<p>Prüfung, ob die nicht funktionsspezifischen Inhalte⁷ der Log-Nachricht für die Protokollierung von Transaktionen den Vorgaben der BSI TR-03151-1 entsprechen.</p>	SM_BASIC	PT

⁴ Siehe Kapitel "System log ASN.1 Definition" der [BSI TR-03151-1]

⁵ Siehe Kapitel "Contents of audit log messages" der [BSI TR-03151-1]

⁶ Siehe Kapitel "Audit log ASN.1 Definition" der [BSI TR-03151-1]

⁷ Siehe Kapitel "Contents of transaction log messages" der [BSI TR-03151-1]

ID	Zielsetzung	Profile	Typ
EXP_LOG_09	Prüfung, ob der Dateiname der Log-Nachricht für die Protokollierung von Transaktionen den Vorgaben der BSI TR-03151-1 entsprechen. Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion nicht aggregieren.	SM_NOAGG	PT
EXP_LOG_10	Prüfung der ASN.1-Struktur der Log-Nachrichten für die Protokollierung von Transaktionen . Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion nicht aggregieren.	SM_NOAGG	PT
EXP_LOG_11	Prüfung, ob der Dateiname der Log-Nachricht für die Protokollierung von Transaktionen den Vorgaben der BSI TR-03151-1 entsprechen. Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion aggregieren .	SM_AGG	PT
EXP_LOG_12	Prüfung der ASN.1-Struktur der Log-Nachrichten für die Protokollierung von Transaktionen . Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion aggregieren .	SM_AGG	PT
EXP_LOG_13	Prüfung, ob bei der Protokollierung von Transaktionen , die zu sichernden Daten den zugehörigen Datenfeldern in den Transaktions-Log-Nachrichten zugeordnet werden. Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion nicht aggregieren. Die TSE kann zu einem Zeitpunkt nur von einem Aufzeichnungssystem für die Protokollierung von Transaktionen verwendet werden.	SM_NOAGG NO_MULTI_CLIENT	PT
EXP_LOG_14	Prüfung, ob bei der Protokollierung von Transaktionen , die zu sichernden Daten den zugehörigen Datenfeldern in den Transaktions-Log-Nachrichten zugeordnet werden. Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion aggregieren . Die TSE kann zu einem Zeitpunkt nur von einem Aufzeichnungssystem für die Protokollierung von Transaktionen verwendet werden.	SM_AGG NO_MULTI_CLIENT	PT

ID	Zielsetzung	Profile	Typ
EXP_LOG_15	Prüfung, ob bei der Protokollierung von Transaktionen , die zu sichernden Daten den zugehörigen Datenfeldern in den Transaktions-Log-Nachrichten zugeordnet werden. Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion nicht aggregieren. Die TSE kann von mehreren Aufzeichnungssystemen gleichzeitig für die Protokollierung von Transaktionen verwendet werden.	SM_NOAGG MULTI_CLIENT	PT
EXP_LOG_16	Prüfung, ob bei der Protokollierung von Transaktionen , die zu sichernden Daten den zugehörigen Datenfeldern in den Transaktions-Log-Nachrichten zugeordnet werden. Das Sicherheitsmodul der Technischen Sicherheitseinrichtung kann Daten des Vorgangs bei Aktualisierungen einer Transaktion aggregieren . Die TSE kann von mehreren Aufzeichnungssystemen gleichzeitig für die Protokollierung von Transaktionen verwendet werden.	SM_AGG MULTI_CLIENT	PT
EXP_LOG_17	Prüfung, ob die funktionspezifischen Inhalte für die Protokollierung von Audit-Daten , die vom Sicherheitsmodul erzeugt werden, im Datenfeld seAuditData protokolliert werden und den Vorgaben der Herstellerdokumentation entsprechen. Es werden alle Log-Nachrichten für die Protokollierung von Audit-Daten betrachtet, die vom Sicherheitsmodul erzeugt werden können.	SM_BASIC	PT
EXP_LOG_18	Prüfung, ob die TSE ausschließlich solche Log-Nachrichten produziert, die in der [BSI TR-03153-1] und dort referenzierten Technischen Richtlinien definiert sind. Die Prüfung erfolgt durch Durchsicht aller während der Tests exportierten Log-Nachrichten.	SM_BASIC	PT
EXP_LOG_19	Prüfung, ob bei Auftritt eines Audit-Events der CSP-Einheit beziehungsweise des CSPs für jede 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.	SM_REMOTE_COMPONENTS	PT
EXP_LOG_20	Prüfung, ob bei einer Unterbrechung der oder Fehler in der Verbindung zwischen den CSP-Einheit und SMA-ERS-Einheit keine Log-Nachrichtenteile verloren gehen können.	SM_REMOTE_COMPONENTS	FP
EXP_LOG_21	Prüfung, ob sich die TSE bei einer unterbrochenen Verbindung korrekt verhält.	SM_REMOTE_COMPONENTS	PT

ID	Zielsetzung	Profile	Typ
EXP_LOG_22	Prüfung, ob durch Fehler bei der Übertragung zwischen SMAERS-Einheit und CSP-Einheit keine Lücken in der Sequenz der Transaktions- und Signaturzählerstände entstehen können.	SM_REMOTE_COMPONENTS	PT
EXP_LOG_23	Prüfung, ob bei Erstellung aller Transaktions-Log-Varianten das Feld additionalInternalData nicht belegt wird.	SM_BASIC	PT
EXP_LOG_24	Prüfung, ob bei Erstellung aller Transaktions-Log-Varianten das Feld additionalExternalData nicht belegt wird, wenn keine zusätzlichen Daten (additionalData/additionalExternalData oder andere) vom Aufzeichnungssystem an die TSE übergeben wurden.	SM_BASIC	PT
EXP_LOG_25	Prüfung, ob die TSE alle Transaktions-Log-Varianten korrekt erstellt, wenn das Aufzeichnungssystem, den Vorgaben zuwider, zusätzliche Daten für das Feld additionalExternalData übergibt.	SM_BASIC	PT
EXP_LOG_26_Template	Prüfung, ob die Log-Nachricht für die Protokollierung einer Systemfunktionalität das Feld additionalInternalData enthält. Es werden die Ereignisse aus Tabelle 116 betrachtet.	Siehe Tabelle 116	PT
EXP_LOG_27	Prüfung, ob sich bei einer Rezertifizierung, die durch eine Aktualisierung der TSE notwendig ist, die Art und Weise von den Aufzeichnungen vor und nach der Aktualisierung nicht unterscheiden, wenn die Beibehaltung der bereits verwendeten Signaturschlüssel geplant ist.	RECERT	PT
EXP_LOG_28	Prüfung, ob in allen Aufzeichnungen und Logs, die im Rahmen der Konformitätsprüfung erstellt wurden, kein indefinite length encoding verwendet wird.	SM_NO_INDEF	PT
EXP_LOG_29	Prüfung, ob in allen Transaktions-Log-Nachrichten, die im Rahmen der Konformitätsprüfung erstellt wurden, das korrekte Tag für das Log-Nachrichten-Element processData verwendet wird.	SM_NO_INDEF	PT
EXP_LOG_30	Prüfung, ob die TSE in Aufzeichnungen indefinite length encoding nur für das Element processData von Aktualisierungen von Transaktionen verwendet.	SM_INDEF	PT
EXP_LOG_31	Prüfung, ob das korrekte Tag für das Element processData und deren Unterelemente verwendet wird, wenn indefinite length encoding verwendet wird.	SM_INDEF	PT
EXP_LOG_32	Prüfung, ob das korrekte Tag für das Element processData verwendet wird, wenn kein indefinite length encoding verwendet wird.	SM_INDEF	PT

Tabelle 115: Prüfungen der Exportschnittstelle gemäß BSI TR-03153-1 – Log-Nachrichten

ID Suffix	Ereignis	Profile
_A	Authentifizierung von Nutzern	SM_BASIC
_B	Abmelden von Nutzern	SM_BASIC
_C	Entsperren der PIN eines autorisierten Nutzers	SM_BASIC
_D	Initialisierung der TSE	SM_BASIC
_E	Erstellen oder Ändern der Beschreibung der TSE	SM_BASIC
_F	Auslösung eines Selbsttests	SM_BASIC
_G	Installation von Updates für die TSE	SM_BASIC II_UPDATEDevice
_H	Außerbetriebnahme des Sicherheitsmoduls der TSE	SM_BASIC
_I	Aktualisierung der Zeit innerhalb des Sicherheitsmoduls	SM_BASIC II_UPDATETIME
_J	Konfiguration der Logging-Einstellungen der TSE	SM_BASIC II_CONFIGLOGGING
_K	Löschen der Log-Nachrichten	SM_BASIC II_DELETELOGS
_L	Registrierung von Aufzeichnungssystemen	SM_BASIC
_M	Deregistrierung von Aufzeichnungssystemen	SM_BASIC
_N	Unterbindung der Aufzeichnung von Transaktionen	SM_BASIC II_LOCKTRANSLOGGING
_O	Ermöglichung der Aufzeichnung von Transaktionen nach einer vorherigen Unterbindung selbiger	SM_BASIC II_UNLOCKTRANSLOGGING
_P	Authentifizierung eines Administrators der Sicherheitsmodulanwendung	SMAADMIN_AVAILABLE
_Q	Sicherheitsmodulanwendung startet die Audit-Funktionalität	SM_BASIC
_R	Sicherheitsmodulanwendung tritt beim Vorherrschen von Fehlern in einen sicheren Zustand ein	SM_BASIC
_S	Fehler, die zum Eintritt der Sicherheitsmodulanwendung in den sicheren Zustand führten, liegen nicht mehr vor und der sichere Zustand wird verlassen	SM_BASIC

ID Suffix	Ereignis	Profile
_T	Selbsttest des Sicherheitsmodul schlägt fehl	SM_BASIC
_U	Audit-Funktionalität der Sicherheitsmodulanwendung wird konfiguriert	SM_BASIC

Tabelle 116: Auf Testfälle *EXP_LOG_01_Template*, *EXP_LOG_02_Template*, *EXP_LOG_03_Template*, *EXP_LOG_04_Template* und *EXP_LOG_26_Template* anzuwendende Verfeinerungen

6.5 Ergänzung zu Prüfungen zur Herstellerdokumentation (DOC)

Der folgenden Testfälle prüfen die Eignung der Herstellerdokumentation zur Sicherstellung der unmittelbaren Aufzeichnung durch die TSE.

ID	Zielsetzung	Profile	Typ
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 dem Betrieb der TSE mit mehreren Aufzeichnungssystemen zu erwarten sind.	SM_BASIC	FP
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.	SM_BASIC	FP
DOC_FUN_01	Prüfung, ob die TSE zusätzliche Funktionen unterstützt, die nicht in der [BSI TR-03153-1] oder einer dort referenzierten Technischen Richtlinie beschrieben sind.	SM_BASIC	FP
DOC_INS_01	Prüfung, ob der Hersteller in einer Herstellerdokumentation Außenprüfer, sowie eine Kassen-Nachschauf Durchführende über die notwendigen Schritte aufklärt, die notwendig sind, um die Korrektheit des Einsatzes der Technischen Sicherheitseinrichtung nachzuvollziehen.	SM_BASIC	FP
DOC_SM_01	Prüfung, ob die Bestandteile des Sicherheitsmoduls nach den erforderlichen Schutzprofilen nach Common Criteria zertifiziert sind.	SM_BASIC	FP

ID	Zielsetzung	Profile	Typ
DOC_SM_02	Prüfung, ob Provisionierungs-, Umgebungsschutz-, Update- und CSP-Konfigurationskonzept vorliegen und durch eine Common Criteria-Prüfstelle, oder übergangsweise/ersatzweise durch das BSI bestätigt worden sind.	SM_BASIC	FP
DOC_KRY_01	Prüfung, ob die allgemeinen Empfehlungen der [BSI TR-02102] eingehalten werden, wenn in der Technischen Sicherheitseinrichtung bzw. der Verarbeitung der aufzuzeichnenden Daten, neben der Berechnung von Prüfwerten, weitere kryptographische Verfahren zum Einsatz kommen, zu denen keine konkreten Vorgaben in [BSI TR-03116-5] enthalten sind.	SM_BASIC	FP
DOC_USR_01	Prüfung, ob der Hersteller im ICS erklärt, dass an der Einbindungsschnittstelle der Technischen Sicherheitseinrichtung, neben den Nutzern unauthenticated, logger, admin und ggf. timeadmin, keine weiteren Nutzer implementiert sind.	SM_BASIC	FP
DOC_USR_02	Prüfung, ob der Hersteller den Anwender / Nutzer (Steuerpflichtigen) in einer Herstellerdokumentation darüber informiert, dass Nutzer sich ausloggen sollen, wenn keine weiteren Aufrufe von Funktionen geplant sind, welche nur von autorisierten Nutzern aufgerufen werden dürfen.	SM_BASIC	FP
DOC_PRC_01	Prüfung, ob der Hersteller im ICS erklärt, dass der PIN Fehlbedienungs-zähler im Sicherheitsmodul geführt wird.	SM_BASIC	FP
DOC_TME_01	Prüfung, ob genau eins der definierten Zeitformate laut ICS von der TSE unterstützt wird.	II_UPDATETIME	FP
DOC_TME_02	Prüfung, ob der Hersteller im Handbuch für den Anwender beschreibt, wie oft die Funktion updateTime aufgerufen werden muss, um eine unverhältnismäßige Abweichung von der offiziellen Zeit zu vermeiden.	II_UPDATETIME NO_CENTRAL_TIME	FP
DOC_DSE_01	Prüfung, ob der Hersteller den Anwender / Nutzer (Steuerpflichtigen) in einer Herstellerdokumentation über die Pflicht zur Sperrung des Zertifikats aufklärt, wenn die Vermutung nahe liegt, dass die Vertrauenswürdigkeit der TSE nicht mehr gegeben ist .	SM_BASIC	FP
DOC_DSE_02	Prüfung, ob der Hersteller den Anwender / Nutzer (Steuerpflichtigen) in einer Herstellerdokumentation darüber aufklärt, dass wenn die TSE außer Betrieb gesetzt wird, ohne dass ein sicherheitsrelevanter Vorfall vorliegt, das Zertifikat der TSE nicht gesperrt werden darf.	SM_BASIC	FP

ID	Zielsetzung	Profile	Typ
DOC_DSE_03	Prüfung, ob der Hersteller den Anwender / Nutzer (Steuerpflichtigen) in einer Herstellerdokumentation über die Empfehlung zur Deaktivierung des Sicherheitsmoduls aufklärt, wenn die TSE auf Ansinnen des Steuerpflichtigen außer Betrieb gesetzt wird.	SM_BASIC	FP
DOC_DSE_04	Prüfung, ob der Hersteller den Anwender / Nutzer (Steuerpflichtigen) in einer Herstellerdokumentation darüber aufklärt, wie und unter welcher Kontaktadresse das Zertifikat der TSE in der PKI gesperrt werden kann.	SM_BASIC	FP
DOC_ARCH_01	Prüfung, ob der Hersteller den Anwender / Nutzer (Steuerpflichtigen) in einer Herstellerdokumentation über die Anforderungen für einen stabilen und störungsfreien Betrieb der TSE aufklärt.	SM_BASIC	FP
DOC_AUD_01	Prüfung, ob alle spezifischen Inhalte, die für das Element seAuditData verwendet werden, dokumentiert sind. Diese Dokumentation muss eine Feinspezifikation des Datenformats der Daten des Elements seAuditData enthalten.	SM_BASIC	FP
DOC_EXP_01	Prüfung, ob der Hersteller eine schlüssige Anleitung bereitstellt, wie die abgesicherten Daten, in Form des TAR-Containers, ohne Hilfe des Aufzeichnungssystems aus der TSE exportiert werden können.	SM_BASIC	FP
DOC_EXP_02	Prüfung, ob der Hersteller eine korrekte Anleitung bereitstellt, wie die abgesicherten Daten, in Form des TAR-Containers, ohne Hilfe des Aufzeichnungssystems, aus der TSE exportiert werden können.	NO_EXPORTTOOL	PT
DOC_EXP_03	Prüfung, ob der Hersteller Hilfstools bereitstellt, die benötigt werden, um die abgesicherten Daten, in Form des TAR-Containers, ohne Hilfe des Aufzeichnungssystems aus der TSE zu exportieren.	EXPORTTOOL	FP
DOC_EXP_04	Prüfung, ob der Hersteller eine korrekte Anleitung bereitstellt, wie die abgesicherten Daten, in Form des TAR-Containers, ohne Hilfe des Aufzeichnungssystems, mit den bereitgestellten Hilfstools aus der TSE exportiert werden können.	EXPORTTOOL	PT

Tabelle 117: Prüfungen zur Herstellerdokumentation

7 Testfälle

7.1 Notation von Testfällen

Diese Technischen Richtlinie enthält eine Auflistung der verschiedenen Testfälle. Hierbei wird für einen Testfall die folgende Information dargestellt:

- eindeutiger Bezeichner,
- kurze Beschreibung der Zielsetzung für den Test,
- relevante Profile,
- Typ des Tests.

Die konkreten Testfälle werden in XML-Dokumenten definiert. Die Spezifikation der logischen Struktur dieser XML-Dokumente erfolgt anhand eines XML Schemas, das in Kapitel 7.2 näher erläutert wird. Der Anhang dieses Dokumentes enthält Testfallbeispiele (siehe Kapitel A.2).

Es folgt eine kurze Erläuterung der Informationen, die einen Testfall repräsentieren.

Ein konkreter Testfall enthält die folgenden Informationen:

- eindeutiger Bezeichner des Testfalls,
- Titel des Testfalls,
- Version des Testfalls,
- Zweck des Testfalls,
- zugeordnete Profile,
- Testschritte, die für den Testfall durchgeführt werden.

Optional kann ein Testfall die folgenden Informationen enthalten:

- Referenzen auf Technische Richtlinien und andere Spezifikationen auf denen der Testfall basiert,
- Vorbedingungen für den Test,
- Alternative Testverfahren.

Innerhalb eines Testschritts erfolgen die folgenden Definitionen:

- Die Aktion, die für einen Testschritt durchgeführt wird. Im Rahmen dieser Technischen Richtlinie kann eine Aktion einen Aufruf einer Funktion der jeweiligen Einbindungsschnittstelle darstellen. In diesem Zusammenhang erfolgt eine textuelle Beschreibung des Funktionsaufrufs, wie z. B. *Invoke the function to start a transaction and pass the process data*. Weiterhin kann eine Aktion eine manuelle Aktion beim Prüfen von exportierten Daten darstellen, wie z. B. *Check, if the file names of the exported log messages comply with the requirements in BSI TR-03151-1*.
- ein oder mehrere erwartete Resultate für den Testschritt.

Die XML-Testfälle werden jeweils durch eine separate Datei zu dieser Technischen Richtlinie bereitgestellt.

Auf Grundlage der XML-Testfälle wird ein PDF-Dokument generiert, das die Informationen für die verschiedenen Testfälle beinhaltet.

7.1.1 Verwendung von Variablen

Innerhalb mancher XML-Testfälle werden Variablen für den Testablauf genutzt. Diese speichern etwa Zwischenergebnisse oder dienen als Platzhalter für Eingabeparameter. Variablen innerhalb der XML-Testfälle haben die Form `$nameDerVariableN`, wobei N eine optional vorhandene Zahl ist.

Variablen mit unterschiedlichen Bezeichnern, d.h. unterschiedliche Namen und Zahlen, sind unterschiedlich. Dies bedeutet, dass sie im Normalfall unterschiedliche Werte enthalten. Dies ist insbesondere der Fall, wenn es sich um Eingabeparameter handelt, beispielsweise `$update01` und `$update02`.

7.2 XML Schema

Die konkreten Testfälle werden mit Hilfe von XML-Beschreibungen [BSI TR-03153-XML] definiert. Die logische Struktur dieser XML-Dokumente wird durch das XML Schema im Anhang dieses Dokumentes (siehe Kapitel A.1) spezifiziert. Es folgt eine Erläuterung der Elementtypen, die für die Definition der Testfälle bereitgestellt werden.

Der Elementtyp `TestCase` spezifiziert die Struktur von Testfällen. Das `TestCase`-Element ist das Wurzel-Element in XML-Dokumenten für Testfälle. Ein Testfall kann eindeutig über den Wert des `id`-Attributs von `TestCase` identifiziert werden. Dieser Wert repräsentiert den eindeutigen Bezeichner eines Testfalls. Tabelle 118 zeigt die Elementtypen, die die Informationen für einen Testfall innerhalb von `TestCase` definieren.

Elementtyp	Beschreibung	Notwendigkeit
Title	Titel des Testfalls	Gefordert
Version	Version des Testfalls	Gefordert
Purpose	Zweck des Testfalls	Gefordert
Profile	Ein oder mehrere zugeordnete Profile	Gefordert
Reference	Eine oder mehrere Referenzen auf Technische Richtlinien und andere Spezifikationen	Optional
Precondition	Eine oder mehrere Vorbedingungen für den Testfall	Optional
TestStep	Ein oder mehrere Schritte des Testfalls	Gefordert
AlternativeTestProcedures	Eine oder mehrere alternative Testverfahren für den Testfall oder einzelne Testschritte	Optional

Tabelle 118: Definition der Informationen für einen Testfall

In der Tabelle 119 werden die Elementtypen aufgeführt, die die Informationen für einen Testschritt innerhalb von `TestStep` spezifizieren.

Elementtyp	Beschreibung	Notwendigkeit
Command	Aktion für den Textschritt	Gefordert

Elementtyp	Beschreibung	Notwendigkeit
Expectedresult	Ein oder mehrere erwartete Resultate für den Testschritt	Gefordert

Tabelle 119: Definition der Informationen für einen Testschritt

Literaturverzeichnis

- BSI TR-02102 BSI: Technische Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- BSI TR-03153-1 BSI: Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme - Teil 1: Anforderungen an die Technische Sicherheitseinrichtung
- BSI TR-03153 1.0.1 BSI: Technische Richtlinie TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1, 20. Dezember 2018
- BSI TR-03153-1-TS BSI: Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme – Testspezifikation (TS) zu Teil 1
- BSI TR-03116-5 BSI: Technische Richtlinie TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung - Teil 5: Anwendungen der Secure Element API.
- BSI TR-03145 BSI: Technical Guideline TR-03145 Secure CA Operation
- BSI TR-03151-1 BSI: Technical Guideline TR-03151 Secure Element API (SE API) - Part 1: Interface Definition
- BSI TR-03151-2 BSI: Technical Guideline TR-03151 Secure Element API (SE API) – Part 2: Interface Mapping
- BSI TR-03153-XML BSI: Testfälle mit Prüfschritten und erwarteten Ergebnisse im XML Format

Anhang

A.1 XML Schema für die XML-Testfälle der BSI TR-03153-1-TS

Text 1 zeigt das XML Schema, das die Struktur der XML-Testfälle definiert.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" attributeFormDefault="unqualified"
elementFormDefault="qualified" targetNamespace="http://bsi.bund.de/TR03153"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="TestCase">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Title" type="xs:string" />
        <xs:element name="Version" type="xs:string"/>
        <xs:element name="Purpose" type="xs:string"/>
        <xs:element name="Profiles">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Profile" type="xs:string" maxOccurs="unbounded" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="References">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Reference" type="xs:string" maxOccurs="unbounded" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="Preconditions" minOccurs="0">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Precondition" type="xs:string" maxOccurs="unbounded" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="TestSteps">
```

```
<xs:complexType>
  <xs:sequence>
    <xs:element name="TestStep" maxOccurs="unbounded">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="Command" type="xs:string" />
          <xs:element name="ExpectedResults">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="ExpectedResult" maxOccurs="unbounded" type="xs:string" />
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="AlternativeTestProcedures" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="AlternativeTestProcedure" type="xs:string" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="id" type="xs:string" use="required" />
</xs:complexType>
</xs:element>
</xs:schema>
```

Text 1: XML-Schema, das die Struktur der XML-Testfälle definiert

A.2 XML Beispiele

Der Text 2 zeigt die XML-Darstellung des Testfalls STO_FUN_07, der in der Tabelle 17 in Kapitel 6.1.1 definiert wird.

```

<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/css" href="../../schema/TR-03153-1-TS.css"?>
<TestCase id="STO_FUN_07" xmlns="http://bsi.bund.de/TR03153" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://bsi.bund.de/TR03153 ../../schema/TR-03153-1-TS_version-1-1-0.xsd">
  <Title>Test case STO_FUN_07</Title>
  <Version>1.1.0</Version>
  <Purpose>Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet einen Absicherungsschritt nach einer Aktualisierung der Zeitführung innerhalb des Sicherheitsmoduls.</Purpose>
  <Profiles>
    <Profile>STORAGE_BASIC</Profile>
  </Profiles>
  <References>
    <Reference>BSI TR-03153-1</Reference>
    <Reference>BSI TR-03151-1</Reference>
  </References>
  <Preconditions>
    <Precondition>Die Technische Sicherheitseinrichtung wurde initialisiert.</Precondition>
    <Precondition>Der Nutzer timeadmin wurde von der Technischen Sicherheitseinrichtung authentifiziert.</Precondition>
  </Preconditions>
  <TestSteps>
    <TestStep>
      <Command>Aufruf der Funktionalität zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.</Command>
      <ExpectedResults>
        <ExpectedResult>Die Ausführung wird ohne Fehlermeldung beendet.</ExpectedResult>
      </ExpectedResults>
    </TestStep>
    <TestStep>
      <Command>Aufruf der Funktionalität für den Export aller Log-Nachrichten sowie Zertifikaten und Zusatzdateien.</Command>
      <ExpectedResults>
        <ExpectedResult>Die Ausführung wird ohne Fehlermeldung beendet.</ExpectedResult>
        <ExpectedResult>Die TSE-Schnittstelle gibt einen TAR-Container zurück.</ExpectedResult>
      </ExpectedResults>
    </TestStep>
  </TestSteps>

```

```

<TestStep>
  <Command>Identifikation der Log-Nachricht für die Aktualisierung der Zeit innerhalb des Sicherheitsmoduls in dem
  TAR-Container. Die Identifikation erfolgt anhand des Dateinamens.</Command>
  <ExpectedResults>
    <ExpectedResult>Der TAR-Container enthält eine Log-Nachricht für die Aktualisierung der Zeit innerhalb des
    Sicherheitsmoduls.</ExpectedResult>
  </ExpectedResults>
</TestStep>
</TestSteps>
</TestCase>

```

Text 2: XML-Darstellung des Testfalls STO_FUN_07

Der Text 3 repräsentiert die Spezifikation des Testfalls II_INI_02 in XML, der in Tabelle 48 in Kapitel 6.3.1.4 definiert wird.

```

<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/css" href="../../schema/TR-03153-1-TS.css"?>
<TestCase id="II_INI_02" xmlns="http://bsi.bund.de/TR03153" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://bsi.bund.de/TR03153 ../../schema/TR-03153-1-TS_version-1-1-0.xsd">
  <Title>Test case II_INI_02</Title>
  <Version>1.1.0</Version>
  <Purpose>Prüfung, ob bei einer wiederholten Initialisierung der Technischen Sicherheitseinrichtung eine gültige
  Fehlermeldung ausgegeben wird.</Purpose>
  <Profiles>
    <Profile>II</Profile>
  </Profiles>
  <References>
    <Reference>BSI TR-03153-1</Reference>
    <Reference>BSI TR-03151-1</Reference>
  </References>
  <Preconditions>
    <Precondition>Die Technische Sicherheitseinrichtung wurde nicht initialisiert.</Precondition>
    <Precondition>Der Nutzer admin wurde von der Technischen Sicherheitseinrichtung authentifiziert.</Precondition>
  </Preconditions>
  <TestSteps>
    <TestStep>
      <Command>Aufruf der Funktionalität zur Initialisierung der TSE.</Command>
      <ExpectedResults>

```

```
<ExpectedResult>Die Ausführung wird ohne Fehlermeldung beendet.</ExpectedResult>
</ExpectedResults>
</TestStep>
<TestStep>
  <Command>Aufruf der Funktionalität für den Export aller Log-Nachrichten sowie Zertifikaten und
Zusatzdateien.</Command>
  <ExpectedResults>
    <ExpectedResult>Die Ausführung wird ohne Fehlermeldung beendet.</ExpectedResult>
    <ExpectedResult>Die TSE-Schnittstelle gibt einen TAR-Container zurück.</ExpectedResult>
  </ExpectedResults>
</TestStep>
<TestStep>
  <Command>Identifikation der Log-Nachricht für die Initialisierung der TSE in dem TAR-Container. Die
Identifikation erfolgt anhand des Dateinamens. </Command>
  <ExpectedResults>
    <ExpectedResult>Der TAR-Container enthält eine Log-Nachricht für die Initialisierung der TSE.</ExpectedResult>
  </ExpectedResults>
</TestStep>
<TestStep>
  <Command>Aufruf der Funktionalität zur Initialisierung der TSE.</Command>
  <ExpectedResults>
    <ExpectedResult>Die Ausführung wird beendet und es wird die Fehlermeldung ErrorDeviceIsInitialized
ausgelöst.</ExpectedResult>
  </ExpectedResults>
</TestStep>
<TestStep>
  <Command>Aufruf der Funktionalität für den Export aller Log-Nachrichten sowie Zertifikaten und
Zusatzdateien.</Command>
  <ExpectedResults>
    <ExpectedResult>Die Ausführung wird ohne Fehlermeldung beendet.</ExpectedResult>
    <ExpectedResult>Die TSE-Schnittstelle gibt einen TAR-Container zurück.</ExpectedResult>
  </ExpectedResults>
</TestStep>
<TestStep>
  <Command>Identifikation der Log-Nachricht für die zweite Initialisierung der TSE in dem TAR-Container. Die
Identifikation erfolgt anhand des Dateinamens.</Command>
  <ExpectedResults>
```

```

    <ExpectedResult>Der TAR-Container enthält neben der in Testschritt 3 identifizierten Log-Nachricht keine weitere
    Log-Nachricht für die Initialisierung der TSE.</ExpectedResult>
  </ExpectedResults>
</TestStep>
</TestSteps>
</TestCase>

```

Text 3: XML-Darstellung des Testfalls II_INI_02

Der Text 4 repräsentiert die XML-Darstellung des Testfalls II_ERR_02_A, der in Tabelle 90 definiert wird.

```

<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/css" href="../../schema/TR-03153-1-TS.css"?>
<TestCase id="II_ERR_02_A" xmlns="http://bsi.bund.de/TR03153" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://bsi.bund.de/TR03153 ../../schema/TR-03153-1-TS_version-1-1-0.xsd">
  <Title>Test case II_ERR_02_A</Title>
  <Version>1.1.0</Version>
  <Purpose>Prüfung, ob Funktionalitäten beendet werden und die Fehlermeldung ErrorTimeNotSet ausgeben, wenn der
  folgende Zustand gilt: Nach der Inbetriebnahme der Technischen Sicherheitseinrichtung, wurde die Zeit innerhalb des
  Sicherheitsmoduls nicht aktualisiert. Es werden Parameter in der Form übergeben, dass die Funktionalitäten bei
  aktualisierter Zeit ohne Fehlermeldung beendet werden würden. Es wird die Funktionalität zum Erstellen oder Ändern der
  Beschreibung der TSE getestet.</Purpose>
  <Profiles>
    <Profile>II </Profile>
  </Profiles>
  <References>
    <Reference>BSI TR-03153-1</Reference>
    <Reference>BSI TR-03151-1</Reference>
  </References>
  <Preconditions>
    <Precondition>Die Technische Sicherheitseinrichtung wurde initialisiert.</Precondition>
    <Precondition>Die Zeit innerhalb des Sicherheitsmoduls wurde nicht aktualisiert.</Precondition>
    <Precondition>Der Nutzer admin wurde von der Technischen Sicherheitseinrichtung authentifiziert.</Precondition>
  </Preconditions>
  <TestSteps>
    <TestStep>
      <Command>Aufruf der Funktionalität zum Erstellen oder Ändern der Beschreibung der TSE.</Command>
      <ExpectedResults>
        <ExpectedResult>Die Ausführung wird beendet und es wird die Fehlermeldung ErrorTimeNotSet
        ausgelöst.</ExpectedResult>
      </ExpectedResults>
    </TestStep>
  </TestSteps>

```

```

</TestStep>
</TestSteps>
</TestCase>

```

Text 4: XML-Darstellung des Testfalls II_ERR_02_A

A.3 Darstellung von XML-Testfällen in einem Webbrowser

Die XML-Testfälle können mit Hilfe des XSLT-Stylesheets „TestCaseTR03153“ in Form von HTML in einem Webbrowser angezeigt werden. Die Abbildung 4 zeigt die HTML-Darstellung des XML-Testfalls STO_FUN_07 aus dem Text 2 in einem Webbrowser.

Test case STO_FUN_07

Version: 1.1.0

Purpose:

Prüfung, ob Log-Nachrichten auf dem Speichermedium gespeichert werden. Der Test betrachtet einen Absicherungsschritt nach einer Aktualisierung der Zeitführung innerhalb des Sicherheitsmoduls.

Profiles:

STORAGE_BASIC

References:

BSI TR-03153-1
BSI TR-03151-1

Preconditions:

- Die Technische Sicherheitseinrichtung wurde initialisiert.
- Der Nutzer timeadmin wurde von der Technischen Sicherheitseinrichtung authentifiziert.

Test steps:

- Step 1: Aufruf der Funktionalität zur Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.

Expected result(s):

- Die Ausführung wird ohne Fehlermeldung beendet.

- Step 2: Aufruf der Funktionalität für den Export aller Log-Nachrichten sowie Zertifikaten und Zusatzdateien.

Expected result(s):

- Die Ausführung wird ohne Fehlermeldung beendet.
- Die TSE-Schnittstelle gibt einen TAR-Container zurück.

- Step 3: Identifikation der Log-Nachricht für die Aktualisierung der Zeit innerhalb des Sicherheitsmoduls in dem TAR-Container. Die Identifikation erfolgt anhand des Dateinamens.

Expected result(s):

- Der TAR-Container enthält eine Log-Nachricht für die Aktualisierung der Zeit innerhalb des Sicherheitsmoduls.

Abbildung 4: Darstellung eines XML-Testfalls in einem Webbrowser

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
CSP	Crypto Service Provider
HTML	Hypertext Markup Language
ICS	Implementation Conformance Statement
PKI	Public-Key-Infrastructure
SDI	Standardized Digital Interface
TAR	Datencontainer (Tape Archiver)
TR	Technische Richtlinie
TSE	Technische Sicherheitseinrichtung
XSL	Extensible Stylesheet Language
XSLT	XSL Transformation
XML	eXtensible Markup Language